ETSI TS 102 836-2 V1.1.1 (2009-11)

Technical Specification

Access, Terminals, Transmission and Multiplexing (ATTM);
Lawful Interception (LI);
Part 2: Interception of IP Data Service on Cable Operator's Broadband IP Network: Internal Network Interfaces

Reference

DTS/ATTM-02007-2

Keywords

access, cable, lawful interception

ETSI

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

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

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

Important notice

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

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

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

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

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, Terminals, Transmission and Multiplexing (ATTM).

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

The present document is part 2 of a multi-part deliverable covering Data Over Cable Systems, as identified below:

Part 1: "Interception of IP Telephony Service on Cable Operator's Broadband IP Network: Intenral Network Interfaces";

Part 2: **"Interception of IP Data Service on Cable Operator's Broadband IP Network: Intenral Network Interfaces";**

Part 3: "Interception of email Service on Cable Operator's Broadband IP Network: Intenral Network Interfaces".

Introduction

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

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

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

1 Scope

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

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

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

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

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

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

The document specifies the internal interfaces for IPv4 and IPv6 networks. For systems that are used in networks that only use IPv4, the requirements specific for IPv6 are not applicable.

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

Systems that use PPPoE over cable networks are out-of-scope.

1.1 Requirements notation

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

MUST This word or the adjective "REQUIRED" means that the item is an absolute requirement of the present document.

MUST NOT This phrase means that the item is an absolute prohibition of the present document.

SHOULD This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

SHOULD NOT This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 References

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

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

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

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

2.1 Normative references

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

[1] Council Resolution of 17 January 1995 on the lawful interception of telecommunications.

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

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

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

[5] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services;Part 4: Network Call Signalling Protocol [Partial Endorsement of ITU-T Recommendation J.162 (11/2005), modified]".

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

[7] CableLabs PKT-SP-ESP1.5-IO2-070412: "Electronic Survellience", April 12 2007.

[8] IETF RFC 768/ST0006 (August 1980): "User Datagram Protocol".

[9] IETF RFC 1305 (March 1992): "Network Time Protocol (Version 3) Specification, Implementation and Analysis.

[10] IETF RFC 791/STD0005 (September 1981): "Internet Protocol".

[11] Void.

[12] Void.

[13] IETF RFC 3924: "Cisco Architecture for Lawful Intercept in IP Networks".

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

2.2 Informative references

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

[i.1] ETSI TR 102 661 (November 2008): "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

[i.2] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

3 Abbreviations

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

CC	Call Content
CCC	Communication Call Content
CMTS	Cable Modem Termination System
CRD	Call Related Details
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
eMTA	embedded Media Terminal Adapter
HFC	Hybrid Fiber Coax
HI	Handover Interface
IAP	Intercept Access Point
IETF	Internet Engineering Task Force
IIF	Internal Intercept Function
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Law Interception
LIAF	Lawful Interception Administration Function
LIMD	Lawful Intercept Mediation Device
MAC	Media Access Control
MD	Mediation Device
MF	Mediation Function
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MTA	Media Terminal Adapter
NCS	Network-based Call Signalling
NWO	Network Operator
SBCF	SNMP Based Configuration Function
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SvP	Service Provider
TAP	Tapping
TCP	Transmission Control Protocol
UDP	User Data Protocol
USM	User-based Security Module
VACM	View-based Access Control Module

4 Requirements

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

a) the network equipment needs to be capable of copying all Communication Call Content (CCC) being carried to and from specified target addresses to an additional delivery address specified by the network operator;

b) in the short term, for practical reasons, identification of voice related calls (including fax and modem calls) may use E.164 addresses;

c) where interception of both data and multi-media content is also required, the delivery address will be specified as an IP address in either the standard IPv4 or IPv6 formats; the target addresses may be either service addresses or IP addresses;

d) the mechanism for lawful interception, where provided, in an IPCablecom system will ideally be capable of correct operation in networks where a customer's IP address is allocated dynamically, e.g. by a DHCP server, by relating the current IP address to the customer's equipment MAC address, or otherwise;

e) it needs to be possible to provide both the Call Content and the Intercept Related Information (IRI) regarding the communication, including that added by the network operator to facilitate correct identification of the intercept to the law enforcement agencies;

f) the mechanism for LI should correctly relate the 'Call Content' and the 'CRD';

g) the capacity of the LI mechanism to provide multiple intercepts should be adequate; this requirement is subject of National Legislation.

h) the LI facility should be capable of providing numerous simultaneous intercepts and be capable of providing several independent intercepts of the same target address; this requirement is subject of National Legislation.

i) operation of the intercept should be invisible to any customer, even by the use of 'traceroute', 'ping' and similar utilities;

j) any malfunction or mis-operation of the interception facility should not affect the customer's service;

k) control of the facility needs to be segregated from normal operation of the system;

l) it needs to be possible to address and control the interception facility remotely by secure means.

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

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

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

The following general requirements apply:

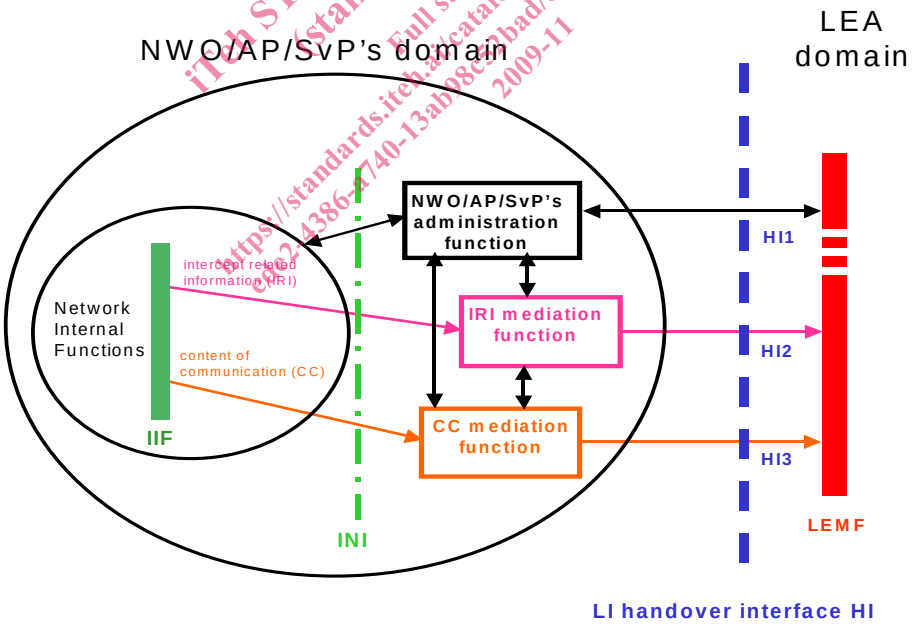
- The LI general requirements as given by TS 101 331 [i.2], including the requirements below apply:
  - Deliver content of communications for voice, fax.
  - Deliver intercept related information.
  - Interception of call features.
  - Real-time delivery.
  - Non-disclosure of information including interception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

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

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

5 Overview

The overall interception framework is extended from the model described in clause 5.2 of ES 201 158 [14] and from the architecture identified in clause 5 of TS 101 671 as given by [3].



IIF: internal interception function
INI: internal network interface
HI1: administrative information
HI2: intercept related information
HI3: content of communication

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

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

The current solution adopts elements of the reference model for LI systems in IP networks defined in RFC 3924 [13], see figure 2.

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

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

The description of the functional elements and interfaces at a generic level as given by RFC 3924 [13], section 2.1 are applied to Cable Networks as described witin clause 5 of the present document.

6 Internal Cable Network Interfaces

6.1 Introduction

The Cable Network provides data services using the (Euro) DOCSIS™ [5] architecture.

The diagram given by figure 2 illustrates the reference model as specified for a Cable Network.

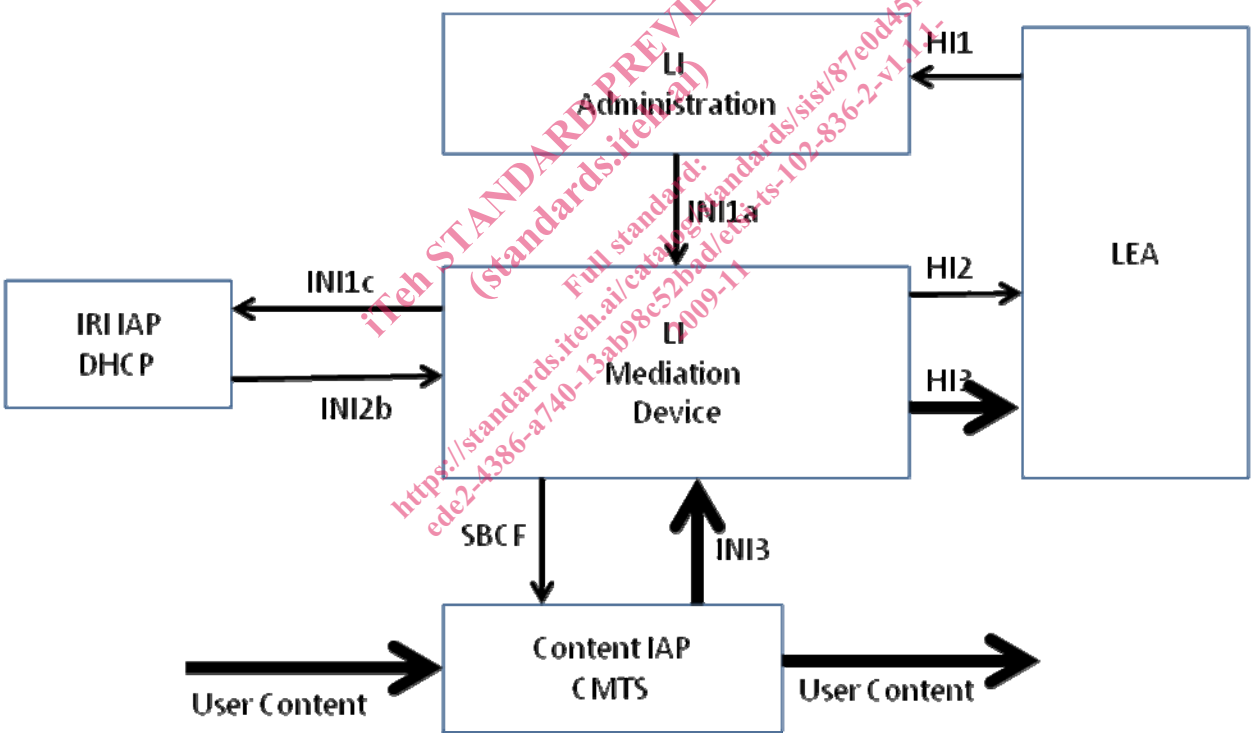


Figure 2: Cable Network Reference model for Lawful Interception

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

6.2 INI1

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