ETSI TS 101 909-20-2 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 2: Streamed multimedia services

Reference

DTS/AT-020020-20-02

Keywords

IPCable, Lawful Interception

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 2, of a multi-part deliverable. Full details of the entire series can be found in part 1 [1].

Introduction

The cable industry in Europe and across other global regions have 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 Internet Protocol (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.

1 Scope

The present set of documents specify 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 Fibre/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 [6] and ES 200 800 [7].

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).

The present document of the above mentioned series of ETSI deliverables specifies the interception of those multi-media services carried over the network defined in the remainder of the above mentioned series of ETSI deliverables that do not fall into the interception domain covered by sub-part 1 of TS 101 909-20-1 [5].

The present document describes the implementation of a Lawful Interception (LI) interface in an IPCablecom system. It provides the requirements and specification of the interface within an IPCablecom system for the purpose of providing data to Law Enforcement Agencies (LEAs) in the area of (LI) of communications.

The provision of a (LI) interface for IPCablecom is a national option, however where it is provided it shall be provided as described in the present document.

The structure of (LI) in telecommunications is in two parts: The internal interface of a network that is built using a particular technology; and, the external interface (known as the Handover Interface) that links the LEA to the network. Between these two parts may lie a mediation function to cater for national variances and delivery of the result of interception.

The Handover Interface is specified in TS 102 232 [11] and TS 102 234 [10]. In addition, the Handover Interface may be the subject of national regulation and therefore the mediation function may also be a matter of national regulation.

The subject of the present document is the internal LI interface that lies between the IPCablecom infrastructure and the mediation function.

The present document describes the data content of information flows from the IPCablecom system to the mediation function. The present document is structured as follows:

- clause 4 describes the IPCablecom architecture and services to which LI applies;
- clause 5 presents architecture for LI in an IPCablecom system;
- clause 6 presents the data model and behaviour for interception of signalling;
- clause 7 presents the data model and behaviour for interception of the content of communication;

NOTE 3: The content of communication in IPCablecom is an IP packet.

- clause 8 presents the security provisions for LI;
- the annexes provide illustrations of the management of LI in an IPCablecom environment.

The present document applies to IPCablecom services where access to the communication of IPCablecom users is available in a network, and where the services being intercepted do not include the PSTN/ISDN emulation services whose interception is described in TS 101 909-20-1 [5].

The present document does not describe the means of transporting data from the IPCablecom network to the LEA, but describes only the means of capturing and encoding the activities of a target within the IPCablecom network and delivering this data to the mediation function.

The present document does not define the operations or technical requirements of the Handover Interface that takes data from the mediation function to the LEMF.

The present document does not define the operations or technical requirements of the Law Enforcement Monitoring Facility (LEMF).

NOTE 4: No test point is provided in the present document to ensure conformance.

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

[2] ETSI TS 101 909-2: "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".

[3] ETSI TS 101 909-5: "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".

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

[5] ETSI TS 101 909-20-1: "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".

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

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

[8] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

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

[10] ETSI TS 102 234: "Lawful Interception (LI); Service-specific details for internet access services".

[11] ETSI TS 102 232: "Lawful Interception (LI); Handover specification for IP delivery".

[12] ITU-T Recommendation J.179: "IPCablecom support for multimedia".

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

[14] 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)".

[15] IETF RFC 2578: "Structure of Management Information Version 2 (SMIv2)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 909-20-1 [5] and the following apply:

access node: a layer two termination device that terminates the network end of the J.112 connection

NOTE: It is technology specific. In J.112 [B16] annex A it is called the INA while in annex B it is the CMTS. In the present 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 J.112 [B] (HFC Access Network) connection

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

CMS: an 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

NOTE: 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

Coordinated Universal Time (UTC): time scale maintained by the Bureau International de l'Heure (International Time Bureau) that forms the basis of a coordinated dissemination of standard frequencies and time signals

NOTE: The source of this definition is ITU-T Recommendation 460-2 of the Consultative Committee on International Radio (CCIR). CCIR has also defined the acronym for Coordinated Universal Time as UTC.

handover interface: physical and logical interface across which the results of interception are delivered from a network operator/service provider to an LEMF

identity: technical label which may represent the origin or destination of any telecommunications traffic

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

(B) includes:

(i) 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;

(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

EXAMPLE: Unsuccessful call attempts, service associated information or data (e.g. service profile management by subscriber) and location information. This is also called call intentifing information in the present document.

interception (lawful interception): action (based on the law), performed by a network operator/service provider, 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: an 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

IPCablecom Telecommunications Service Provider (IPCC/TSP):. as used in the present document, 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 the present document.

IRI transaction: intercept related information messages associated to a specific communication case or attempt indicating the actual begin and end through separate message types

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

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

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 the present document

lawful authorization: permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator/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: 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

NOTE: 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).

Quality of Service (QoS): quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of Service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

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

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 an LEA. 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: function logically part of the OSS

NOTE: May be implemented according to operator preferences or national requirements.

target identity: identity associated with a target service (see below) used by the interception subject

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

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

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

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

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:

AM	Application Manager
ASN.1	Abstract System Notation 1
BER	Basic Encoding Rules
CC	Content of Communication
CCIF	Content of Communication Interception Function
CID	Call IDentifier
CM	Cable Modem
CMS	Call Management Server
CMTS	Cable Modem Termination System
COPS	Common Open Policy Service
DF	Delivery Function
DHCP	Dynamic Host Configuration Protocol
DSS1	Digital Subscriber Signalling System No 1
DTMF	Dual Tone Multi Frequence
EMTA	Embedded Multimedia Terminal Adaptor
ESP	Encapsulated Security Payload
HFC	Hybrid Fibre/Coaxial
HI	Handover Interface
IANA	Internet Assigned Number Authority
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCablecom/TSP	IPCablecom Telephony Service Provider
IRI	Intercept Related Information
IRIIF	Intercept Related Information Interception Function
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIAF	Lawful Interception Administration Function
LIF	Lawful Interception Function
LIID	Lawful Interception IDentifier
LIMF	Lawful Interception Mediation Function
MAC	Medium Access Control
MD	Mediation Device
MF	Mediation Function
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MPLS	Multi Protocol Label Switching
MSO	Multiple System Operator
MTA	Multimedia Terminal Adaptor
NCS	Network Controlled Signalling
NWO	NetWork Operator
OLC	Open Logical Channel
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PS	Policy Server
QoS	Quality of Service
RCD	Resource Control Domain
RKS	Record Keeping Server
RSVP	Resource ReSerVation Protocol
RTSP	Real Time Streaming Protocol
SAP	ServiceAccess Point
SCD	Service Control Domain
SCE	Signalling Control Entity
SDL	Specification and Description Language
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMIv2	Structure of Management Information version 2

SMS	Short Message Service
SNMP	Simple Network Management Protocol
SP	Service Provider
TCP	Transmission Control Protocol
TSP	Telephony Service Provider
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
WWW	World Wide Web

4 Overview and analysis of IP multimedia Time Critical Services

4.1 Overview

This clause introduces the core concepts of the IPCablecom domain to place the L requirements in context. Clause 4.2 describes the architecture of IPCablecom networks, and clause 4.3 introduces the service models supported by IPCablecom.

4.2 Architecture (TS 101 909-2)

The following scenarios are possible for the provision of multimedia services in an IPCablecom environment:

1) Multimedia services with signalling control at the Call Management Server (CMS), corresponding to an IPCablecom architecture (see figure 1).

2) Multimedia services using a separate Signalling Control Entity (SCE) (see figure 2).

3) Decentralized multimedia services (peer-to-peer communications) (see figure 3).

NOTE: An additional case which may be considered is the cable access legacy layer 2 architectures based on PPPOE, VLAN, or MPLS. These architectures do not comply with TS 101 909-2 [2] (IPCablecom), and sometimes do not comply with TS 101 909-11 [4] (EuroDOCSIS) (PPPOE and MPLS cases). These cases are partially treated in ES 201 158 [8].

4.2.1 IPCablecom architecture

The architecture of an IPCablecom system is shown in figure 1. It identifies the main components of the system and is the basis for Lawful Interception (LI) considerations.

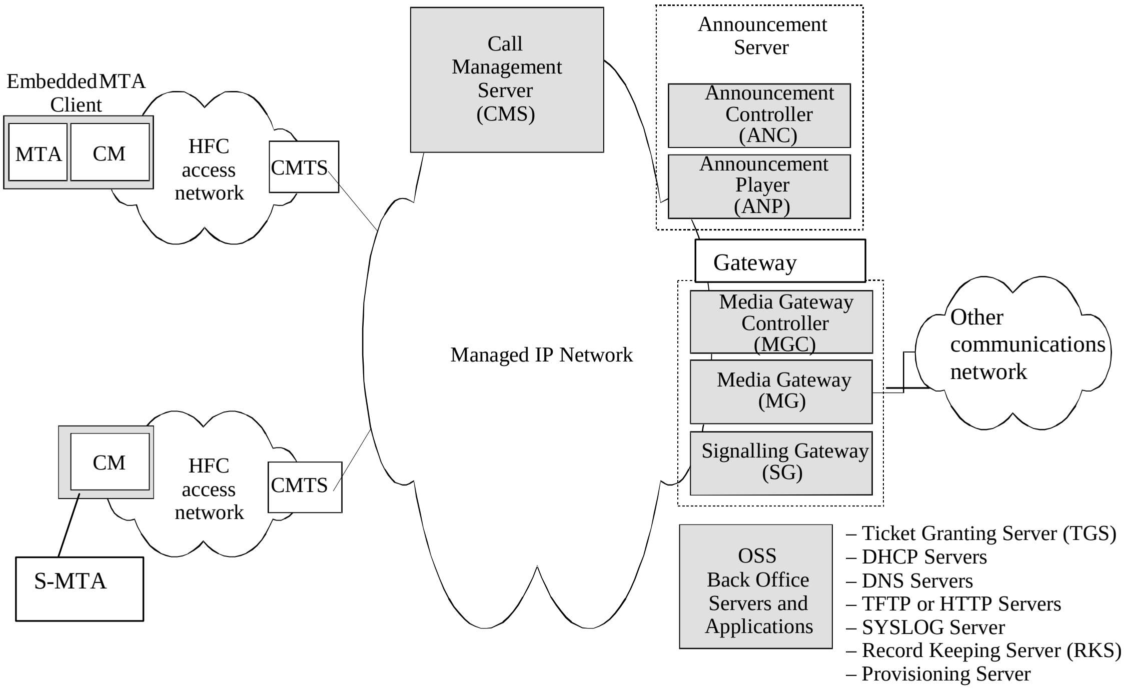


Figure 1: IPCablecom architecture (source TS 101 909-1 [1])

Conventional multimedia services where the signalling is controlled by the CMS use the architecture depicted in figure 1. The services supported by this architecture include but are not restricted to voicebox services, reminder services, and call conference.

4.2.2 Generic centralized architecture

Figure 2 describes the architecture required to support services that are controlled by an entity different from the CMS. The signalling control protocol may differ from Network Controlled Signalling (NCS).

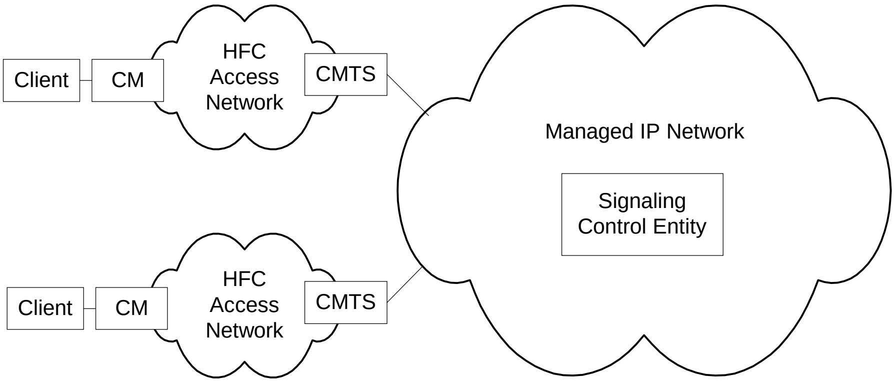


Figure 2: Architecture for centralized multimedia services using a SCE

Two distinct cases need to be considered:

- The SCE is not part of the IPCablecom system:
  - IPCablecom/TSP has no control over the SCE;
- The SCE is part of the IPCablecom system:
  - IPCablecom/TSP has control over the SCE;
  - IPCablecom may prescribe interfaces for SCE to the IPCablecom system.

ITU-T Recommendation J.179 [12] defines a multimedia framework that allows for multimedia services using a SCE different from the CMS.

4.2.3 Decentralized architecture (peer-to-peer)

Decentralized multimedia services, also called peer-to-peer services, do not use any central signalling entity. The architecture for such services is illustrated in figure 3. The sessions are established directly between the two clients.

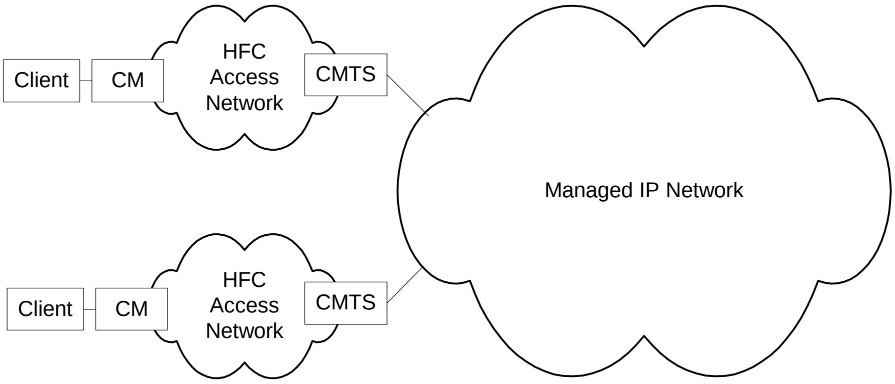


Figure 3: Architecture for decentralized multimedia services

4.2.4 Multimedia architecture in IPCablecom

In order to extend the services supported by the IPCablecom architecture, ITU-T has defined multimedia support for this architecture, recognizing that:

- It is difficult to identify a unique session signalling protocol used for multimedia applications:
  - both proprietary and standard protocols are used currently by application service providers.
- It is difficult to identify a unique security architecture:
  - the security architecture as described in ES 201 488 [6] may continue to be applied.

As explained below, this architecture covers the cases described in clauses 4.1.1 to 4.1.3.

The multimedia architecture is shown in figure 4 and the defined interfaces within it are shown in figure 5.

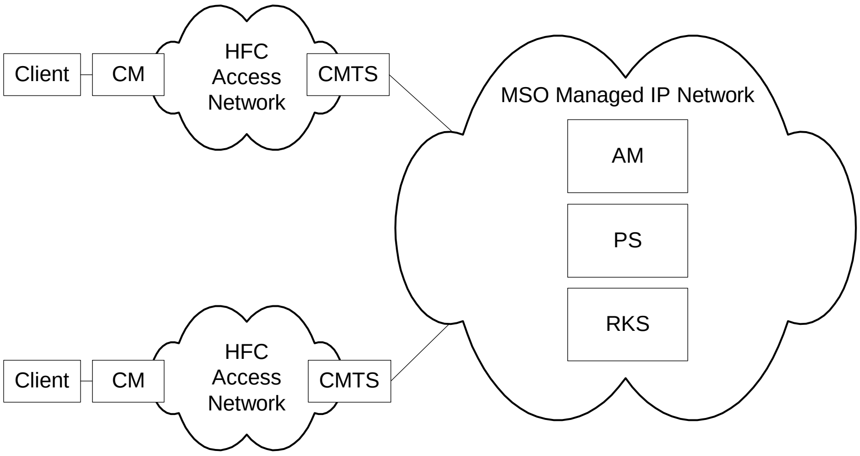


Figure 4: Multimedia framework architecture

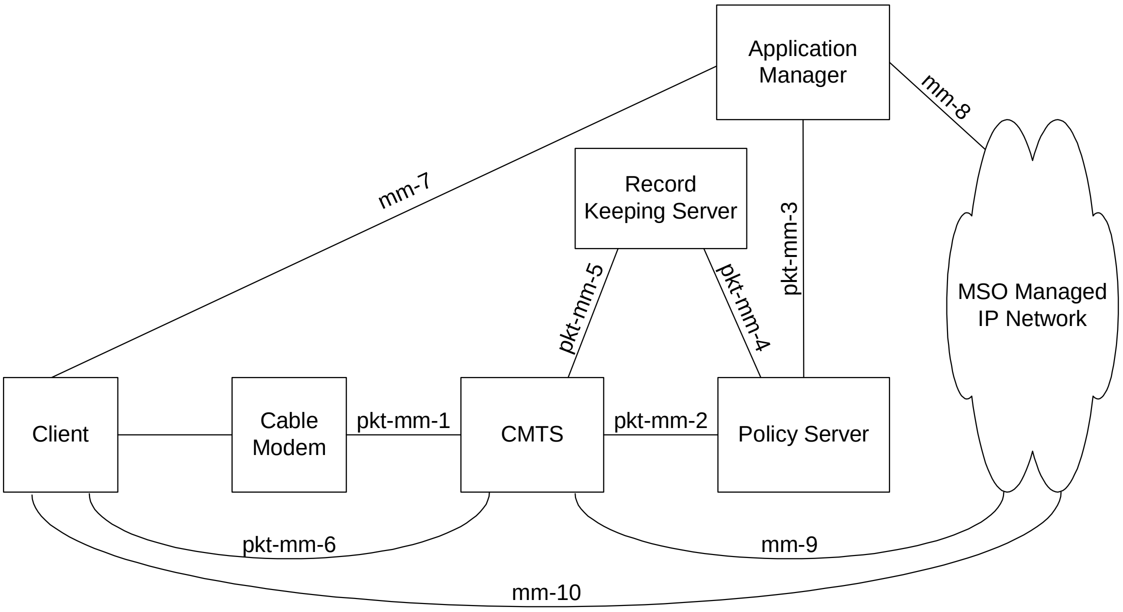


Figure 5: Multimedia QoS interfaces breakdown

When comparing this architecture to the IPCablecom architecture:

- The Embedded Multimedia Terminal Adaptor (EMTA) or remote Multimedia Terminal Adaptor (MTA) has been replaced by one or several clients, which represent the upper layer entity (layer 3 and above), as compared with the Cable Modem (CM) which covers layers 1 and 2. The client is a generic entity:
  - It can be an IPCablecom MTA.
  - It can be a legacy client (PC, handset, game console, etc.) which is Quality of Service (QoS) aware or non QoS aware.
- The CMS is replaced by a generic Application manager (AM) and PS; whereas the application signalling (mm-7) can be standard or proprietary, the interfaces been AM and PS, and between the PS and the CMTS are standard.

A brief description of each interface of the multimedia architecture is given in table 1.

Table 1: Multimedia architecture interfaces

Interface	Description	Notes
pkt-mm-1	CMTS - CM	The CM may request QoS from the CMTS via DSx signalling. Alternatively, the CMTS may instruct the CM to setup, teardown or change a service flow in order to satisfy a QoS request, again via DSx signalling.
pkt-mm-2	PS - CMTS	This interface is fundamental to the policy-management framework. It controls policy decisions, which may be: (a) pushed by the PS onto the CMTS, or (b) pulled from the PS by the CMTS. The interface also allows for proxied QoS requests on behalf of a client. In some scenarios, this interface may also be used to inform the PS when QoS resources have become inactive.
pkt-mm-3	AM - PS	The AM may request that the PS install a policy decision on the CMTS on behalf of the client. This interface may also be used to inform the AM of changes in the status of QoS resources.
pkt-mm-4	PS - RKS	The PS sends event messages to the Record Keeping Server (RKS) to track policy decisions related to QoS.
pkt-mm-5	CMTS - RKS	The CMTS sends the RKS event messages to track requests for and usage of QoS (e.g., service flow additions, changes, deletions, and volume metrics).
pkt-mm-6	Client - CMTS	The client may use this interface to directly request and manage QoS network resources. If authorized, these resources are provided by the CMTS.
mm-7	Client - AM	This interface may be used by the client to interact with the AM and to request and manage QoS resources indirectly. This interface is out of scope for this version of the present document.
mm-8	AM - Peer	The AM may use this interface to interact with some other entity that is part of the application in question. This interface is out of scope for this version of the present document.
mm-9	CMTS - MSO-Managed IP Network	This interface on the CMTS may be used in support of end-to-end QoS requests beyond the access network. This interface is out of scope for this version of the present document.
mm-10	Client - Peer	The Client may use this interface to interact with some other entity that is part of the application in question. This interface is out of scope for this version of the present document.

4.2.5 AM - PS - CMTS policy architecture

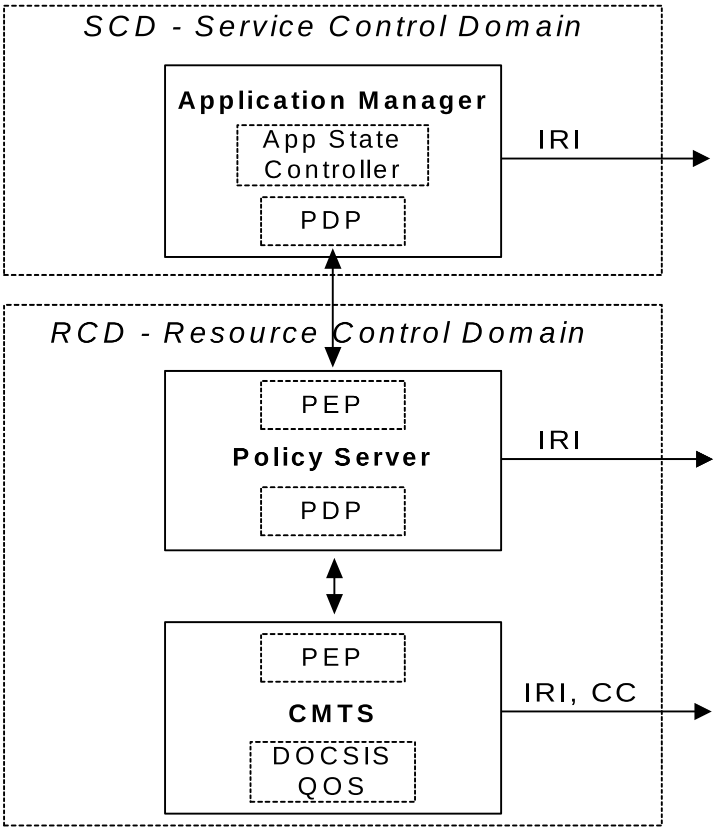
The interface between the AM and the PS, and between the PS and the CMTS is based on Common Open Policy Service (COPS).

Two distinct domains are defined:

- The Resource Control Domain (RCD):
  - The logical grouping of elements that provide connectivity and network resource level policy management in the access cable network domain.
  - The RCD includes the CMTS and the PS.
- The Service Control Domain (SCD):
  - The logical grouping of elements that offer applications and content to service subscribers.
  - The AM resides in the SCD.

NOTE 1: There may be one or more SCDs related to a single RCD.

NOTE 2: Each RCD may interact with one or more SCDs.



PEP: Policy Enforcement Point.
PDP: Policy Decision Point.

Figure 6: Policy architecture

The roles of the multimedia components are the following:

- The AM is responsible for application or session-level state and for applying SCD policy;
- The PS is responsible for applying RCD policy and for managing relationships between AMs and ANs;
- And the CMTS is responsible for performing admission control and managing network resources through service flows as defined in ES 201 488 [6].

4.2.6 Traffic control using gates

COPS conveys policy decisions by using the concept of gates to control traffic.

A gate is associated to traffic in one direction (a bi-directional session will open 2 gates), and may reside in the following logical states:

- Authorized - the PS has authorized the flow with resource limits defined.
- Reserved - resources have been reserved for the flow.
- Committed - resources are active and are being used.

The gate contains identification, QoS and traffic profile information about the session.

4.3 Multimedia service scenarios

This clause describes scenarios that may be supported by an IPCablecom Network Operator (NWO).

The scenarios cover services where the IPCablecom NWO controls the call control signalling and QoS signalling, through to cases where the IPCablecom NWO is only transporting IP traffic for the end customers. The following clauses describe those scenarios .

4.3.1 Scenarios for QoS-based multimedia services

ITU-T Recommendation J.179 [12] defines a framework that support QoS-based multimedia services and identifies three architectural scenarios in support of three client types.

The following three clauses describe the scenarios corresponding to these client types in more detail.

4.3.1.1 Support of client type 1

Client Type 1 represents existing "legacy" endpoints that are not QoS-aware and do not have QoS-oriented signalling capabilities. These clients do not implement messaging as described in TS 1-1 909-5 [3]. This client type communicates with an AM to request service. It does not request QoS resources directly from the access network.

Figure 7 shows an overview of the entities involved in the QoS signalling.

The client issues a "Service Request" to the AM who determines the QoS required for the requested service and starts the QoS reservation process by sending a "Policy Request" to the PS. The PS validates the request against internal rules, depending on the SP internal policies, and sends on a positive outcome a "Policy Set" message to the CMTS granting the client the requested QoS levels.

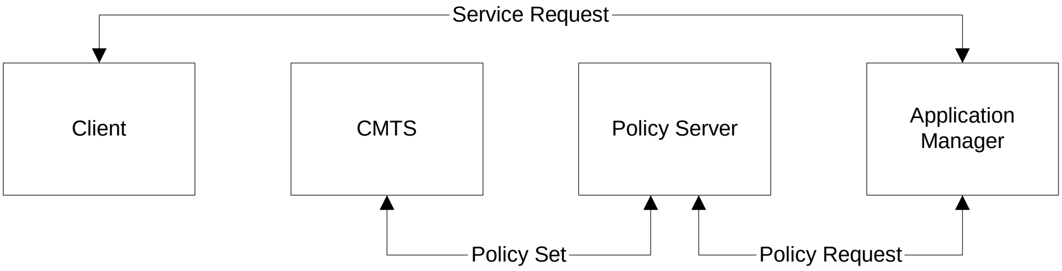


Figure 7: Information flow for proxied QoS with policy push

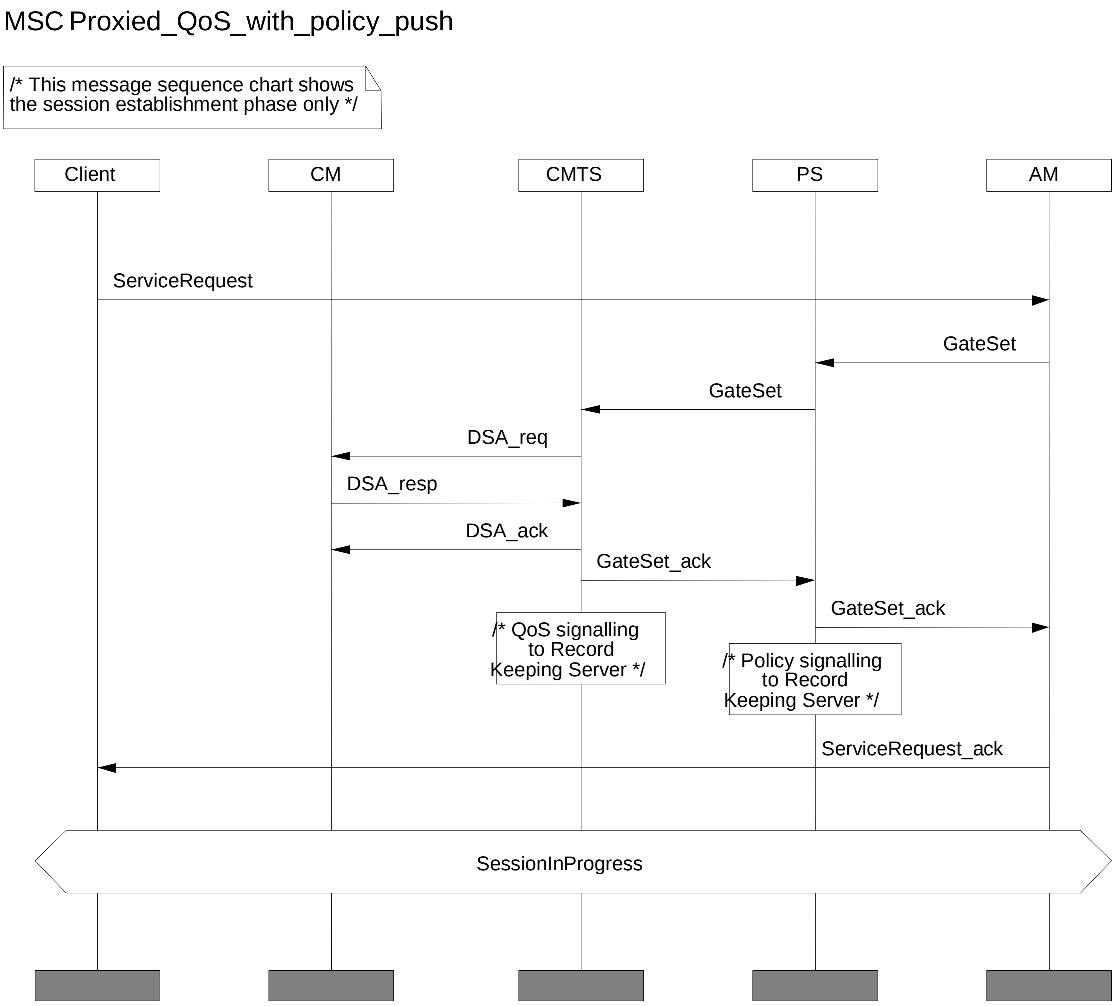

MSC Proxied_QoS_with_policy_push
/* This message sequence chart shows the session establishment phase only */
Client
CM
CMTS
PS
AM
ServiceRequest
GateSet
GateSet
DSA_req
DSA_resp
DSA_ack
GateSet_ack
GateSet_ack
/* QoS signalling to Record Keeping Server */
/* Policy signalling to Record Keeping Server */
ServiceRequest_ack
SessionInProgress

Figure 8: Message Sequence Chart for client type 1 requesting QoS

4.3.1.2 Support of client type 2

Client Type 2 supports QoS signalling based on TS 101 909-5 [3]. An overview of the QoS request scenario is illustrated in figure 9.

The client requests a service from the AM who sends the "Policy Request" on behalf of the client to the PS. In the following, the PS "pushes" the policy to the CMTS which grants the QoS levels on the client's request.

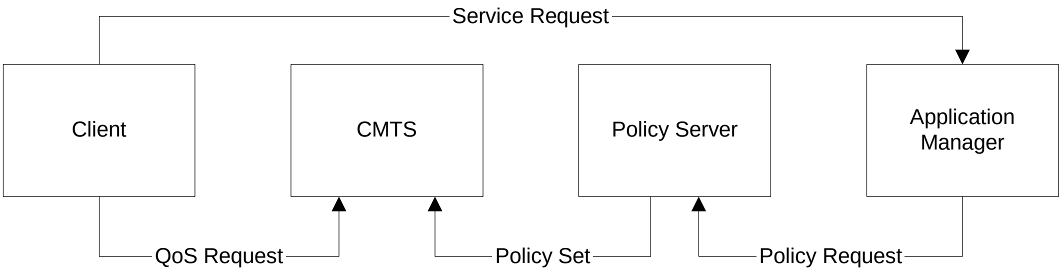


Figure 9: Information flow for client-requested QoS with push policy

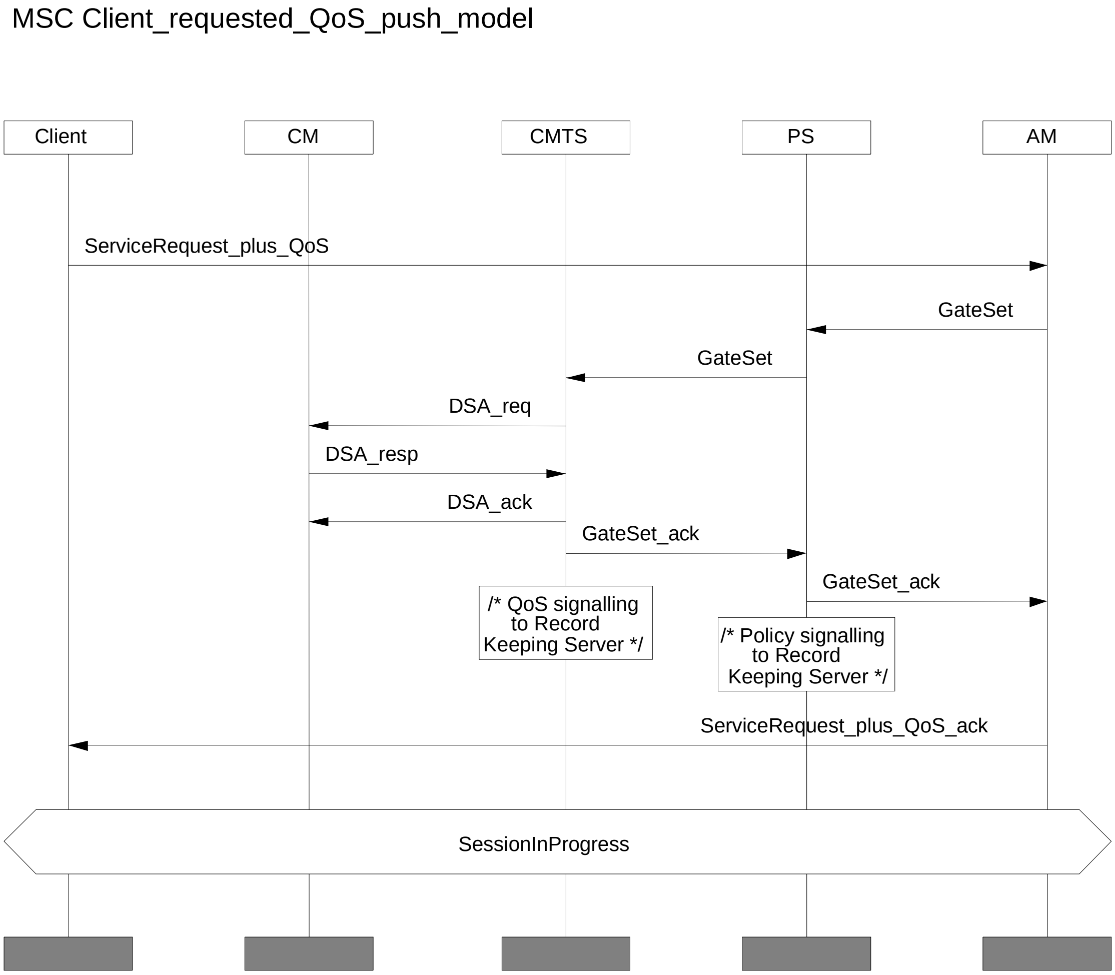

MSC Client_requested_QoS_push_model
Client
CM
CMTS
PS
AM
ServiceRequest_plus_QoS
GateSet
GateSet
DSA_req
DSA_resp
DSA_ack
GateSet_ack
GateSet_ack
/* QoS signalling to Record Keeping Server */
/* Policy signalling to Record Keeping Server */
ServiceRequest_plus_QoS_ack
SessionInProgress

Figure 10: Message Sequence Chart for client type 2 requesting QoS

4.3.1.3 Support of client type 3

Client Type 3 does not interact with an AM. It directly requests QoS treatment from the access network. This client type uses Internet Engineering Task Force (IETF) standards-based Resource Reservation Protocol (RSVP) to request QoS resources directly from the CMTS.

This scenario relates to QoS-supporting peer-to-peer multimedia services. The clients requests QoS directly at the CMTS which constructs a policy request that it sends to the PS asking for the validation of the request. On a positive reply the CMTS authorizes the resource reservation and establishes the service flow. Figure 11 illustrates the information flow for this scenario.

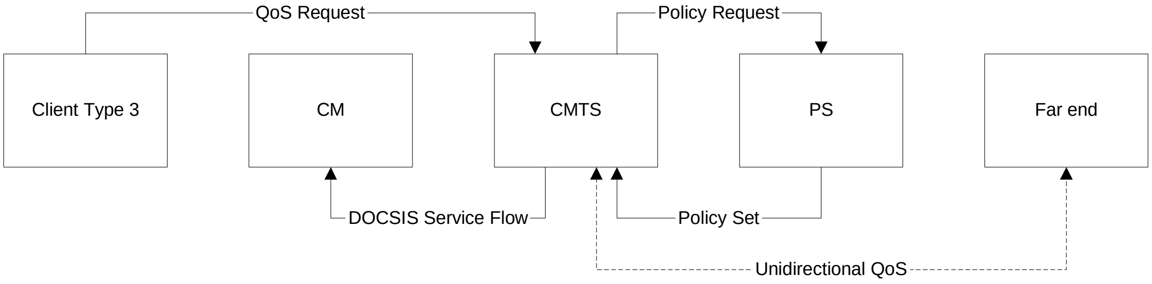


Figure 11: Information flow for client-request QoS with pull-policy

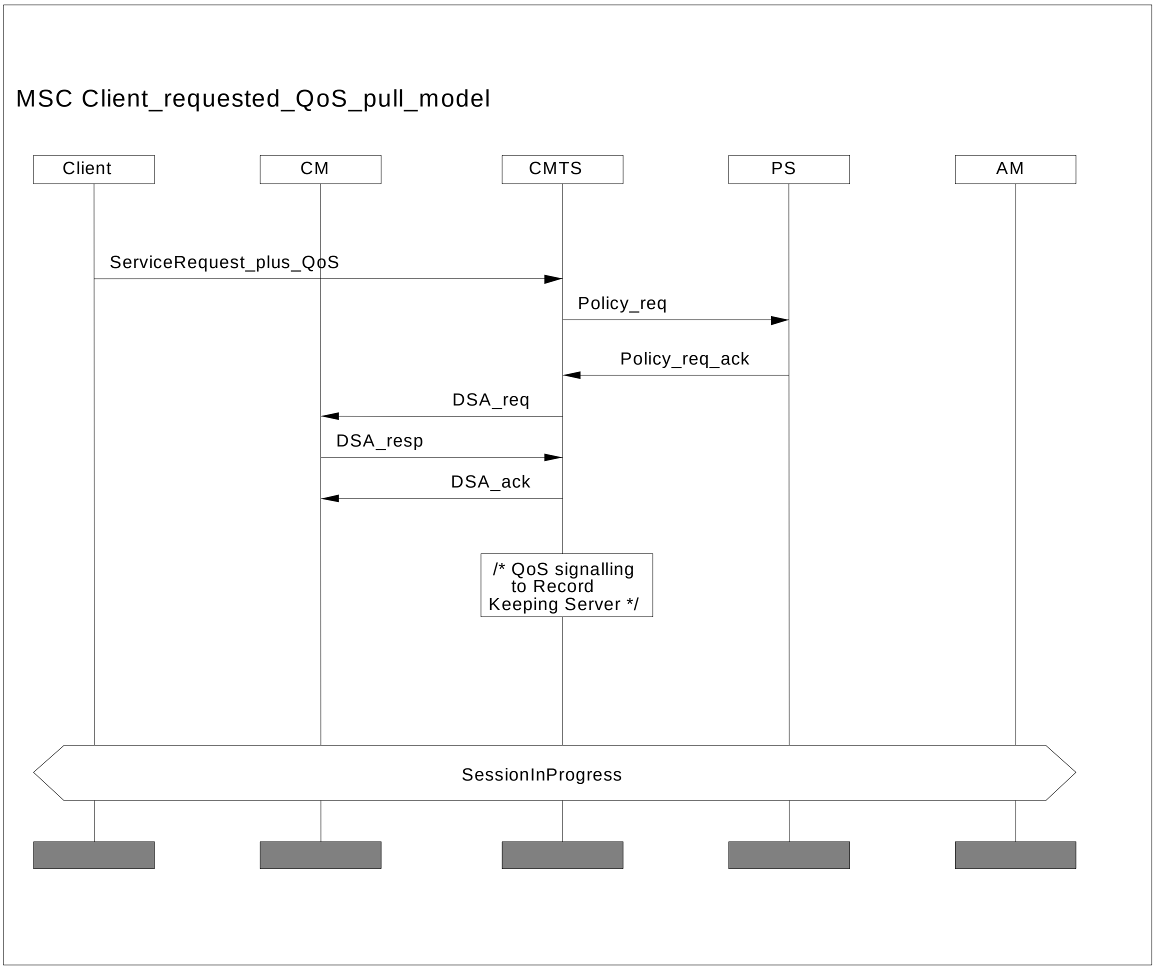


Figure 12: Message Sequence Chart for client type 3 requesting QoS

4.3.2 QoS-unaware multimedia communications scenarios

One basic property of the IPCablecom architecture is that it provides the end user with IP connectivity. This allows for conventional "Internet" services including:

- E-Mail service.
- Access to the World Wide Web (WWW).
- 3rd party services, e.g. Web-Short Message Service (SMS).

The signalling entities of the IPCablecom architecture do not take part in such services.

In these scenarios the IPCablecom architecture only conveys IP traffic. IPCablecom is able to identify the source and the target of this traffic.

4.3.2.1 Centralized services

Centralized services are those services where an IPCablecom NWO provides the IP access and some 3rd party acts as SP. The IPCablecom NWO does not have access to service related information. Figure 13 depicts the architecture of such a scenario. In the figure two aspects of the network are mixed the IP access aspect and the service aspect. The access is covered by end-user 1 being connected via the CM and the CMTS to the IPCablecom network. The 3rd party SP may be located, as indicated in the figure, in a separate IP domain. Technically it may also be located in the IPCablecom domain just using the IP access to provide its service.

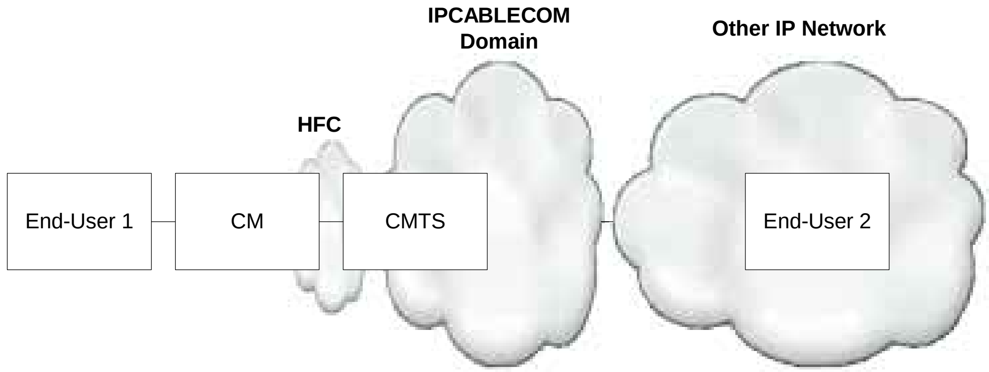


Figure 13: Centralized 3rd party service

4.3.2.2 Peer-to-peer applications

In this scenario the end users communicate directly with each other. There is no signalling visible to the IPCablecom NWO.

As shown in figure 14 there may be more than two parties involved in the communication.

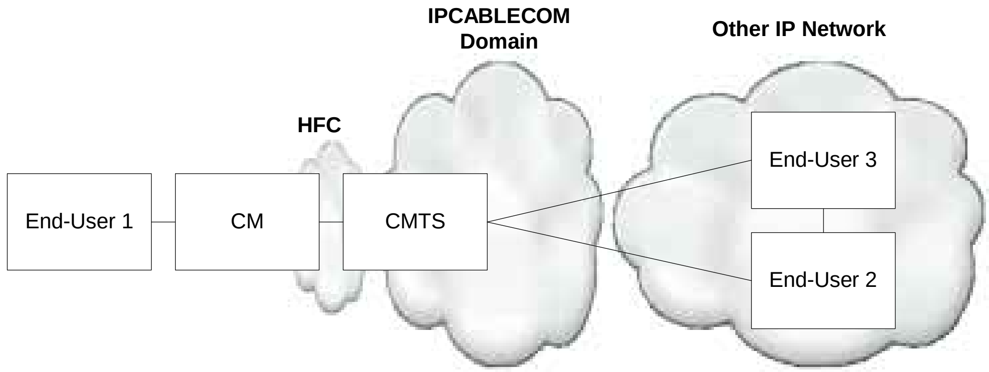


Figure 14: Example of a peer-to-peer multimedia applications

5 LI architecture for IP multimedia Time Critical Services

5.1 Overview

The overall interception framework is extended from the model described in clause 5.2 of ES 201 158 [8] and from the architecture identified in clause 5 of TS 101 671 [9] (see figure 15).

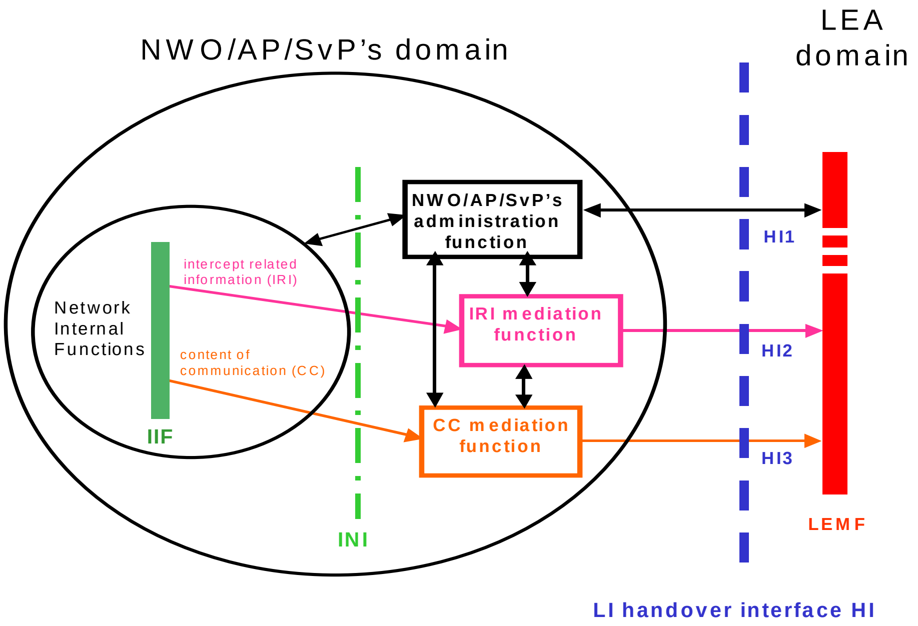

NWO/AP/SvP's domain
LEA domain
NWO/AP/SvP's administration function
Network Internal Functions
intercept related information (IRI)
content of communication (CC)
IRI mediation function
CC mediation function
IIF
INI
HI1
HI2
HI3
LEMF
LI handover interface HI

Figure 15: Functional block diagram showing Handover Interface HI (from TS 101 671 [9])

The scope of the present document is the NMW/AP/SvP's domain as shown in figure 15. The present document describes the internal interfaces INI1, INI2 and INI3 as shown in figure 16.

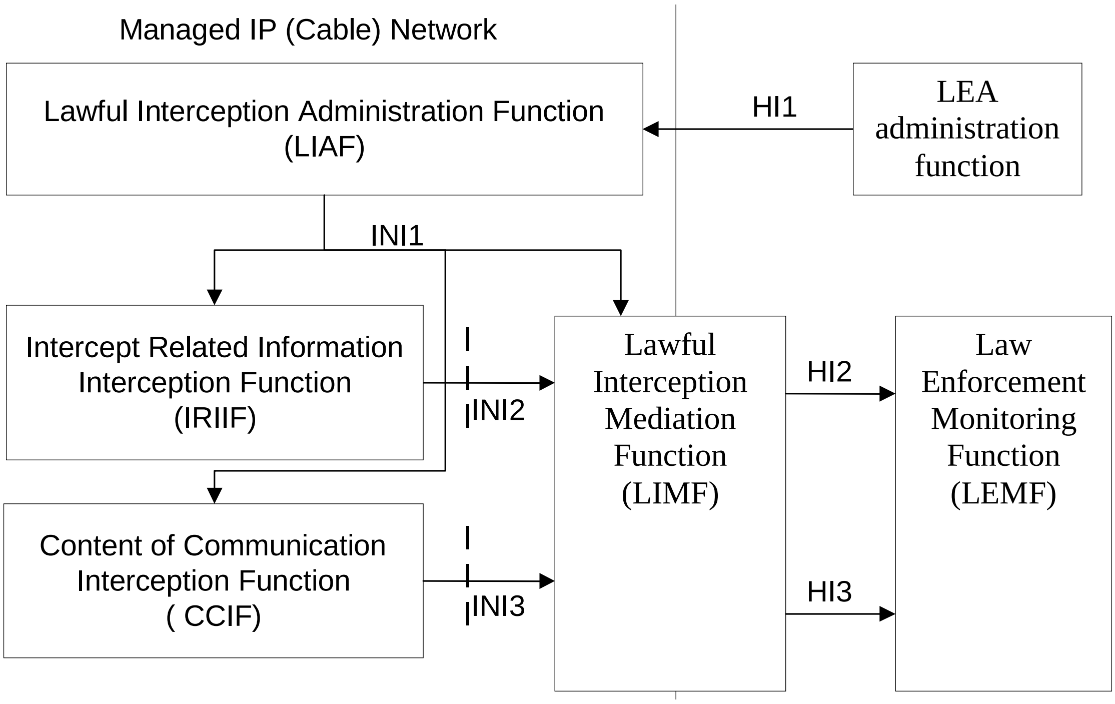

Managed IP (Cable) Network
Lawful Interception Administration Function (LIAF)
HI1
LEA administration function
INI1
Intercept Related Information Interception Function (IRIIF)
INI2
Lawful Interception Mediation Function (LIMF)
HI2
Law Enforcement Monitoring Function (LEMF)
Content of Communication Interception Function (CCIF)
INI3
HI3

Figure 16: Reference Model for Lawful Interception

The administrative information is exchanged between the LIAF, the LI functions and the Lawful Interception Mediation Function (LIMF) via INI1.

Internal interface INI2 carries Intercept Related Information (IRI) from the Intercept Related Information Interception Function (IRIIF). Internal interface INI3 carries Content of Communication (CC) information.

5.2 Description of functional elements

5.2.1 Intercept Related Information Interception Function (IRIIF)

The purpose of the IRIIF is to generate information related to calls or sessions or and other information involving interception targets identified by Law Enforcement Agency (LEA) sessions, i.e. IRI.

NOTE: The terms call and session are used within the multimedia applications world. Some applications may emulate the behaviour normally associated with telephony and the term call is used (bounded session), other applications may be of an unbounded nature and the term session is used. Neither term is more correct than the other.

The IRI information is sent to the LIMF to be delivered to the Law Enforcement Monitoring Facility (LEMF) over interface HI2.

5.2.2 Content of Communication Interception Function (CCIF)

The CCIF shall cause the CC to be duplicated and passed to the 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 CC is sent to the LIMF and it is formatted in accordance with later clauses for delivery to the LEMF over interface HI3.

NOTE: Intercepted content of communication is always an IP packet.

5.2.3 Lawful Interception Mediation Function (LIMF)

The LIMF receives information from the IRIIF(s) and CCIF(s) within the IPCablecom network and formats that received information to be passed on to the LEMF. If there is more than one IRIIF within an IPCablecom network the LIMF shall manage the reporting state of the call so that information is sent to the LEMF as if it were from a single IRIIF. In this case the LIMF shall ensure that the reported information elements represent a consistent and single view of the intercept.

The LIMF incorporates the mediation function defined in ES 201 158 [8] as "A function which selects sequences and transforms information, including CC when necessary, between a number of IIFs and the HI. Sometimes the mediation function may be a null function, e.g. direct delivery of CC to the LEMF via HI3 with no changes."

5.2.4 Lawful Intercept Administration Function (LIAF)

In each IPCablecom network there shall exist an 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 is described here only for completeness.

The information available at the LIAF includes:

NOTE 1: This list is adapted from clause 7.1 of TS 101 671 [9].

- Identification of the interception subject (Target Identity);

NOTE 2: The target identity is any valid ID used in a cable system that is uniquely related to the target at the time and point of interception. This may include but not be restricted to: MAC address, e-mail address, login name, IP address (granted by DHCP or other), E164 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;
- Address of the LEMF to which IRI information should be sent i.e. the HI2 destination address (if applicable);

- 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 transported via INI1 to the relevant elements (the IRIIF, LIMF and CCIF as necessary).

NOTE 3: More than one LEA may intercept the same target requiring that for the same target several LEA need to be served with each individual interception being uniquely identified and maintained. The present document does not specify how to serve multiple instances of interception.

5.3 LI Architecture

5.3.1 LI in the multimedia architecture of J.179

The multimedia architecture specified in ITU-T Recommendation J.179 [12] maps to the LI reference model as follows.

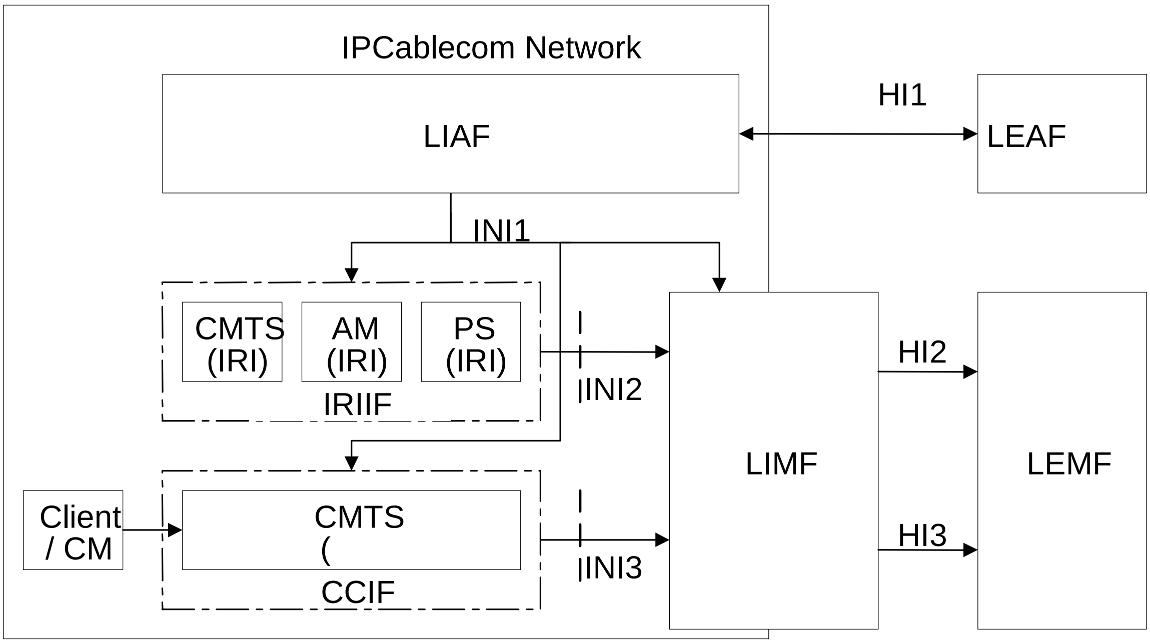


Figure 17: architecture for LI

The CMTS, AM or PS may take the role of the IRIIF. Which entity serves as IRIIF depends also on the communication scenario. In an actual implementation of the architecture there may be even more than one entity delivering IRI to the DF. Only the CMTS acts as CCIF.

In the multimedia case , the AM belongs to the MSO managed domain; and may provide IRI information to the LIMF, including session information, session status information (start, stop, etc.), and security information. The multimedia architecture can be extended by considering that the AM is outside the MSO managed domain. In such a case, only a restricted set of IRI information can be delivered by the AM.

NOTE: In the case of a decentralized architecture (including peer to peer application) as shown in figure 3, the architecture presented in figure 8 is still valid. However, the AM may not exist and therefore the information exchange may be limited to the one between the CMTS and the PS.

IRI information which can be delivered to the LIMF by the CMTS and the PS includes:

- Events like session start/stop/redirection;
- Session information including classifiers, QoS parameters, security information (when accessible).

The CMTS can provide the CC information, with the following options:

- Duplication of complete traffic belonging to one service flow (default option);
- Duplication of a part of the traffic belonging to one service flow, defined by additional classifiers (see TS 101 909.11 [4] for classifiers definition); the latter requires additional functionality in the CMTS and may cause scalability issues.

5.3.2 LI architecture for QoS unaware communication

The mapping of the multimedia architecture [12] to the LI reference model for QoS unaware communication is shown in figure 18.

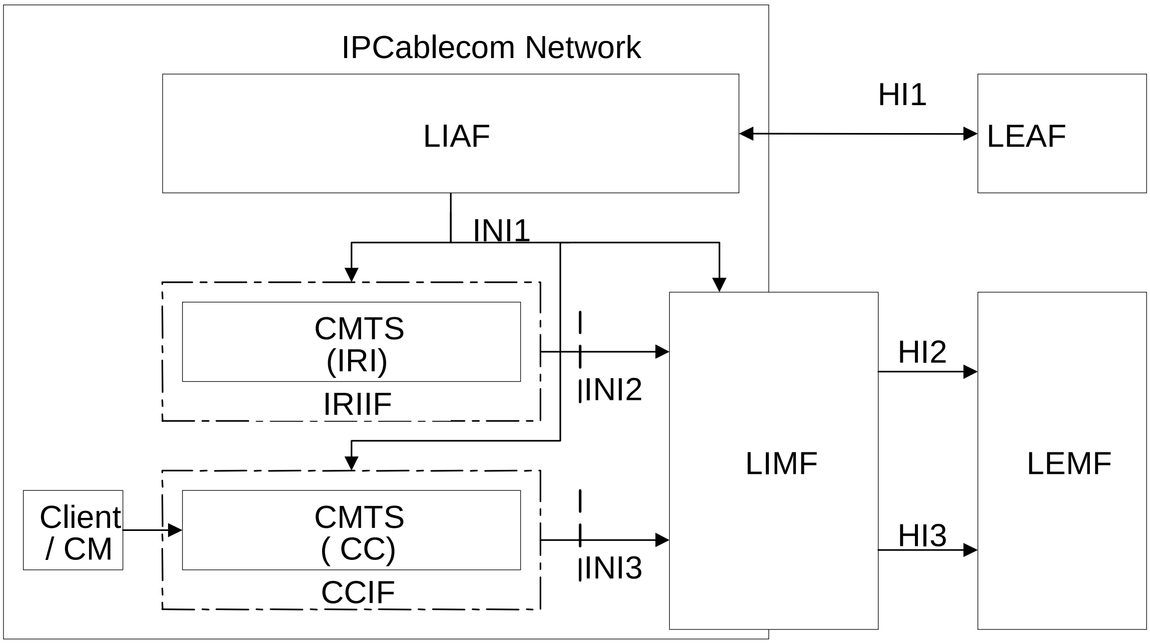


Figure 18: LI architecture for QoS unaware communication

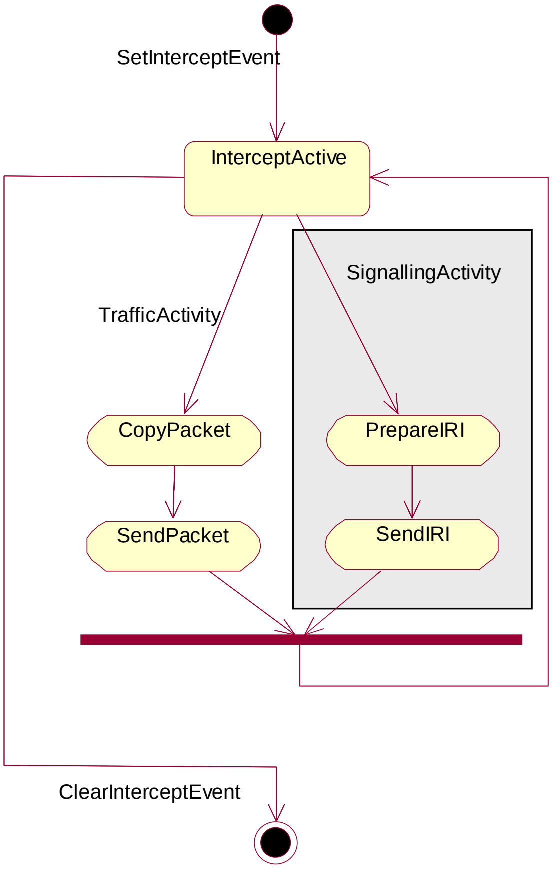
For QoS unaware communication there is no QoS signalling or no call control signalling that is passing any of the domains entities. Hence, the only information that may be intercepted is the IP traffic between the target of the interception and other parties and the only entity of the IPCablecom architecture of relevance for LI is the CMTS. The CMTS is the point for collecting IRI and CC related information.

The CMTS may provide restricted IRI information and CC information as in the clause 5.3.1, with the following options:

- Duplication of complete traffic owning to one service flow (default option);
- Duplication of a part of the traffic owning to one service flow, defined by additional classifiers.

6 Interception of user signalling

Figure 19 illustrates the required interception activities. This clause covers the interception of user signalling whereas the interception of CC is described in clause 7.



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

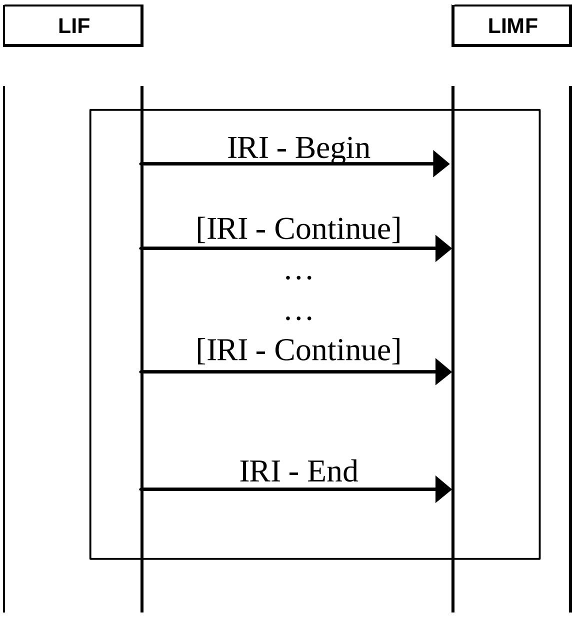
Figure 19: Simplified interception activity diagram

6.1 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 20: IRI protocol sequence chart

The use of each IRI record types is defined by table 2.

Table 2: 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

6.1.1 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.

6.2 Signal sets and interception

All signals in an IPCablecom environment can be classified using set theory as below (see also figure 21):

$$anySignal \in \{AllSignals\}$$

$$\{TransactionSignals\} \subset \{AllSignals\}$$

$$\{BeginSignals\} \subset \{TransactionSignals\}$$

$$\{EndSignals\} \subset \{TransactionSignals\}$$

$$\{ContinueSignals\} \subset \{TransactionSignals\}$$

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".

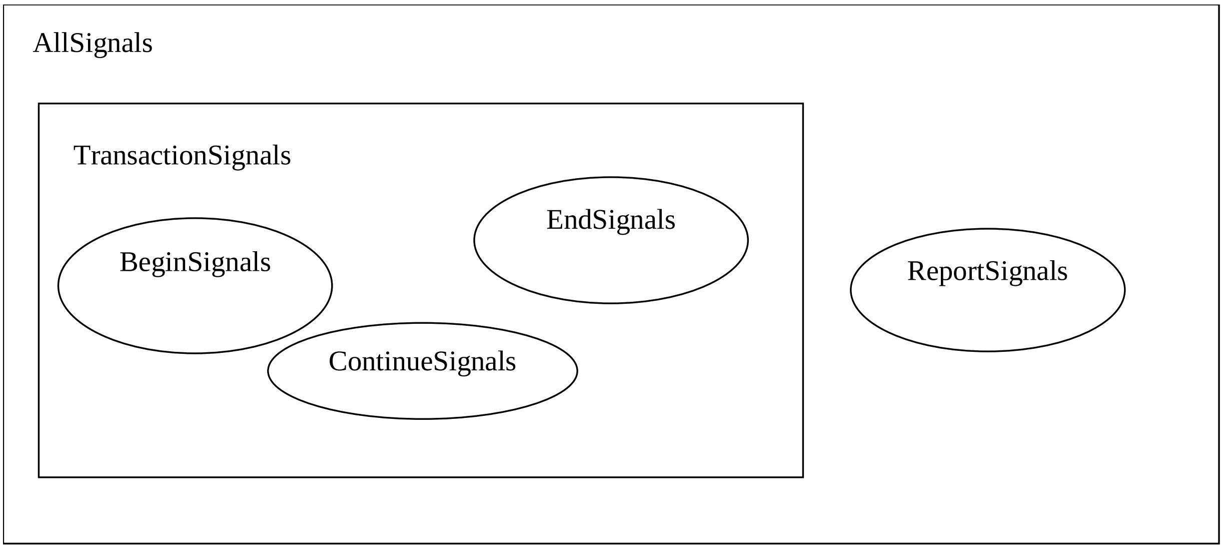


Figure 21: Venn diagram showing signal sets

Annex E of classifies common signalling protocols used in the IPCablecom environment using the above model.

6.3 Location of LI functions

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

- The Application Manager:
  - Where the AM belongs to the cable operator domain, or outside the operator domain and accessible.

- Policy Server:
  - If the Application Manager does not belong to, or cannot be accessed by, the operator domain.
- Cable Modem Termination System:
  - If the Application Manager does not belong to, or cannot be accessed by, the operator domain.

The CCIF function is always located within the CMTS functional entity.

In the normal case interception the IRIIF is assumed to exist only in the Application manager (see figure 22).

The following three figures illustrate the different possible locations of the IRIIF functional entity.

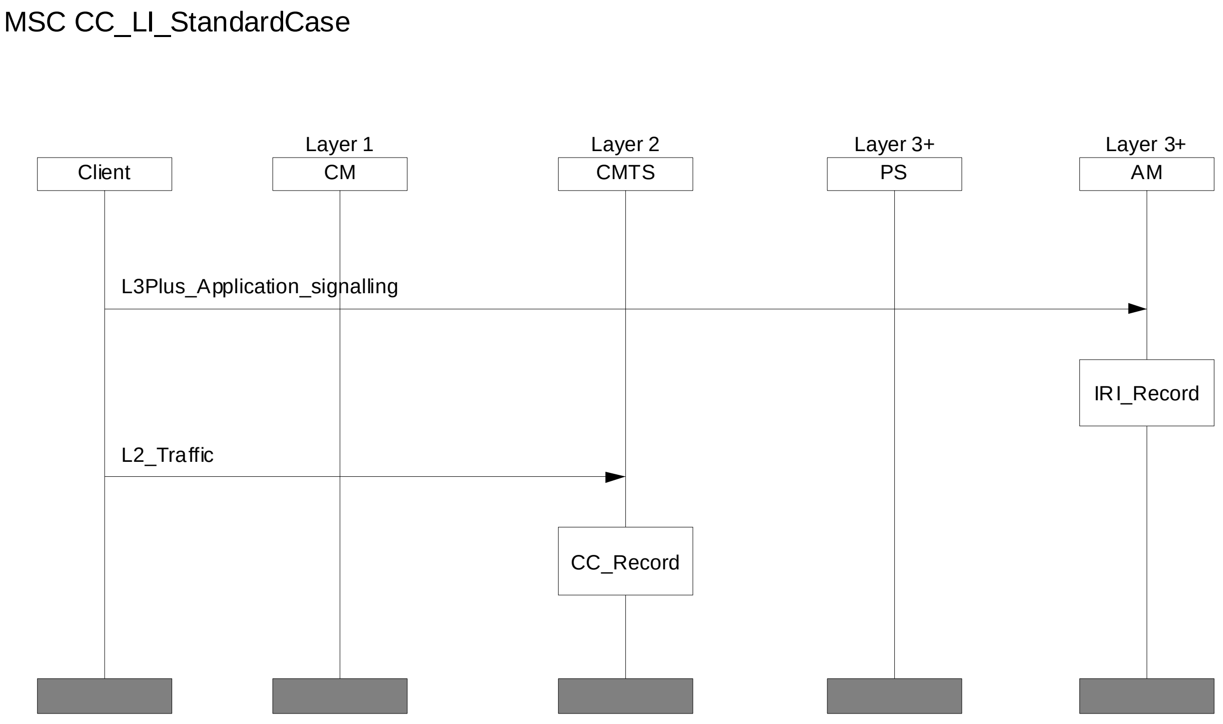


Figure 22: Normal interception model for message sequences

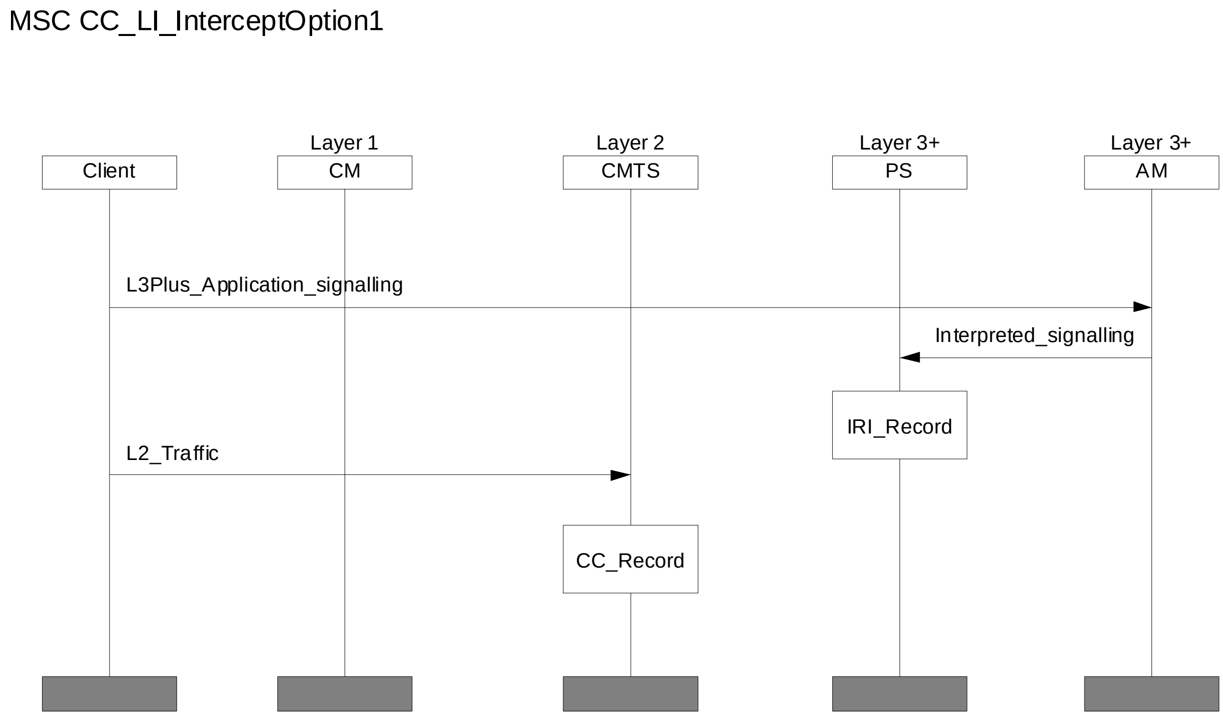


Figure 23: Optional interception model showing PS offering only interpreted signalling (IRI)

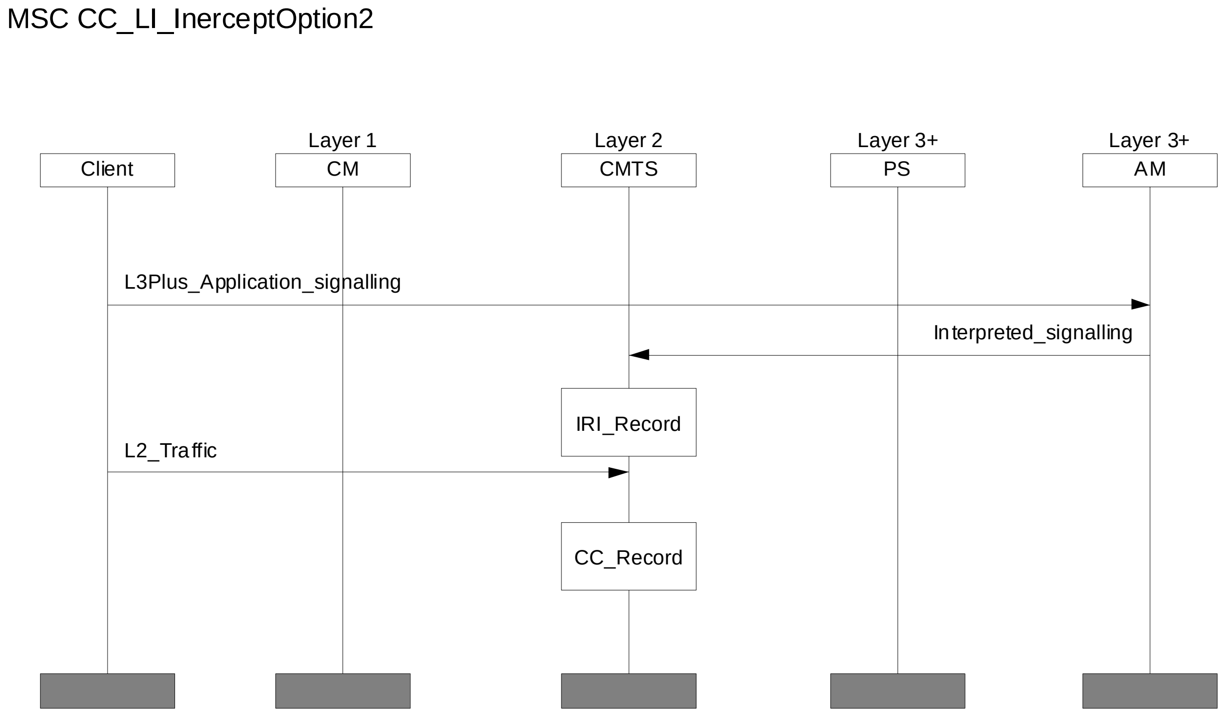


Figure 24: Optional interception model showing CMTS offering only interpreted signalling (IRI)

6.4 Interception of specific signalling

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

6.4.1 IRI protocol service model

The IRI protocol model offers a single Service Access Point (SAP) as shown in figure 25 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.

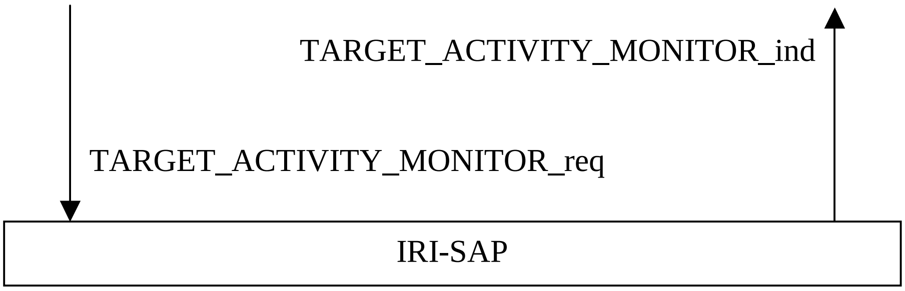


Figure 25: IRI protocol service model

The transmission protocol should employ the security mechanism defined in TS 101 909-11 [4] as pkt-s21 (and/or pkt-s23) as modified by clause 8 of the present document.

6.4.2 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 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
}
```

Protocol constraints:

- Response to = None
- Response expected = None

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

6.4.2.1 Data provision and encoding

6.4.2.1.1 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 specification, the value of this field is 1.

The version number shall be incremented by 1 when new ASN.1 parameters are added or when existing parameters are modified.

6.4.2.1.2 Lawful Interception (LI) 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 -

6.4.2.1.3 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).

6.4.2.1.4 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))
}
```

6.4.2.1.5 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
}
```

6.4.2.1.6 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
}
```

6.4.2.1.7 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.

The IRI transaction number allows for correlation of the IRI and the CC as the same IRI transaction number is used in the CC packets to allow for correlation of the IRI (intercepted signalling) and CC packets (intercepted traffic related to the signalling).

6.4.2.1.8 User signal

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

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

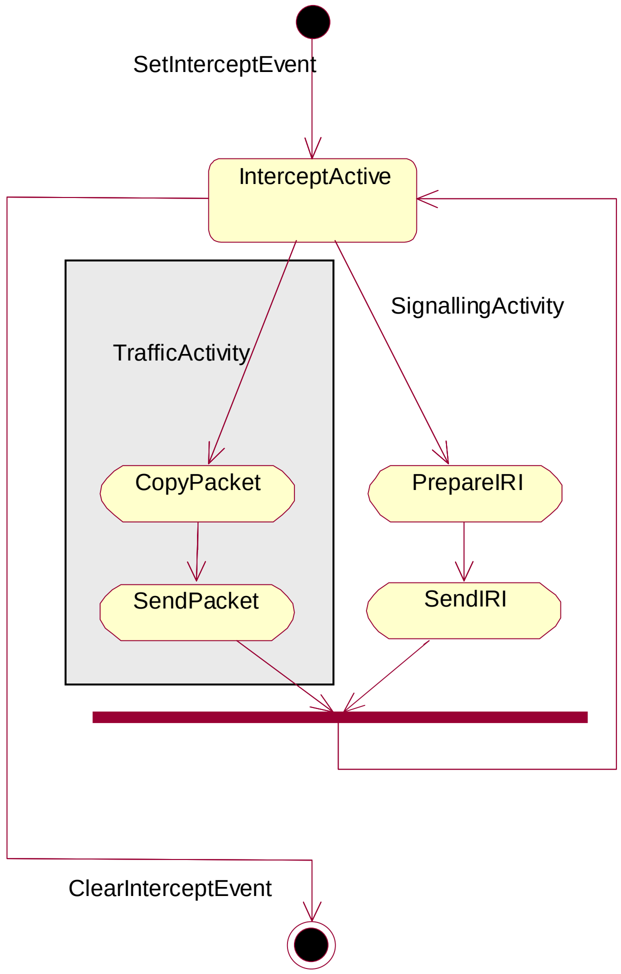
For signalling systems that are text based, e.g. SIP, the use of the PrintableString datatype is recommended.

6.4.2.1.9 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.

7 Interception of Content of Communication (CC)

Figure 26 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 6.



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

Figure 26: Simplified interception activity diagram

7.1 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.

7.1.1 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.

7.1.2 CC protocol service model

The CC protocol model offers a single Service Access Point (SAP) as shown in figure 27 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.

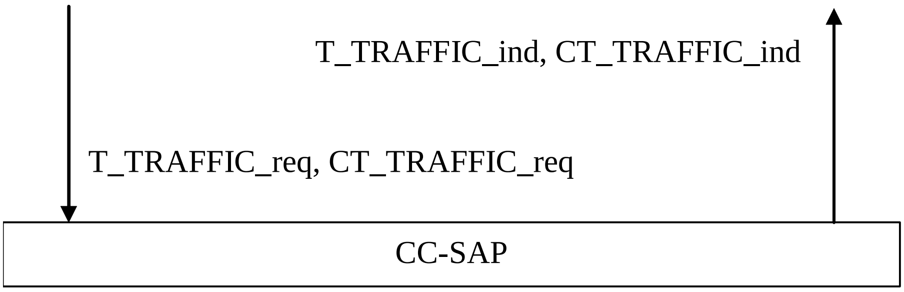


Figure 27: CC protocol service model

The transmission protocol should employ the security mechanism defined in TS 101 909-11 [4] as pkt-s22 or as modified by clause 8.

7.1.2.1 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.

7.1.2.2 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.

7.1.2.3 Data provision and encoding

7.1.2.3.1 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 specification, the value of this field is 1.

The version number shall be incremented by 1 when new ASN.1 parameters are added or when existing parameters are modified.

7.1.2.3.2 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.

The same value of the LIIDType is used for the corresponding IRI, see clause 6.4.2.1.2.

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

7.1.2.3.3 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".

7.1.2.3.4 IRI transaction number

Along with the Lawful Interception (LI) 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 defined in clause 6.2 of TS 101 671 [9].

7.1.2.3.5 Traffic packet

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

7.1.2.3.6 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.

8 Security

8.1 General

The transmission of intercept related material, IRI and CC, shall employ the security mechanisms defined in TS 101 909-11 [4] with the following restriction:

- In table 2 of TS 101 909-11 [4] "IPSec ESP transform identifiers" ESP_NULL shall not be supported when using IPsec for IRI or CC transfer.

Where the LIMF is external to the IPCablecom NWO domain ESP tunnel mode should be supported between CCIF and LIMF, and between IRIIF and LIMF. Where intercepted material is required for evidential purposes ESP tunnel mode should be employed between the IRIIF and LEMF and between CCIF and LEMF.

8.2 Security requirements

ES 201 158 [8] clause 8 requires that the operation of interception facilities should be discreet, confidential and efficient. This is further elaborated as follows:

- Only specifically authorized personnel should be able to control interception.
- The LEA should not have access to any network element.
- The entire communication between the administration system and the interception function should be confidential.
- Interfaces between internal systems which permit automatic administration of intercepting measures should be protected.
- Internal system interfaces should support mutual authentication of the communicating entities and confidentiality of content.

There is an underlying requirement to physically segregate and protect equipment used to control and implement interception measures.

8.3 Interface INI1

This interface is not standardized but in order to comply with the requirements stated above should support the following security services:

- source authentication;
- message integrity;
- content confidentiality.

Source authentication ensures that LI requests are only made by authorized parties. Integrity guarantees that sent messages are not modified on the transmission path and confidentiality does not let unauthorized third parties know what kind of actions and on which identities are carried out.

In general the interface shall implement the same security mechanisms as defined for the other interfaces in IPCablecom.

8.4 Interfaces to the DF

8.4.1 Security services

This clause deals with both interface INI2 and interface INI3. The description here is based on the functional architecture rather than the LI architecture to visualize the security interdependencies. Interfaces between the entities conveying INI1 information are not included here.

Figure 28 illustrates the interfaces between the LI functions and the DF and the kind of information that is exchanged. IRI and CC are conveyed in `Target_Activity_Monitor` messages. The interfaces between AM-PS, and between PS-CMTS are not relevant in regard to INI2 and INI3.

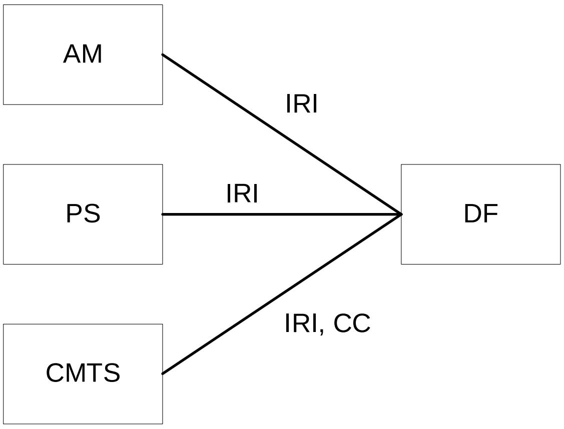


Figure 28: Interfaces invoked in LI

The following clauses describe the required security services for the individual interfaces in more detail.

8.4.1.1 Interface AM-DF

The AM is the central administration entity of many possible scenarios. Since it is the controlling entity on the application layer it is able to deliver a lot of information about the sessions of the targets to intercept. Therefore it is well suited to deliver call related information.

Required security services for this interface are:

- Source authentication;
- Message integrity;
- Confidentiality.

8.4.1.2 Interface PS-DF

The PS is the central functional entity for layer 2 related QoS signalling. It may be especially important in case of the AM being located in a domain different from the domain of the NWO.

Required security services for this interface are:

- Source authentication;
- Message integrity;
- Confidentiality.

8.4.1.3 Interface CMTS-DF

The CMTS is the entity where all IP traffic originated by the target has to pass. It is therefore the entity that intercepts CC and delivers it to the DF. In addition, if the IPCablecom system is not also the service provider for the application used by the provider, the CMTS may also deliver IRI information.

Note, that there may be two connections to secure, one for the IRI and one for the CC.

Required security services for this interface are:

- Source authentication;
- Message integrity;
- Confidentiality.

Confidentiality is optional since the CC may already be encrypted and the required key be delivered to the LEA by means out of the scope of the present document.

8.4.2 Security mechanisms

Table 3 lists the security mechanisms that are based on the ITU-T Recommendation J.179 [12], clause 8 to provide the required security services.

Table 3: Security mechanisms of the IPCablecom multimedia architecture

AM - PS	IPsec using IKE or Kerberos-based key management
PS - CMTS	IPsec using IKE or Kerberos-based key management
AM-DF (IRI)	IPsec using IKE or Kerberos-based key management
PS-DF (IRI)	IPsec using IKE or Kerberos-based key management
CMTS-DF (IRI)	IPsec using IKE or Kerberos-based key management
CMTS-DF (CC)	IPsec using IKE or Kerberos-based key management

8.5 End-to-End security

Where client-based end-to-end encryption is used the IPCablecom/TSP is not able to provide an en-clair copy of the transmitted data, and is not able to provide the corresponding keys to the LEA.

8.6 Use of IPSec to secure intercepted content (INI3)

IPSec may be used to protect intercepted data from eavesdropping and from manipulation. Appropriate key management techniques may provide source authentication, and/or restrict receipt to specified parties.

Annex A (normative): ASN.1 Module

The data definitions for lawful interception 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 [13], and follow the Basic Encoding Rules (BER) defined in ITU-T Recommendation X.690 [14].

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: 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.

```
TS101909202 {itu-t (0) identified-organization (4) etsi (0) ts101909 (1909) part20 (20) subpart2(2)
interceptVersion (0)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN
```

```
TARGETACTIVITYMONITOR ::= 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,
  copyCharSignal  PrintableString,
  interpretedSignal INTEGER  -- Place holder
}
```

```
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 flows on INI1

This annex describes the requirements for interface INI1. It introduces the required information flows as well as the required data for both the IRIIF and the CCIF. For the purpose of simplification of the diagrams IRIIF and CCIF are both called Lawful Interception Function (LIF) in this clause.

It is not the intention of this annex 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 a LIF. The means of transport may be UDP, TCP or embedded in an application protocol such as SNMP or COPS.

B.1 Activation of LI

Clause 5.2.4 shows a list of data available at the LIAF. This information has to be conveyed to the LIF for the activation of the LI.

The information passed from the LIAF to the LIF 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, CC;
- Credentials to fulfil the security service requirements for the delivery to the DF.

Figure B.1 illustrates the information flow for the activation of LI. Depending on the architecture that implements this flow the LIF may be either the AM, PS or CMTS. The number of concurrent LI activations in one message is an implementation issue and may or may not be allowed by the chosen protocol. However, the activation of an entered LI at the HI1 shall be forwarded to the LI functions immediately on reception.

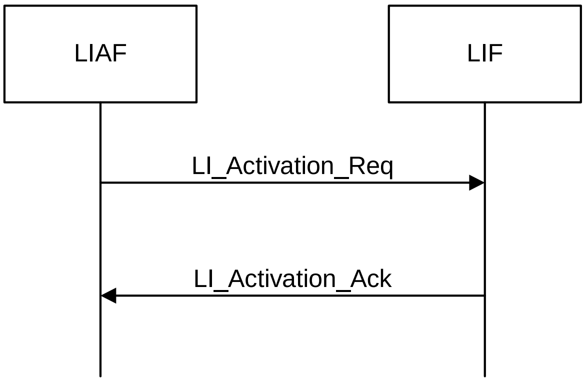


Figure B.1: Information flow for the activation of LI

Table B.1 lists the parameters of the message `LI_Activation_Req.` For a detailed break-down of all parameters please see annex A, the ASN.1 encoding.

Table B.1: Message LI_Activation_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
TargetAddress	M	Application level address of the target to intercept; may be a telephone number
TargetName	O	Name of the target
AdditionalTargetData	O	Additional information about the target
MonitorServiceList	M	A List of services to intercept
LIMFIRIAddress	O	Transport address of the LIMF to send intercepted IRI data to; be negotiated on the fly
LIMFCCAddress	O	Transport address of the LIMF to send intercepted CC data to; be negotiated on the fly
LIParameterList	O	List of additional parameters like traffic filters

Table B.2 illustrates the answer of the LIF, message `LI_Activation_Ack.`

Table B.2: Message LI_Activation_Ack

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
LiTapMediationContentID	O	Identifier for the connection to the LIMF set by the CMTS
LiTapStreamIndex	O	Identifier for the stream set by the CMTS
ActivationError	O	The kind of error if the activation operation failed

B.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 B.2. The message to acknowledge the request contains the positive or negative result of the processed request.

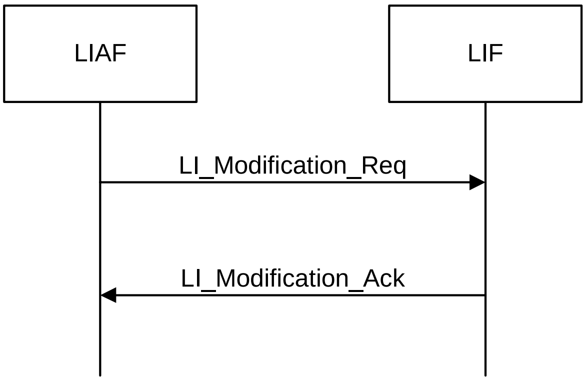


Figure B.2: Information flow for the modification of an LI activity

Table B.3 lists the parameters of the message `LI_Modification_Req.`

Table B.3: Message LI_Modification_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
LiTapMediationEntry	O	It contains the required parameters for a session between the LIMF and a LIF
LiTapStreamEntry	O	It allows the definition of a particular stream to be used for the interception
LiptapStreamEntry	O	It specifies an IP traffic filter for the stream
Li802tapStreamEntry	O	It specifies a MAC traffic filter for the stream

Table B.4 illustrates the answer of the LIF, message `LI_Modification_Ack.`

Table B.4: Message LI_Modification_Ack

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
LiTapMediationContentID	O	Identifier for the connection to the LIMF set by the CMTS
LiTapStreamIndex	O	Identifier for the stream set by the CMTS
ModificationError	O	The kind of error if the modification operation failed

B.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 B.3.

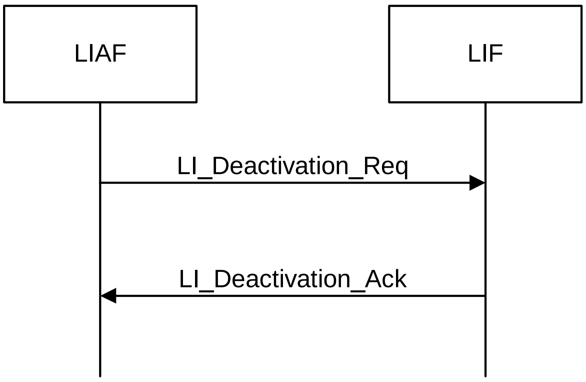


Figure B.3: Information flow for the deactivation of an LI activity

Table B.5 lists the parameters of the message `LI_Deactivation_Req.`

Table B.5: Message LI_Deactivation_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
DeactivateServiceList	M	It specifies the services for which interception shall be ceased

Table B.6 illustrates the answer of the LIF, message `LI_Deactivation_Ack.`

Table B.6: Message LI_Deactivation_Ack

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
DeactivationError	O	The kind of error if the deactivation operation failed

B.4 Interrogation of LI

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

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

Figure B.4 demonstrates the corresponding message exchange.

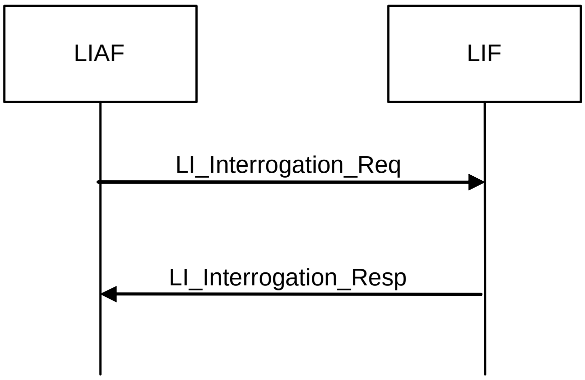


Figure B.4: Information flow for requesting status about an LI activity

Table B.7 lists the parameters of the message `LI_Interrogation_Req.`

Table B.7: Message LI_Interrogation_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
LIInterogateList	M	A list of parameters to be retrieved from the LIF

Table B.8 illustrates the answer of the LIF, message `LI_Interrogation_Resp.`

Table B.8: Message LI_Interrogation_Resp

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
ModificationResult	O	Result of the modification operation
LiTapMediationEntry	O	Describes where intercepted data shall be sent to at the LIMF
DeviceCapabilities	O	Describes the interception capabilities of the LIF
LiptapStreamCapabilities	O	Describes the capabilities for the specification of IP traffic filters
Li802tapStreamCapabilities	O	Describes the capabilities for the specification of MAC traffic filters
LiTapStreamEntry	O	Describes the current stream that is intercepted
LiptapStreamEntry	O	Describes the current IP traffic filters
Li802tapStreamEntry	O	Describes the current MAC traffic filters
InterrogationError	O	The kind of error if the interrogation operation failed

B.5 ASN.1 model of INI1 flows

```
LIACTIVATIONREQ ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    targetAddress       AddressType,
    targetName        VisibleString      OPTIONAL,
    additionalTargetData   VisibleString      OPTIONAL,
    monitorServiceList    SEQUENCE OF ActivityType,
                 -- At least one element may be allServices
    LIMFIRIAddress      LiTapMediationEntry     OPTIONAL,
    LIMFCCAddress       LiTapMediationEntry     OPTIONAL,
    lIParameterList      SEQUENCE
    {
      liTapMediationEntry   LiTapMediationEntry     OPTIONAL,
      liTapStreamEntry     LiTapStreamEntry     OPTIONAL,
      liptapStreamEntry    LiptapStreamEntry     OPTIONAL,
      li802tapStreamEntry   Li802tapStreamEntry     OPTIONAL
    }OPTIONAL
}
```

```
LIACTIVATIONACK ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    liTapMediationContentID  Unsigned32        OPTIONAL,
    liTapStreamIndex     Unsigned32        OPTIONAL,
    activationError      ActivationError     OPTIONAL,
     -- in case of success the error field is omitted!
}
```

```
LIMODIFICATIONREQ ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    liTapMediationEntry    LiTapMediationEntry     OPTIONAL,
    liTapStreamEntry     LiTapStreamEntry     OPTIONAL,
    liptapStreamEntry     LiptapStreamEntry     OPTIONAL,
    li802tapStreamEntry    Li802tapStreamEntry     OPTIONAL
}
```

```
LIMODIFICATIONACK ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    liTapMediationContentID  Unsigned32        OPTIONAL,
    liTapStreamIndex     Unsigned32        OPTIONAL
    modificationError     ModificationError    OPTIONAL
     -- in case of success the error field is omitted!
}
```

```
LIDEACTIVATIONREQ ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    deactivateServiceList   SEQUENCE OF ActivityType
     -- At least one element may be allServices
}
```

```
LIDEACTIVATIONACK ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    deactivationError     DeactivationError    OPTIONAL
     -- in case of success the error field is omitted!
}
```

```
LIINTERROGATIONREQ ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID           INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum      BIT STRING        OPTIONAL,
    lIInterrogateList     InterrogateParameterList
}
```

```
LIINTERROGATIONRESP ::= SEQUENCE
{
    protocolVersion      INTEGER,
    lIID            INTEGER,
    timeStamp         UTCTime,
    cryptoCheckSum       BIT STRING         OPTIONAL,
    lIMediationEntry      LIMediationEntry      OPTIONAL,
    deviceCapabilities     DeviceCapabilities     OPTIONAL,
    liptapStreamCapabilities  LiptapStreamCapabilities  OPTIONAL,
    li802tapStreamCapabilities Li802tapStreamCapabilities OPTIONAL,
    liTapStreamEntry      LiTapStreamEntry      OPTIONAL,
    liptapStreamEntry     LiptapStreamEntry     OPTIONAL,
    li802tapStreamEntry    Li802tapStreamEntry    OPTIONAL,
    interrogationError     InterrogationError     OPTIONAL
     -- in case of success the error field is omitted!
}
```

```
ActivityType ::= ENUMERATED
{
    allServices,
    telephonyVoiceCall,
    unknown,
    cableBroadcast,
    applicationRegistration,
    radiusRequest,
    radiusResponse,
    iPAddressRequest, -- DHCP query
    dNSRequest,
    dNSResponse
}
```

```
ActivationError ::= CHOICE
{
    error          Null,
    ...
}
```

```
ModificationError ::= CHOICE
{
    error          Null,
    ...
}
```

```
DeactivationError ::= CHOICE
{
    error          Null,
    ...
}
```

```
InterrogationError ::= CHOICE
{
    error          Null,
    ...
}
```

```
InterrogateParameterList ::= SEQUENCE
{
    liTapMediationEntry    Boolean,
    deviceCapabilities     Boolean,
    liptapStreamCapabilities  Boolean,
    li802tapStreamCapabilities Boolean,
    liTapStreamEntry      Boolean,
    liptapStreamEntry     Boolean,
    li802tapStreamEntry    Boolean
}
```

```
LiTapMediationEntry::= SEQUENCE
{
    liTapMediationContentID     Unsigned32      OPTIONAL,
     -- A session identifier, from the intercept application's perspective, and a contentID
     -- from the LIF/CCIF perspective; it is set by the intercepting device to avoid the risk
     -- of using the same values for 2 different LIMFEntries'
    liTapMediationDestAddressType  InetAddressType,
    liTapMediationDestAddress    InetAddress,
     -- IP Address of the LIMF network interface to which to direct intercepted traffic.
    liTapMediationDestPort      INTEGER (0..65535),
     -- port number on the LIMF network interface to which to direct intercepted traffic.
    liTapMediationSrcInterface    Unsigned32      OPTIONAL,
     -- interface on the device from which to transmit intercepted data. If zero, any
     -- interface may be used according to normal IP practice
    liTapMediationDscp        INTEGER (0..65535)  OPTIONAL,
     -- Differentiated Services Code Point the intercepting device applies to the IP packets
     -- encapsulating the intercepted traffic.
    liTapMediationTimeout      UTCTime,
     -- time at which this entry and all related Stream information should be automatically
     -- removed, and the intercept function     cease. Since the initiating network manager
     -- may be the only device able to manage a specific intercept or know of its existence,
     -- this acts as a fail-safe for the failure or removal of the network manager. The object
     -- is only effective when the value of LiMediationStatus is 'active'.
    liTapMediationTransport     LiTapMediationTransport
     -- The protocol used in transferring intercepted data to the Mediation Device.
}
```

```
LiTapMediationTransport ::= ENUMERATED
{
    uDP(1), -- IPCablecom udp format
    tCP(2), -- TCP with head of line blocking
    sCTP(3) - SCTP with head of line blocking
}
```

```
DeviceCapabilities ::= ENUMERATED
 -- This object displays the Device capabilities with respect to certain fields in Device table.
 -- This may be dependent on hardware capabilities, software capabilities.
{
    iPV4SrcInterface(0),
     -- SNMP ifIndex Value may be used to select the interface (denoted by
     -- LiMediationSrcInterface) on the intercepting device from which to transmit intercepted
     -- data to an IPv4 address Mediation Device.
    iPV6SrcInterface(1),
     -- SNMP ifIndex Value may be used to select the interface (denoted by
     -- LiMediationSrcInterface) on the intercepting device from which to transmit intercepted
     -- data to an Ipv6 address Mediation Device.
    uDP(2),
     -- UDP may be used as transport protocol (denoted by LiMediationTransport) in transferring
     -- intercepted data to the Mediation Device.
    tCP(3),
     -- TCP may be used as transport protocol (denoted by LiMediationTransport) in transferring
     -- intercepted data to the Mediation Device.
    sCTP(4)
     -- SCTP may be used as transport protocol (denoted by LiMediationTransport) in
     -- transferring intercepted data to the Mediation Device.
}
```

```
LiTapStreamEntry ::= SEQUENCE {
    LiTapMediationContentID     Unsigned32      OPTIONAL,
    liTapStreamIndex         Unsigned32      OPTIONAL,
     -- The index of the stream itself. It is set by the intercepting device to void the risk
     -- of using the same values for 2 different interception streams
    liTapStreamType         ENUMERATED
     -- Identifies the type of intercept filter associated to this generic stream.
    {
      iP (1),
       -- The specific filter is an IP filter with same indices as that of this table.
       -- The exact filter is defined in the corresponding LiptapStreamEntry
      mAC (2)
       -- The specific filter is a MAC with same indices as that of this table.The exact
       -- filter is a row in the corresponding LI802StreamEntry.
    }
}
```

```
LiptapStreamCapabilities ::= ENUMERATED
{
 -- This object displays what types of intercept streams can be configured on this type of device.
 -- This may be dependent on hardware capabilities, software capabilities.
    interface(1),
     -- SNMP ifIndex Value may be used to select interception of all data crossing an interface
     -- or set of interfaces.
    iPV4(2),
     -- IPv4 Address or prefix may be used to select traffic to be intercepted.
    iPV6(3),
     -- Ipv6 Address or prefix may be used to select traffic to be intercepted.
    l4Port(4),
     -- TCP/UDP Ports may be used to select traffic to be intercepted.
    dSCP(5),
     -- DSCP (Differentiated Services Code Point) may be used to select traffic to be
     -- intercepted.
}
```

```
LiptapStreamEntry::= SEQUENCE {
    LiTapMediationContentID      Unsigned32      OPTIONAL,
    liTapStreamIndex          Unsigned32      OPTIONAL,
    liptapStreamInterface       Integer32,
     -- The ifIndex value of the interface over which traffic to be intercepted is received
     -- or transmitted.
    liptapStreamAddrType       InetAddressType,
     -- The type of address, used in packet selection.
    liptapStreamDestinationAddress  InetAddress,
     -- The Destination address or prefix used in packet selection. This address will be of
     -- the type specified in LiptapStreamAddrType.
    liptapStreamDestinationLength   Unsigned32,
     -- The length of the Destination Prefix. A value of zero causes all addresses to match.
     -- This prefix length will be consistent with the type specified in LiptapStreamAddrType.
    liptapStreamSourceAddress     InetAddress,
     -- The Source Address used in packet selection. This address will be of the type specified
     -- in LiptapStreamAddrType
    liptapStreamSourceLength     Unsigned32,
     -- The length of the Source Prefix. A value of zero causes all addresses to match. This
     -- prefix length will be consistent with the type specified in LiptapStreamAddrType.
    liptapStreamTosByte        Integer32,
     -- The value of the TOS byte, when masked with LiptapStreamTosByteMask, of traffic to be
     -- intercepted.
    liptapStreamTosByteMask      Integer32,
     -- The value of the TOS byte in an IPv4 or IPv6 header is ANDed with LiptapStreamTosByteMask
     -- and compared with LiptapStreamTosByte. If the values are equal, the comparison is equal.
     -- If the mask is zero and the TosByte value is zero, the result is to always accept.
    liptapStreamFlowId        Integer32,
     -- The flow identifier in an IPv6 header. -1 indicates that the Flow Id is unused.
    liptapStreamProtocol       Integer32,
     -- The IP protocol to match against the IPv4 protocol number or
     -- the IPv6 Next- Header number in the packet. -1 means 'any IP protocol'.
    liptapStreamDestL4PortMin     INTEGER (0..65535),
     -- The minimum value that the layer-4 destination port number in the packet must have in
     -- order to match. This value must be equal to or less than the value specified for this
     -- entry in LiptapStreamDestL4PortMax.
    liptapStreamDestL4PortMax     INTEGER (0..65535),
     -- The maximum value that the layer-4 destination port number in the packet must have in
     -- order to match this classifier entry. This value must be equal to or greater than the
     -- value specified for this entry in LiptapStreamDestL4PortMin.
     -- If both LiptapStreamDestL4PortMin and LiptapStreamDestL4PortMax are at their default
     -- values, the port number is effectively unused.
    liptapStreamSourceL4PortMin    INTEGER (0..65535),
     -- The minimum value that the layer-4 destination port number in the packet must have in
     -- order to match. This value must be equal to or less than the value specified for this
     -- entry in LiptapStreamSourceL4PortMax.
     -- If both LiptapStreamSourceL4PortMin and LiptapStreamSourceL4PortMax are at their default
     -- values, the port number is effectively unused."
    liptapStreamSourceL4PortMax    INTEGER (0..65535),
     -- The maximum value that the layer-4 destination port number in the packet must have in
     -- order to match this classifier entry. This value must be equal to or greater than the
     -- value specified for this entry in LiptapStreamSourceL4PortMin.
     -- If both LiptapStreamSourceL4PortMin and LiptapStreamSourceL4PortMax are at their default
     -- values, the port number is effectively unused.
}
```

```
Li802tapStreamCapabilities ::= ENUMERATED
 -- This object displays what types of intercept streams can be configured on this type of device.
 -- This may be dependent on hardware capabilities, software capabilities.
{
    interface (1),
     -- SNMP ifIndex Value may be used to select interception of all data crossing an interface
     -- or set of interfaces.
    dstMacAddr (2),
     -- Destination MAC Address may be used to select traffic to be intercepted.
    srcMacAddr (3),
     -- Source MAC Address may be used to select traffic to be intercepted.
    ethernetPid (4),
     -- Ethernet Protocol Identifier may be used to select traffic to be intercepted.
    dstLlcSap (5),
     -- IEEE 802.2 Destination SAP may be used to select traffic to be intercepted.
    srcLlcSap (6)
     -- IEEE 802.2 Source SAP may be used to select traffic to be intercepted."
}
```

```
Li802tapStreamEntry ::= SEQUENCE
{
    liTapMediationContentID       Unsigned32      OPTIONAL,
    liTapStreamIndex          Unsigned32      OPTIONAL,
    li802tapStreamFields        Li802tapStreamFields,
     -- This object displays what attributes must be tested to identify traffic which requires
     -- interception. The packet matches if all flagged fields match.
    li802tapStreamInterface       Integer32,
     -- The ifIndex value of the interface over which traffic to be intercepted is received or
     -- transmitted. The interface may be physical or virtual. If this is the only parameter
     -- specified, and it is other than -1 or 0, all traffic on the selected interface will be
     -- chosen
    li802tapStreamDestinationAddress  OCTET STRING (SIZE (6)), -- MAC Address
     -- The Destination address used in packet selection.
    li802tapStreamSourceAddress     OCTET STRING (SIZE (6)), -- MAC Address
     -- The Source Address used in packet selection.
    li802tapStreamEthernetPid      Unsigned32,
     -- The value of the Ethernet Protocol Identifier, which may be found on Ethernet traffic
     -- or IEEE 802.2 SNAP traffic.
    li802tapStreamSourceLlcSap     Unsigned32,
     -- The value of the IEEE 802.2 Source SAP.
    li802tapStreamDestinationLlcSap   Unsigned32,
     -- The value of the IEEE 802.2 Destination SAP.
}
```

```
Li802tapStreamFields ::= ENUMERATED
{
    interface (1),
     -- indicates that traffic on the stated interface is to be intercepted
    dstMacAddress (2),
     -- indicates that traffic destined to a given address should be intercepted
    srcMacAddress (3),
     -- indicates that traffic sourced from a given address should be intercepted
    ethernetPid (4),
     -- indicates that traffic with a stated Ethernet Protocol Identifier should be intercepted
    dstLlcSap (5),
     -- indicates that traffic with an certain 802.2 LLC Destination SAP should be intercepted
    srcLlcSap (6),
     -- indicates that traffic with an certain 802.2 LLC Source SAP should be intercepted
}
```

```
InetAddress ::= CHOICE
{
    inetAddressIPv4         OCTET STRING (SIZE (4)),
    inetAddressIPv6         OCTET STRING (SIZE(16)),
    inetAddressIPv4z        OCTET STRING (SIZE(8)),
    inetAddressIPv6z        OCTET STRING (SIZE(20)),
    fQDN              OCTET STRING (SIZE(1..255))
     -- Fully Qualified Domain Name
}
```

```
InetAddressType ::= ENUMERATED
{
    iPv4 (1),
    iPv6 (2),
    iPv4z (3),
    iPv6z (4),
    fQDN (5)
     -- Fully Qualified Domain Name
}
```

```
Integer32 ::= INTEGER (-2147483648..2147483647) -- neg and pos values of a 32 bit integer
```

```
Unsigned32 ::= INTEGER (0..4294967295)     -- all positive values of a 32 bit integer
```

B.6 Implementation example for INI1 using SNMPv3 MIBs

B.6.1 Introduction to SNMP

The Simple Network Management Protocol (SNMP) is a suite of protocols that allow remote monitoring and configuration of nodes. The elements of a node that can be managed are defined in a Management Information Base (MIB). The installation of a MIB in a node implies that the node can act on the actions it is asked to undertake.

A MIB defines the management information that is maintained in managed nodes and that is made remotely accessible by management agents. The management protocol itself allows access to management information in essentially two different ways:

- a request-response interaction:
  - used to retrieve or modify management information associated with the managed device.
- an unconfirmed interaction:
  - an agent sends a unsolicited message, termed a trap, to a manager, and no response is returned. This is used to notify a manager of an exceptional situation which has resulted in changes to management information associated with the managed device.

The management interactions defined in the present document closely map to the former mode. The construction of a MIB is defined by RFC 2578 [15]. MIBs are defined using a subset of ASN.1 and in particular introduces a set of ASN.1 macros to define objects that are managed, which themselves may contain elements defined in normal ASN.1 syntax.

NOTE: ASN.1 syntax checking tools do not recognize macros which have been deprecated in ASN.1.

An unconfirmed interaction may be used to send an IRI-Record whenever a watched for condition arises. The filtering profile used to establish the watched for condition is examined more in the succeeding clauses of this annex.

B.6.2 LI MIB description

The purpose of this clause is to outline the structure of a MIB used in the context of LI. The MIB described implements the requirements established in clauses B.1 to B.4.

NOTE: The MIB is provided as an electronic attachment to the present document.

The LI MIB is structured in such a way that it can be extended. At the core is ETSILI-TAP-MIB, a generic interception MIB, which describes interception context, and defines generic streams to intercept. This MIB can be extended and 2 such extensions are defined:

- ETSILI-IP-TAP-MIB; and
- ETSILI-802-TAP-MIB.

These are extension to ETSILI-TAP-MIB and allow to set specialized IP filters, and layer 2 filters respectively for the intercepted streams.

Within the MIB themselves are a number of data structures that may allow an implementation of the information flows described in B.1 to B.4.

- **LiTapMediationTable** in ETSILI-TAP-MIB lists the Mediation devices with which the LIF communicates:
  - **LiTapMediationEntry** in ETSILI-TAP-MIB allows to set-up an interception context and define its parameters (LIMF credentials, LIF interface, transport protocol etc.); liTapMediationContentID is set uniquely by the LIF and acts as the interception context identifier.
  - **LiTapStreamEntry** in ETSILI-TAP-MIB is used to set-up an interception stream. **LiTapStreamEntry** is indexed by **liTapMediationContentID** and therefore is correlated to the interception context. **liTapStreamID** is set by the LIF and provides a unique identifier for the stream.

Once the contexts and streams are setup, IP or 802 filters can be defined in ETSILI-IP-TAP-MIB and ETSILI-802-TAP-MIB respectively:

- **LiptapStreamEntry** is used to define a set of layer 3 and layer 4 filters;
- **Li802tapStreamEntry** is used to define a set of layer 2 filters.

The specific device and filtering capabilities are addressed by the following:

- **LiTapMediationCapabilities** (in ETSILI-TAP-MIB) defines the LIF capabilities with respect to some fields of **LiMediationEntry**, and include interfaces and transport protocols;
- **LiptapStreamCapabilities** and **Li802tapStreamCapabilities** (in the extension MIBs) display what type of Layer 3 to 4 and Layer 2 intercept streams can be configured on the LIF respectively.

B.6.3 Provisioning Intercepts through SNMPv3

This annex demonstrates an intercept provisioning mechanism of using SNMPv3. It uses IP intercept as an example of specific type of intercept.

B.6.3.1 Creation of an MD Entry

As an example of creation of a Mediation Device entry for lawful interception the interception parameters listed below are used:

- CCCid = 1
- TTl = up to 27 February 2004 00:00:00[hh:mm:ss]
- MD IP Address = 11.0.0.1
- MD UDP port = 2000
- DSCP value = af41

The parameter liTapMediationTimeout corresponds to the Time To Live (TTl) above.

The parameter liTapMediationDestAddress corresponds to the MD IP address above.

The parameter liTapMediationDestPort corresponds to the MD UDP port above.

B.6.3.1.1 Use of "CreateAndWait" Method.

```
setany -v3 10.76.37.24 user1 liTapMediationStatus.1 -i 5
setany -v3 10.76.37.24 user1 liTapMediationDestAddressType.1 -i 1
setany -v3 10.76.37.24 user1 liTapMediationTimeout.1 -o "07 d4 2 1b 00 00 00 00"
setany -v3 10.76.37.24 user1 liTapMediationTransport.1 -i 1
setany -v3 10.76.37.24 user1 liTapMediationSrcInterface.1 -i 0
setany -v3 10.76.37.24 user1 liTapMediationDestAddress.1 -o "b 0 0 1"
setany -v3 10.76.37.24 user1 liTapMediationDestPort.1 -g 2000
setany -v3 10.76.37.24 user1 liTapMediationStatus.1 -i 1
```

B.6.3.1.2 Use of "CreateAndGo" Method.

```
setany -v3 10.76.37.24 user1 \
liTapMediationDestAddressType.1 -i 1 \
liTapMediationDestAddress.1 -o "b 0 0 1"  \
liTapMediationDestPort.1 -g 2000 \
liTapMediationSrcInterface.1 -i 0 \
liTapMediationTimeout.1 -o "07 d4 2 1b 00 00 00 00" \
liTapMediationTransport.1 -i 1 \
liTapMediationStatus.1 -i 4
```

B.6.3.2 Creation of a stream entry

A specific stream and associated specific stream are related together by having the same index -<CCCid, stream index>.

In the following examples, IP intercept is used as a specific stream to be provisioned.

B.6.3.2.1 Provision of generic stream

Create this generic stream with stream Index 2 using "CreateAndWait" Method.

```
setany -v3 10.76.37.24 user1 liTapStreamStatus.1.2 -i 5
setany -v3 10.76.37.24 user1 liTapStreamType.1.2 -i 1
setany -v3 10.76.37.24 user1 liTapStreamInterceptEnable.1.2 -i 2
setany -v3 10.76.37.24 user1 liTapStreamStatus.1.2 -i 1
```

Create this generic stream with stream Index 2 using "CreateAndGo" Method.

```
setany -v3 10.76.37.24 user1 \
liTapStreamType.1.2 -i 1 \
liTapStreamInterceptEnable.1.2 -i 2 \
liTapStreamStatus.1.2 -i 4
```

The SNMP code samples that follow establish an interception capability all IPv4 packets meeting following criteria and send it to MD with CCCid 1:

• source Machine:	60.0.0.1
• Source port range:	0 - 65535
• Destination Machine:	90.0.0.1
• Destination port range:	0 - 65535
• Protocol:	All Protocols

An interception filter is crated using the "CreateAndWait" Method as follows:

```
setany -v3 10.76.37.24 user1 liptapStreamStatus.1.2 -i 5
setany -v3 10.76.37.24 user1 liptapStreamAddrType.1.2 -i 1
setany -v3 10.76.37.24 user1 liptapStreamInterface.1.2 -i -1
setany -v3 10.76.37.24 user1 liptapStreamDestinationAddress.1.2 -o "5a 0 0 1"
setany -v3 10.76.37.24 user1 liptapStreamSourceAddress.1.2 -o "3c 0 0 1"
setany -v3 10.76.37.24 user1 liptapStreamDestinationLength.1.2 -g 32
setany -v3 10.76.37.24 user1 liptapStreamSourceLength.1.2 -g 32
setany -v3 10.76.37.24 user1 liptapStreamProtocol.1.2 -i -1
setany -v3 10.76.37.24 user1 liptapStreamDestL4PortMin.1.2 -g 0
setany -v3 10.76.37.24 user1 liptapStreamDestL4PortMax.1.2 -g 65535
setany -v3 10.76.37.24 user1 liptapStreamSourceL4PortMin.1.2 -g 0
setany -v3 10.76.37.24 user1 liptapStreamSourceL4PortMax.1.2 -g 65535
setany -v3 10.76.37.24 user1 liptapStreamStatus.1.2 -i 1
```

Alternatively the same intercept can be created using "CreateAndGo" Method.

```
setany -v3 10.76.37.24 user1 \
liptapStreamAddrType.1.2 -i 1 \
liptapStreamInterface.1.2 -i -1 \
liptapStreamDestinationAddress.1.2 -o "5a 0 0 1" \
liptapStreamSourceAddress.1.2 -o "3c 0 0 1" \
liptapStreamDestinationLength.1.2 -g 32 \
liptapStreamSourceLength.1.2 -g 32 \
liptapStreamProtocol.1.2 -i -1 \
liptapStreamDestL4PortMin.1.2 -g 0 \
liptapStreamDestL4PortMax.1.2 -g 65535 \
liptapStreamSourceL4PortMin.1.2 -g 0 \
liptapStreamSourceL4PortMax.1.2 -g 65535 \
liptapStreamStatus.1.2 -i 4
```

After creating the specific stream, the generic stream can be enabled by setting its interceptEnable flag to TRUE, as follows.

```
setany -v3 10.76.37.24 user1 liTapStreamInterceptEnable.1.2 -i 1
```

B.7 Implementation example for INI1 using COPS

B.7.1 COPS gate control object for LI

The gate control object illustrated in table B.9 extends the defined one from clause 7.3.2.10 of TS 101 909-5 [3] by the LI-Identifier.

Table B.9: COPS Gate Control Object for LI Parameters

Length = 24	S-Num = 10	S-Type = 1
DF-IP-Address-for-IRI (32 bits)		
DF-Port-for-IRI (16 bits)	Flags	
DF-IP-Address-for-CC (32 bits)		
DF-Port-for-CC (16 bits)	Reserved	
LI-Identifier (32 bits)		

All parameters of the LI Gate Control Object except the field `LI-Identifier` are described in clause 7.3.2.10 of TS 101 909-5 [3].

LI-Identifier is included to correlate the intercepted content packets with the interception case. It is not required if separate `DF-Port-for-CC` values are used for individual sessions. In that case the correlation is done via the port.

B.7.2 LI Requirements for the CMTS

In case of an interception a PS shall include the COPS LI gate control object in a Gate-Set message. Furthermore, the flags `DUP-EVENT` and `DUP-CONTENT` flags shall be set, and the LIMF's IP address and port tuple for IRI and CC shall be filled.

When a session is not subject to an interception the COPS LI gate control object shall not be included in a Gate-Set message.

On the reception of a Gate-Info request the CMTS shall, if LI is performed on the Gate in question and if appropriate, include the LI gate control object in the returned Gate-Info-Ack message.

Annex C (informative): Handover of intercepted material

C.1 Overview

The general model of handover is shown in figure C.1. On receipt of an IRI, in the form of an X2Message() in the sequence diagram of figure C.1, at the LIMF/MF it is sent to the LEMF in an HI2Message().

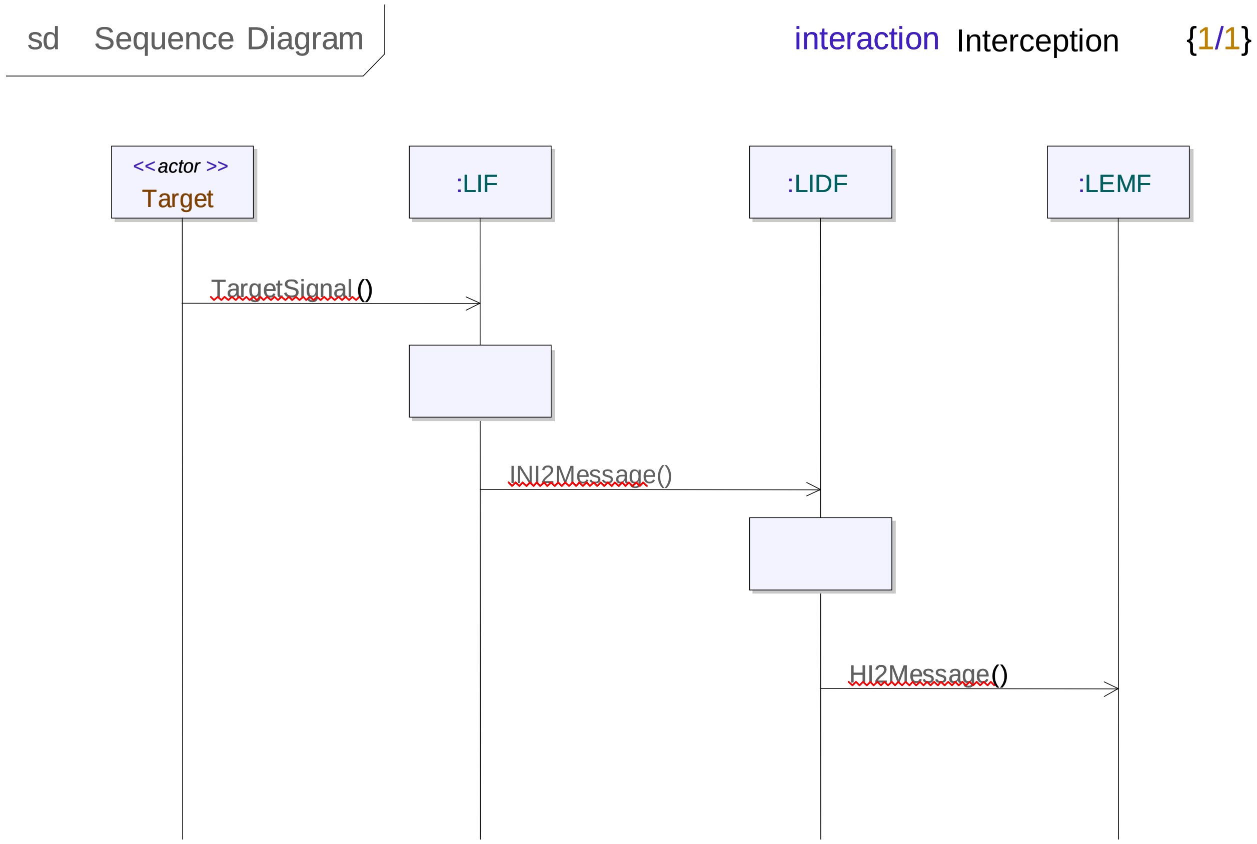


Figure C.1: Sequence chart of interception process

C.2 Mapping to Handover Interface

The internal interfaces INI1, INI2 and INI3 are mapped by a Mediation Device (MD) to the handover interfaces described in TS 101 671 [9] or TS 102 232 [11].

Annex D (informative): SDL Model

The SDL model described in this annex illustrates the interception processes required in a multimedia environment. The model does not restrict where the processes are placed but only serves to summarize their behaviour.

D.1 System model

The SDL model for analysis of LI is based on figure 15 in clause 5.1

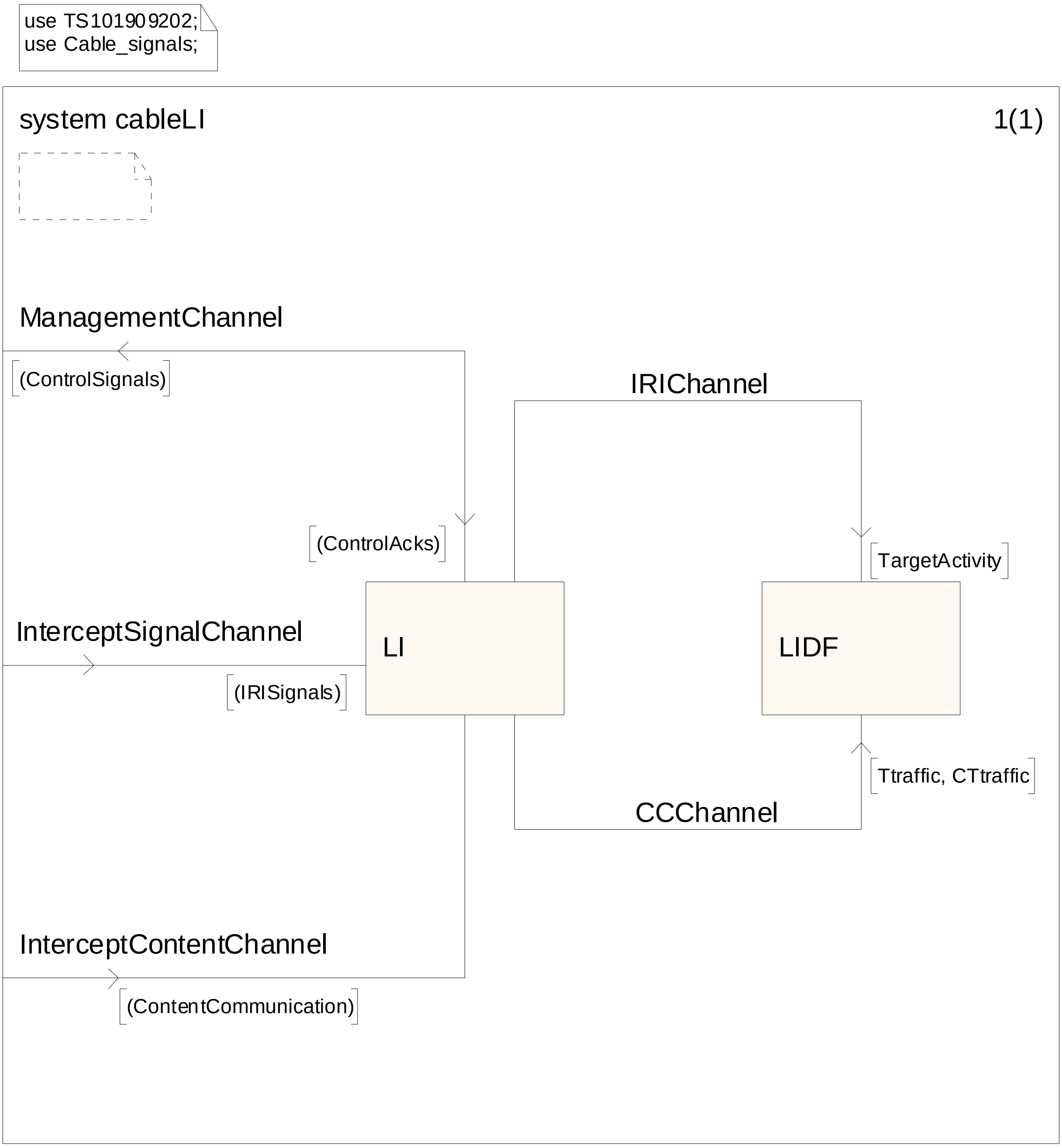


Figure D.1: SDL System diagram for LI

The model is composed of 2 blocks, the first is the main LI unit and contains processes to simulate the functions of LIAF, IRIIF and CCIF. The second block contains stub processes to receive the intercepted material. The environment is the IPCablecom system and is visible through three distinct channels:

- Management:
  - This is a bidirectional channel used to implement the HI1 to INI1 control information and therefore to setup, clear down, and modify the parameters of the interception.
- Intercept Signals:
  - This is a unidirectional channel carrying the target's signalling.
- Intercept Content:
  - This is a unidirectional channel carrying the target's content of communication.

D.2 LI Block definition

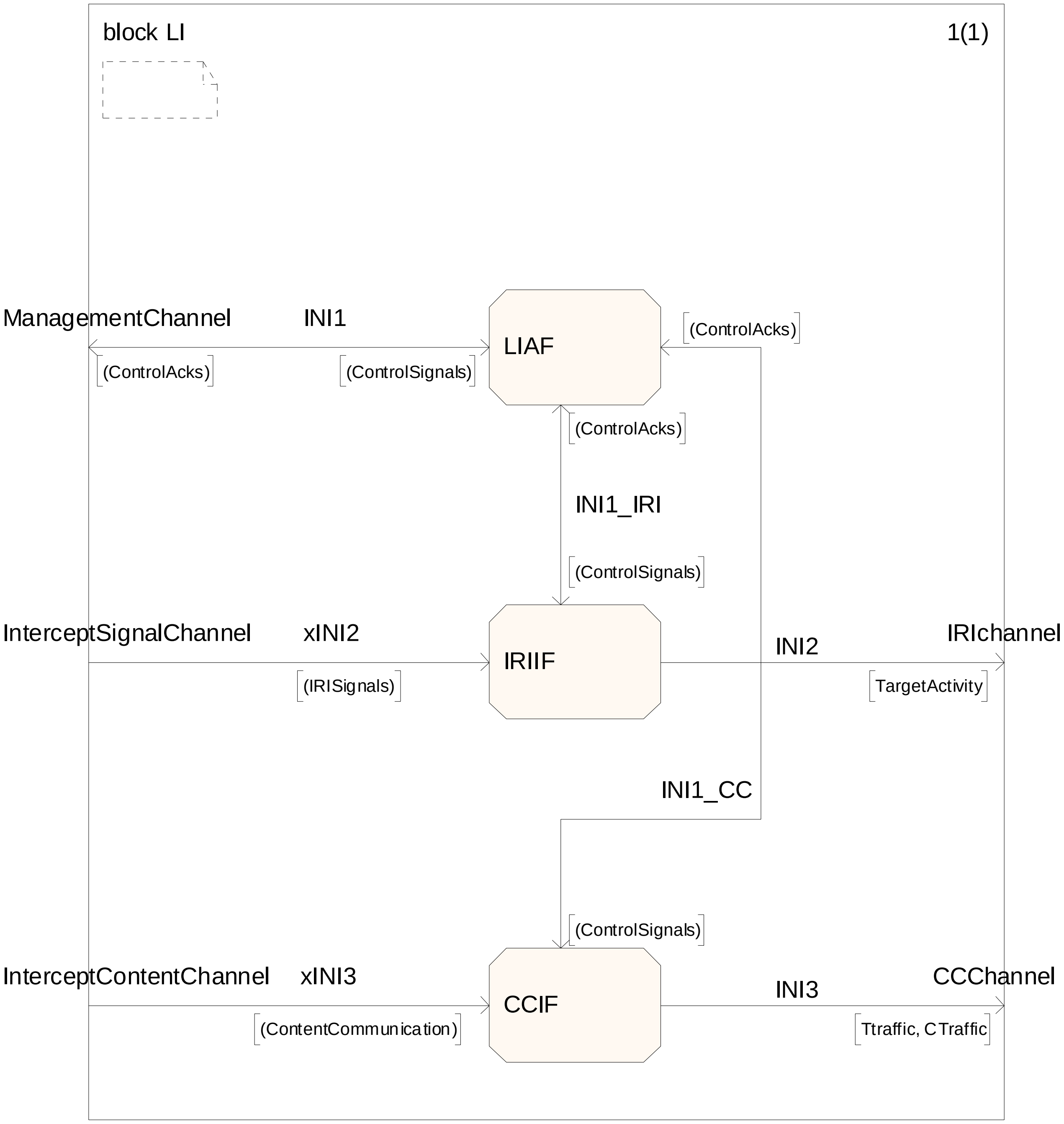
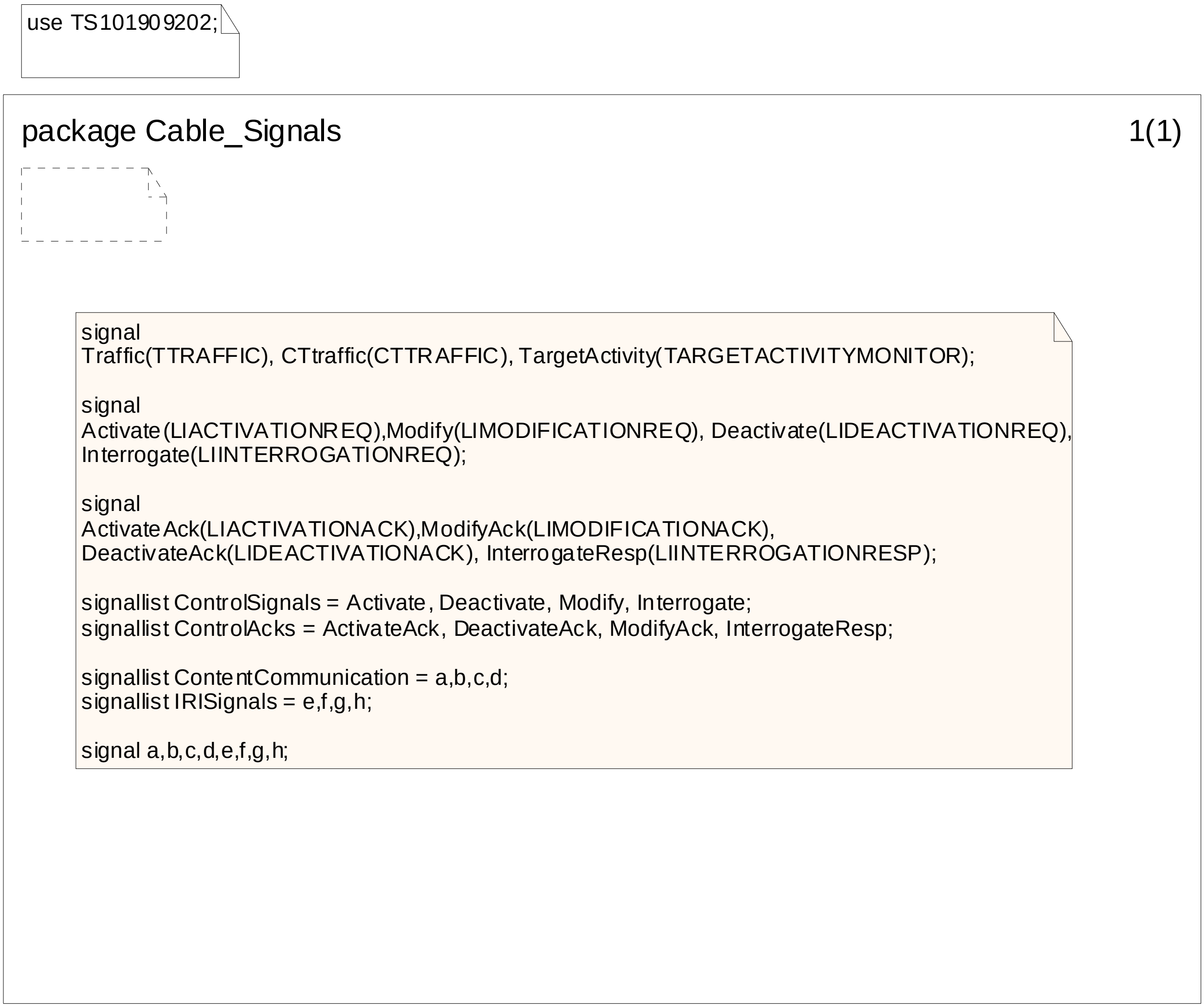


Figure D.2: SDL block structure for LI in Packet Cable Interception

The LI block is expanded to provide three processes for each of the LIAF, CCIF and IRIIF functional elements.

D.3 Signal definitions

The core data definitions used in the SDL model come from the ASN.1 module defined in annex A, augmented for the purpose of the model only by stub definitions of the INI1 data from annex B.



```
use TS101909202;
```

package Cable_Signals 1(1)

```
signal
Traffic(TTRAFFIC), CTtraffic(CTTRAFFIC), TargetActivity(TARGETACTIVITYMONITOR);

signal
Activate(LIACTIVATIONREQ),Modify(LIMODIFICATIONREQ), Deactivate(LIDEACTIVATIONREQ),
Interrogate(LIINTERROGATIONREQ);

signal
ActivateAck(LIACTIVATIONACK),ModifyAck(LIMODIFICATIONACK),
DeactivateAck(LIDEACTIVATIONACK), InterrogateResp(LIINTERROGATIONRESP);

signallist ControlSignals = Activate, Deactivate, Modify, Interrogate;
signallist ControlAcks = ActivateAck, DeactivateAck, ModifyAck, InterrogateResp;

signallist ContentCommunication = a,b,c,d;
signallist IRISignals = e,f,g,h;

signal a,b,c,d,e,f,g,h;
```

NOTE: The ASN.1 module TS 101 909 202 is used.

Figure D.3: Signal definitions for LI in Packet Cable Interception

D.4 Process models

There are 3 processes defined as described in clause 5:

- LIAF:
  - The administration function is modelled to show the main control links sufficient to emulate starting, stopping and extension of the interception.

NOTE: As the behaviour of the LIAF, and of signals in INI1 are only provided for information this entity is not modelled.

- IRIIF:
  - The IRI interception function is modelled to show the essential interpretation of signals, and the setting of data in the IRI record with encapsulation of the signal to the IRI.

- CCIF:
    - The CCIF function is modelled to show the encapsulation of interpreted content to the internal handover point.

D.4.1 IRIIF process model

NOTE: As the behaviour of the LIAF, and of signals in INI1 are only provided for information the interaction of LIAF with IRIIF is not modelled.

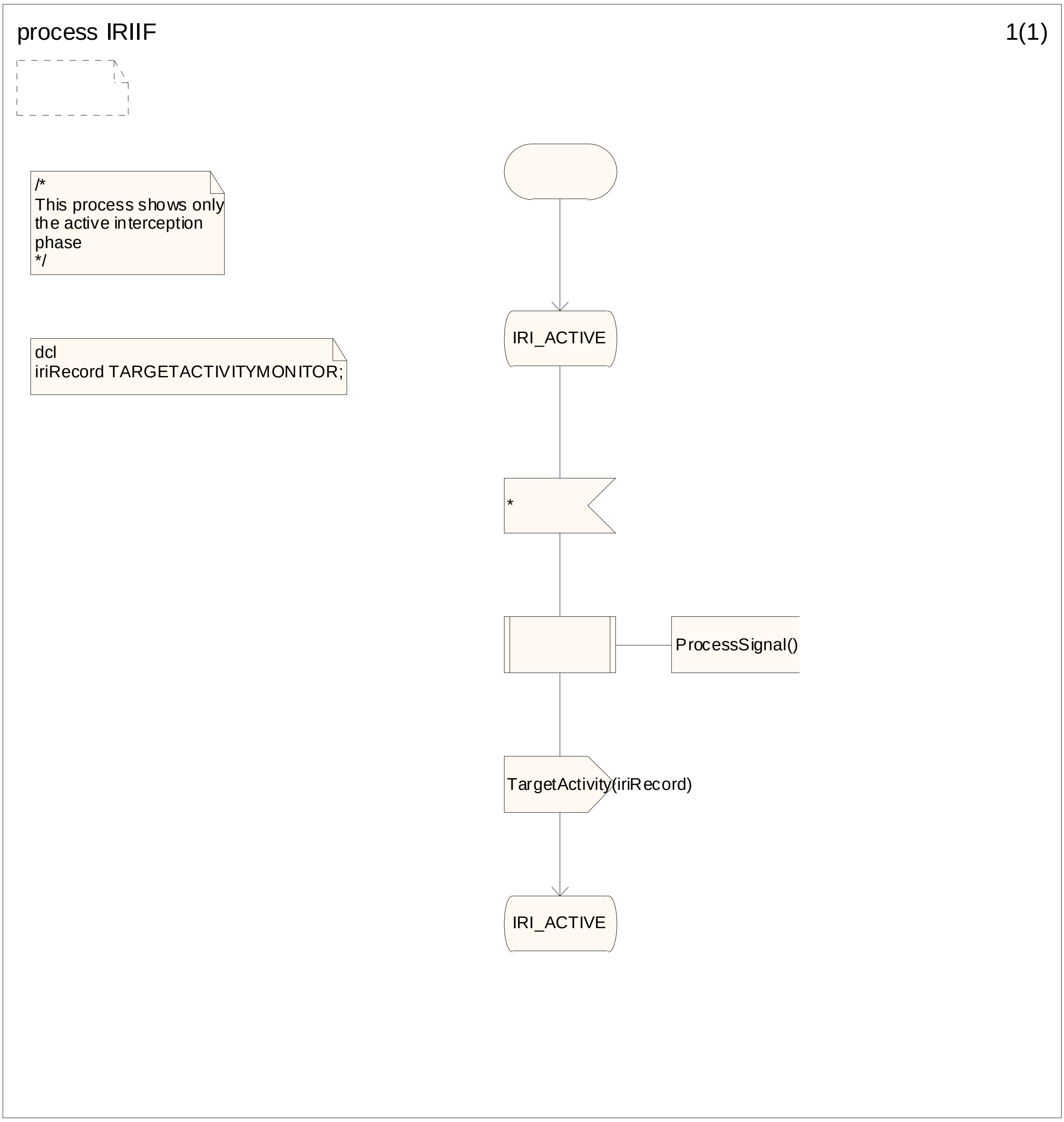


Figure D.4: Simplified IRIIF process model

D.4.2 CCIF process model

NOTE: As the behaviour of the LIAF, and of signals in INI1 are only provided for information the interaction of LIAF with CCIF is not modelled.

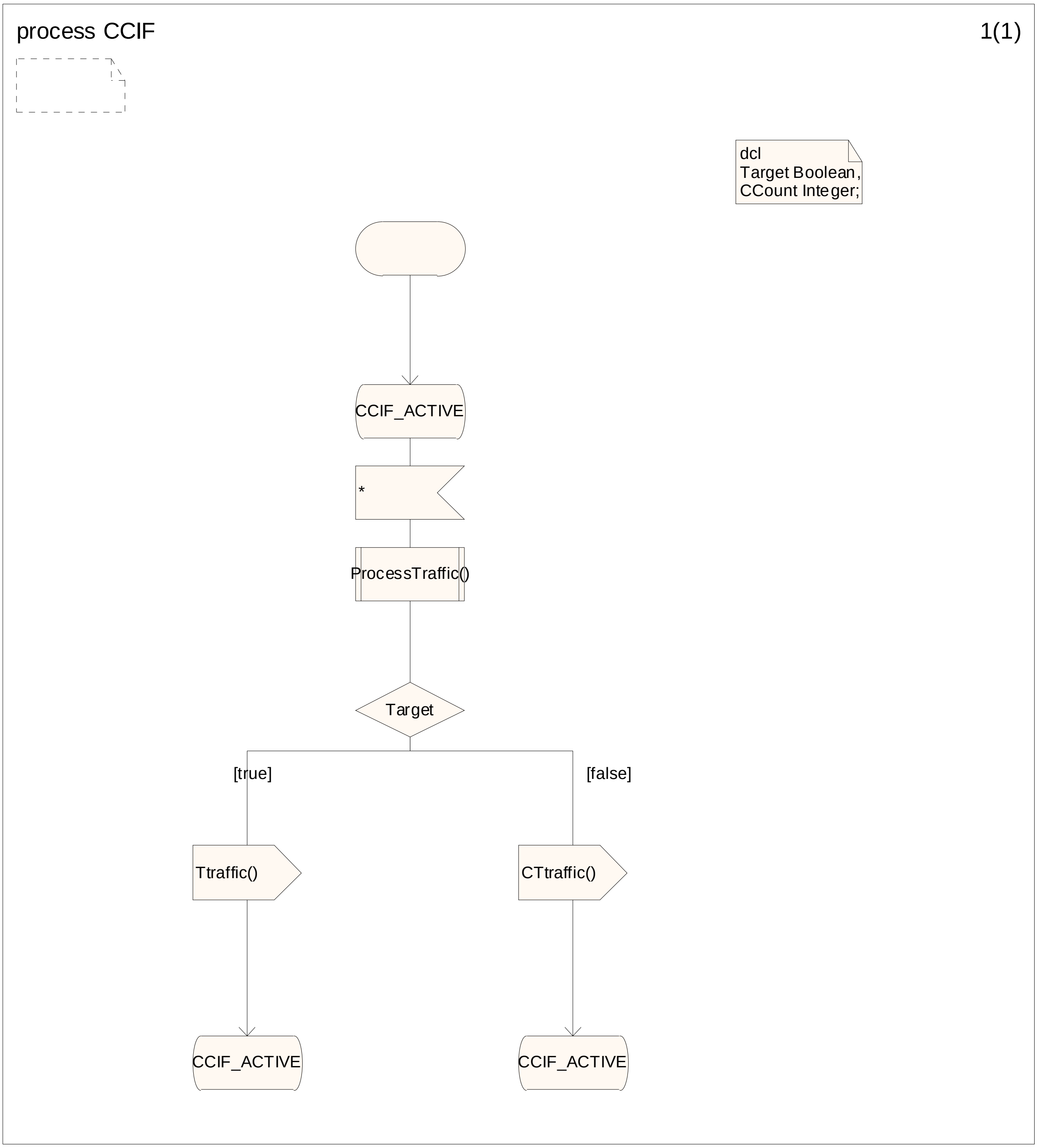


Figure D.5: Simplified CCIF process model

Annex E (informative): Signalling message classification

This clause maps signalling messages of various protocols to the corresponding messages of an IRI transaction. The definition of transaction signals as stated in clause 6 are the basis for the classification.

The analysed signalling protocols provide a centralized service according to clause 5.2.1 in a network implementing the general architecture as stated in clause 4.1.2 where the SCE is part of the IPCablecom system. In a different scenario the NWO would not have any control over the SCE. Hence, the NWO would not be able to hand over any LI related application signalling information.

NOTE 1: This mapping is only one possible solution and does not claim completeness. Since the same signalling message may depending on the service serve different purposes during a communication session it may appear in more than one category.

NOTE 2: It is assumed that signalling messages that do not have any impact on the actual communication session (media) are to be classified as "ReportSignals".

E.1 SIP

The interception of SIP services is also described in TS 33.107 [B13] and in TS 33.108 [B14]. Where the services offered by IPCablecom are as described in TS 33.107 and TS 33.108 the interception guidance given there may be applied.

SIP [B4] is the protocol standardized in the IETF to initiate Sessions. It uses the Session Description Protocol (SDP) [B5] for the description of the session's parameters including used codec optional security methods.

NOTE: For the purpose of LI proxies need to be in the signalling path of the endpoints during the entire period of the communication session. The header-field proxies must insert into INVITE messages is "Record-Route".

E.1.1 Analysed services

The following services have been analysed for this purpose:

- Basic call;
- Call transfer.

Furthermore, all SIP methods registered at the IANA have been analysed.

E.1.2 Signal classification

The following methods belong to the class "BeginSignals":

- INVITE:

The following signals belong to the class "EndSignals":

- BYE:
- 4XX Failure messages.

The following signals belong to the class "ContinueSignals":

- 2xx responses
  - as response to INVITE method;
  - as response to UPDATE method (RFC 3311) [B10].
- INVITE
  - After the reception of a redirection or failure message in response to an INVITE-BeginSignal:
    - 302 Moved Temporarily;
    - 407 Proxy Authorization required.

NOTE: If the new communication setup to the contact in the response shall trigger a new IRI transaction those message would belong to the category "EndSignals".

The following messages belong to the class "ReportSignals":

- INFO (RFC 2976) [B8]:
  - e.g. for mid-call information.
- MESSAGE (RFC 3488) [B11].
- NOTIFY (3265) [B9].
- REGISTER (RFC 3261) [B4]>
- 200 OK:
  - for the granting of a subscription subsequent to the reception of a SUBSCRIBE message (RFC 3265) [B9]
  - for the responses to capability requests with the OPTION method (RFC 3261) [B4]
- 202 Accepted:
  - for the confirmation in response to a REFER method (RFC 3515) [B12].

E.2 MGCP

The Media Gateway Control Protocol (MGCP) (RFC 2326) [B6] is used in the decomposed media gateway architecture to control media gateways, entities transforming media streams. For the session descriptions MGCP uses SDP.

E.2.1 Analysed services

The following services have been analysed for this purpose:

- Basic call.

E.2.2 Signal classification

The following methods belong to the class "BeginSignals":

- NTFY:
  - The "off-hook" of one party initiates a call.

The following signals belong to the class "EndSignals":

- NTFY:
    - The "on-hook" of a party concludes the call.

The following signals belong to the class "ContinueSignals":

- NTFY:
    - The "off-hook" of the second party concludes the call establishment.
- 200 OK:
    - is used if the confirmation of the MDCX command is used to signal call establishment.

The following signals belong to the class "ReportSignals":

- NTFY:
    - DTMF signals are also delivered by NTFY messages.

In MGCP all user side events are notified with the signalling message "Notify". Hence, all IRI signals are prepared after having received a Notify message. The context of the message (time of appearance, content) decides the action to be taken.

E.3 H.323

ITU-T Recommendation H.323 [B1] is an umbrella standard standardized in the ITU-T using the standards ITU-T Recommendation H.225.0 [B2] for signalling and ITU-T Recommendation H.245 [B3] for session parameter negotiation.

E.3.1 Analysed services

The following services have been analysed for this purpose:

- Basic call;
- Call transfer;
- Call forwarding unconditional;
- Call forwarding on busy;
- Call forwarding on no reply.

E.3.2 Signal classification

The following signals belong to the class "BeginSignals":

- ARQ;
- Setup.

Depending on the used functionality (e.g. PregrantedARQ) both signals may be used for this purpose.

The following signals belong to the class "EndSignals":

- DRQ:
  - DRQ is used in case of call transfer when the first call is released.
- ReleaseComplete.

The following signals belong to the class "ContinueSignals":

- Connect.
- OpenLogicalChannel (OLC):
  - if FastStart is not used, the received OLC provides the media description of the other party.

The following signals belong to the class "ReportSignals":

- Facility:
  - DTMF signals are conveyed in facility messages.

E.4 RTSP

Real Time Streaming Protocol (RTSP) according to RFC 2326 [B7] establishes and controls either a single or several time-synchronized streams of continuous media. SDP is one of the means to describe sessions in RTSP.

E.4.1 Signal classification

The following methods belong to the class "BeginSignals":

- Setup.

The following signals belong to the class "EndSignals":

- Teardown.

The following signals belong to the class "ContinueSignals":

- Play;
- Record;
- Pause;
- Redirect.

The following signals belong to the class "ReportSignals":

- Options;
- Describe.

Annex F (informative): Bibliography

[B1] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

[B2] ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[B3] ITU-T Recommendation H.245: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[B4] IETF RFC 3261: "SIP: Session Initiation Protocol".

[B5] IETF RFC 2327: "SDP: Session Description Protocol".

[B6] IETF RFC 3435: "Media Gateway Control Protocol".

[B7] IETF RFC 2326: "Real Time Streaming Protocol".

[B8] IETF RFC 2976: "The SIP INFO Method".

[B9] IETF RFC 3265: "Session Initiation Protocol (SIP)-Specific Event Notification".

[B10] IETF RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method".

[B11] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[B12] IETF RFC 3515: "The Session Initiation Protocol (SIP) Refer Method".

[B13] 3GPP TS 33 107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (3GPP TS 33 107 Release 6)".

[B14] 3GPP TS 33 108: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (3GPP TS 33 108 Release 6)".

[B15] ITU-R Recommendation 460-2 of the Consultative Committee on International Radio (CCIR). CCIR has also defined the acronym for Coordinated Universal Time as UTC.

[B16] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

[B17] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[B18] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

History

Document history		
V1.1.2	October 2005	Publication