TECHNICAL REPORT

ISO/TR 11766

First edition
2010-04-15

Intelligent transport systems — Communications access for land mobiles (CALM) — Security considerations for lawful interception

Systèmes intelligents de transport — Accès aux communications des services mobiles terrestres (CALM) — Considérations de sécurité pour interception licite

Reference number
ISO/TR 11766:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 11766 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

Intelligent transport systems — Communications access for land mobiles (CALM) — Security considerations for lawful interception

1 Scope

This Technical Report reviews the ITS landscape and the provisions of lawful interception to ITS deployments. In particular it considers the CALM environment and the services offered in the IPv6 domain served by CALM and ITS in general.

2 Conformance

There are no conformance requirements. This clause is included to provide numerical consistency between this Technical Report and other CALM International Standards.

3 Normative references

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

ISO 21217, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

ETSI ES 201 671, *Telecommunications security — Lawful Interception (LI) — Handover interface for the lawful interception of telecommunications traffic*

ETSI TS 101 331, *Telecommunications security — Lawful Interception (LI) — Requirements of Law Enforcement Agencies*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 21217 and ETSI ES 201 671 apply.

5 Abbreviated terms

CSP communication service provider

ECN electronic communication network

ECS electronic communication service

ITS intelligent transport systems

IUR International User Requirement[1)]

LEA law enforcement agency

LEMF law enforcement monitoring facility

LI lawful interception

MF mediation function

OSS operations support system

PoI point of interception

6 Overview

6.1 General requirement

A lawful interception (LI) capability is required to support the activities of LEAs. The requirements for LI have been developed by LEAs in the IUR and published for the specific needs of telecommunications providers in ETSI TS 101 331. The obligation to support and provide LI facilities applies to any CSP operating either an ECN or an ECS. This Technical Report identifies the consequences for standardization of the provision of LI for CALM-based ITS.

The core requirements in regional regulation that enforce LI are given in Annexes A to C, where the main impact is as follows.

— A CSP should provide mechanisms to ensure the interception and handover of signalling of specific users, if required to by a lawful authority.

— A CSP should provide mechanisms to ensure the interception and handover of the content of communication of specific users, if required to by a lawful authority.

The structure of a CSP is outlined in Figure 1, where providers of ECNs and ECSs are shown as specialisms of the generic CSP.

1) The IUR is provided as an annex to Reference [11].

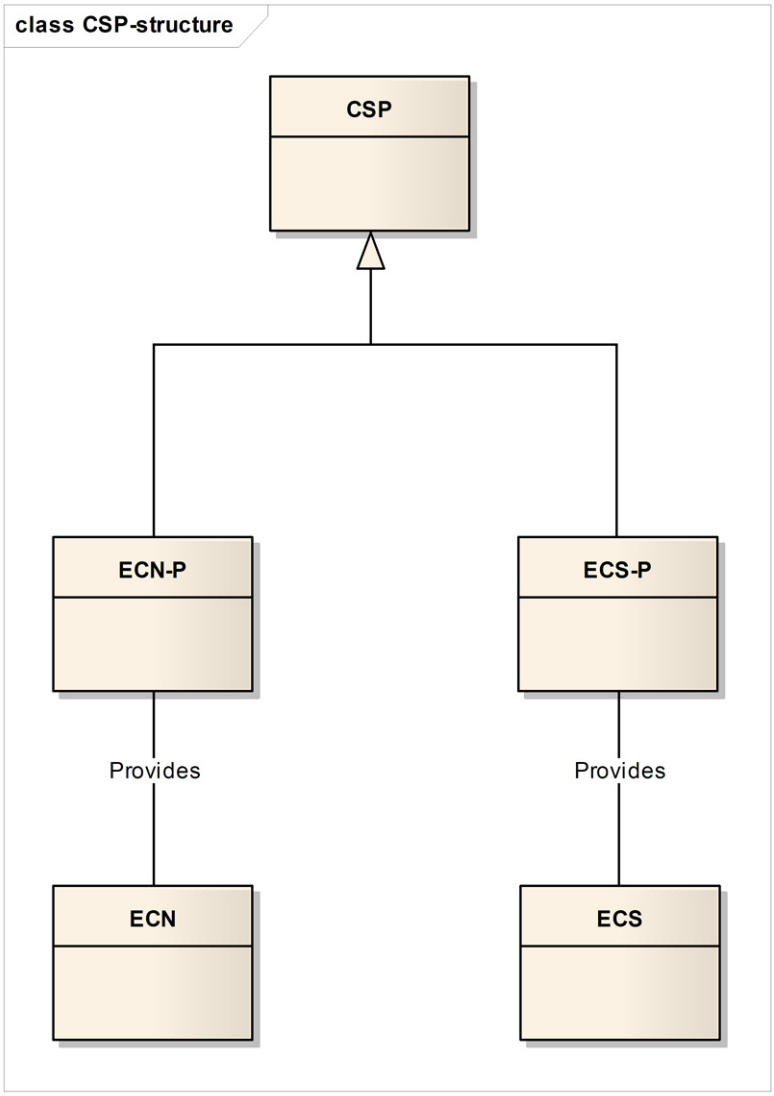


Figure 1 — Structure of CSP relationship to ECN and ECS

6.2 Handover domain capabilities in CALM/ITS

The CALM-based ITS network should interface to the LEA and its associated LEMF using the capabilities defined in

— ETSI ES 201 671 (where handover is provisioned over ISDN networks), or

— ETSI TS 102 232-1 [4] [where handover is provisioned over packet switched (IP) networks],

or using any appropriate handover interface defined by the LEA.

6.3 Interception domain capabilities in CALM/ITS

6.3.1 General

The general architecture for the interception domain (which covers both CALM and ITS) is defined in ETSI ES 201 158 [1] and the generic reference model for the interception domain is defined in ETSI TR 102 528 [3].

The internal intercept functions

— intercept related information internal intercept function (IRI-IIF),

— content of communication internal intercept function (CC-IIF), and

— content of communication trigger function (CCTF),

and the internal interfaces

— INI1, INI2, INI3,

— content of communication trigger interface (CCTI), and

— content of communication control interface (CCCI)

are also adopted for CALM and ITS (see Figure 2).

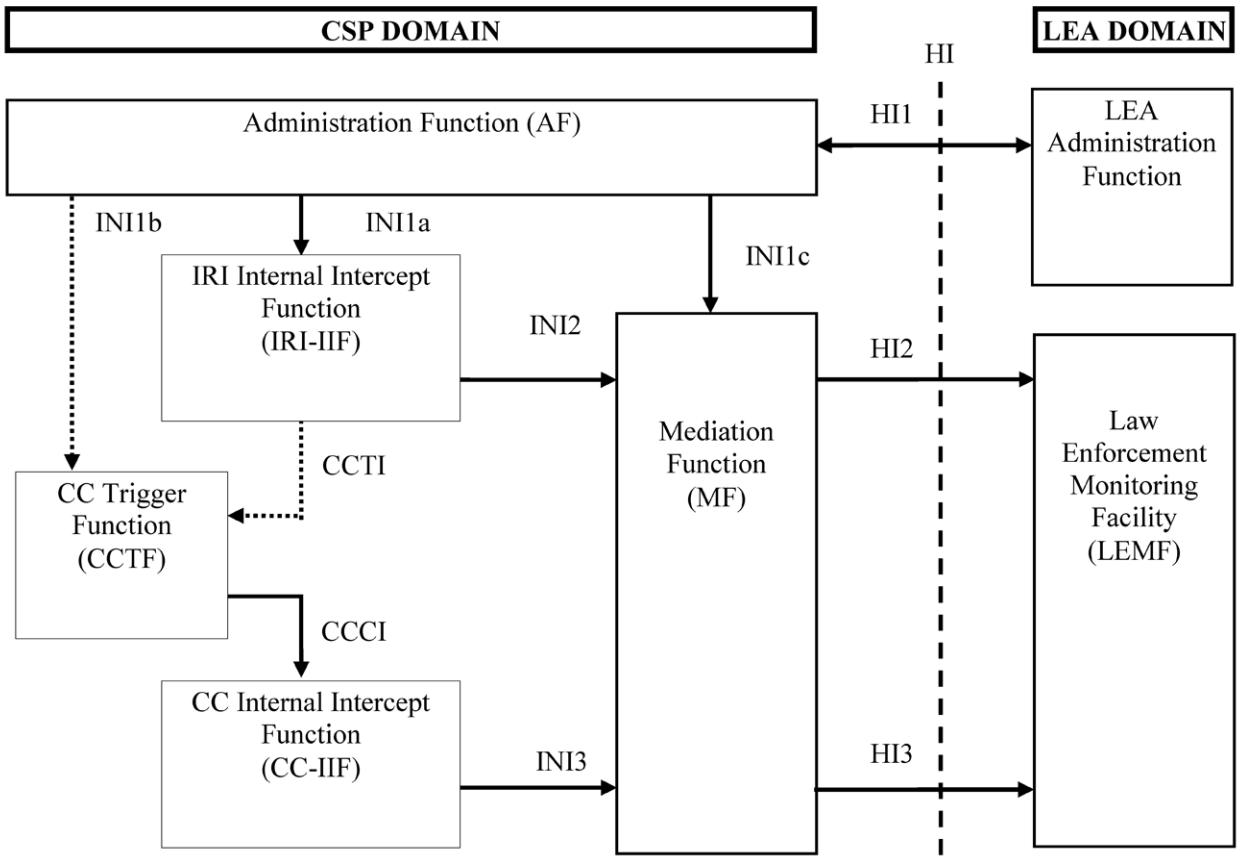


Figure 2 — Reference model for LI based on ETSI TR 102 528

The reference model describes the following functions and interfaces.

— IRI-IIF generates signalling intercept material.

— CC-IIF generates content intercept material.

— CCTF controls the CC-IIF.

— Internal interface INI1 carries provisioning information from the lawful interception administration function (AF) to the internal intercept functions (IIF).

— Internal interface INI2 carries intercept related information (IRI) from the IRI-IIF to the MF.

— Internal interface INI3 carries content of communication (CC) information from the CC-IIF to the MF.

— CCTI carries trigger information from the IRI-IIF to the CCTF.

— CCCI carries controls information from the CCTF to the CC-IIF.

The model for LI is given as a UML class model in Figure 3.

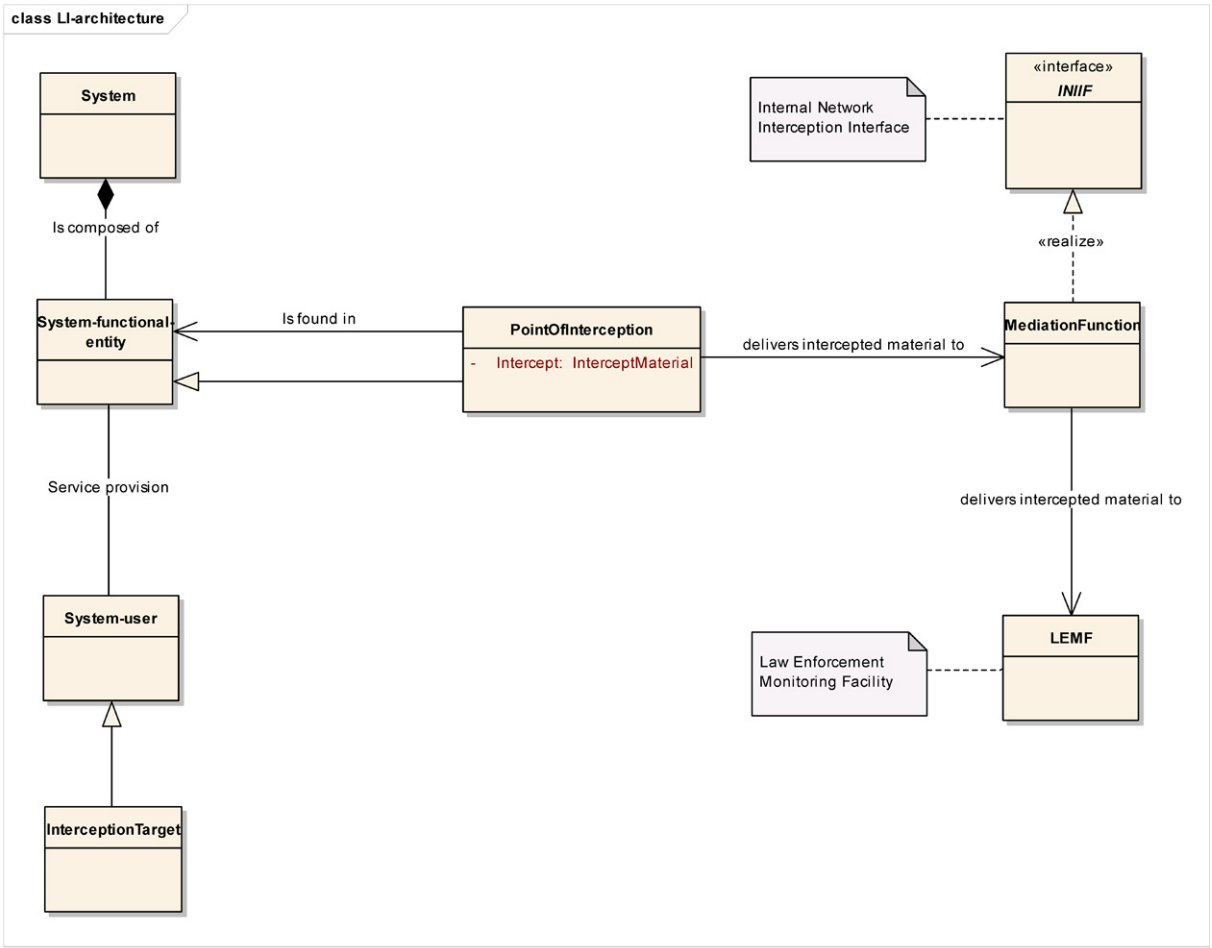


Figure 3 — UML class model of interception

The key concepts shown in the model are as follows.

a) The “target” is a system user with the specialization that he is subject to interception.

b) The “point of interception” (PoI) is a specialization of a system functional entity (FE) that is also found in an FE (e.g. the PoI may be found in a call processing FE).

The data model for LI is given in Figure 4.

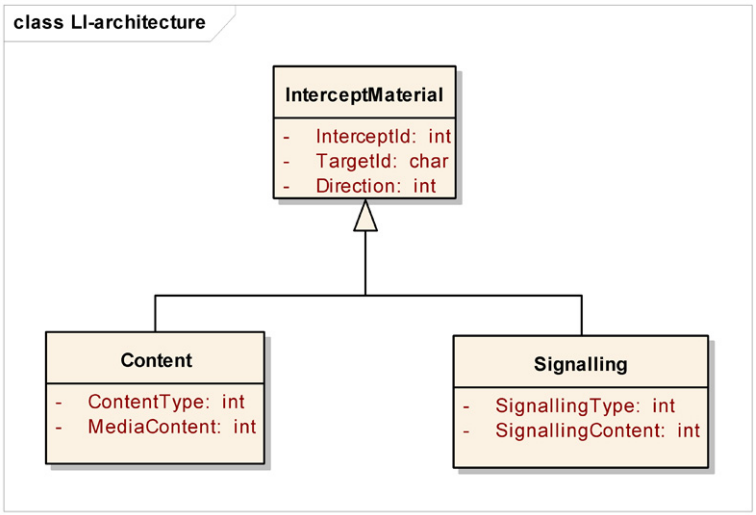


Figure 4 — Data model for LI

Interception data has two specializations:

— content (media streams);

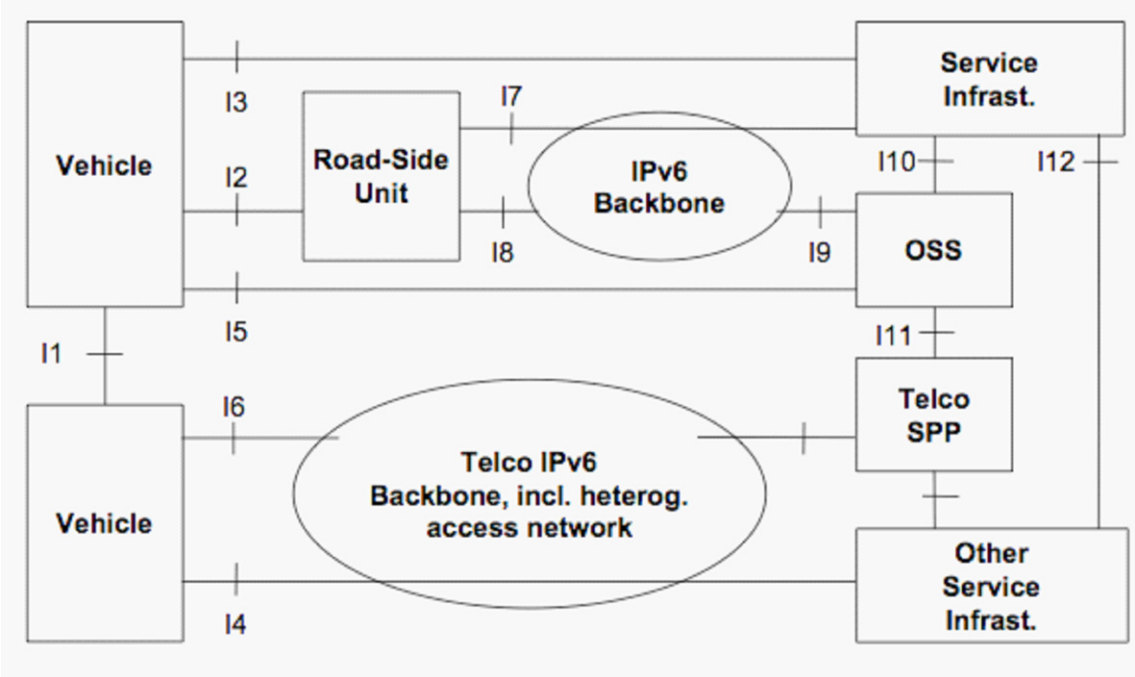
— signalling.

The data contains sufficient information to identify the target, the LEA, and the direction of the data (to or from the target). In both the interception domain and the handover domain there should be a clear means to allow the LEA/LEMF to correlate content and signalling (i.e. content x arising from signalling y, belonging to a common target).

6.3.2 Characteristics of PoI

In the CALM architecture, routing nodes may be vehicles, roadside beacons, roadside concentrators and core network breakout points. Non-routing CALM nodes shall not be used for interception (i.e. end points do not act as the PoI).

The use of CALM in a generic ITS architecture, as shown in Figure 5, is used to highlight those elements that may become a PoI.



NOTE The road-side unit might not have interfaces I7 and I8 in some deployments.

Figure 5 — CALM network interconnection reference model

Communications that traverse interfaces I3, I7, I6 and I4 may be intercepted. The physical location of the PoI should be in all cases at the fixed infrastructure end of the interface.

6.3.3 Characteristics of CALM and identification of CALM users

As shown in Figure 2, the target for LI is a specialization of a system user (where the system is ITS over CALM). The interception of CALM where the media has a public identity, e.g. 2G and 3G cellular networks, can be explicitly intercepted against the public identity.

7 Stage 1 description of the LI interception facility

7.1 General

The requirements given in both this clause and Clause 8 are examples of how a translation of the IUR could be presented in a future International Standard or other technical standard.

7.2 Description

In recognizing the need identified in Clause 6 for CSPs to support the activities of LEAs, the CSP should provide mechanisms to ensure the interception and handover of signalling and of the content of communication of specific users, if required to by a lawful authority. Where possible, the CSP should use existing facilities to hand over any intercepted information.

7.3 Procedures

7.3.1 Provision/withdrawal

The LI interception service shall always be provided.

7.3.2 Normal procedures

7.3.2.1 Activation/deactivation/registration

The LI interception service shall be activated upon issue of a valid interception order from an LEA. The LI interception service shall be deactivated when the interception order expires or as defined by the LEA.

7.3.2.2 Invocation and operation

The LI interception service shall be invoked on any communication from or to the target visible in the network.

7.3.2.3 Interrogation

Interrogation shall be possible only from an authorized user.

For the purposes of interrogation, an authorized user is one who is allowed by both LEA and the network operator/service provider to administer the LI interception service.

7.4 Interaction with other services

There shall be no interaction, i.e. the invocation of LI shall not alter the operation of any service.

8 Stage 2 description of the LI interception facility

The stage 2 specification identifies the key functional elements for interception in a CALM/ITS network and the information flows associated to interception.

The handover interface from which the LEA/LEMF receives intercepted material consists of the following three key elements.

— HI1: control information for administration of the interception (start, stop, target data, etc.).

— HI2: intercepted material relating to the signalling to and from the target.

— HI3: intercepted material relating to the content of communication to and from the target.

At the time of publication of this Technical Report, only HI2 and HI3 have been specified in international standards.

The HI2 interface is composed of the following four record types.

— IRI_Begin

  Intercept related information (IRI) identifying the start of a stateful transaction and containing the user signalling (e.g. an ISDN voice call setup message).

— IRI_Continue

  An IRI record identifying intermediate signalling in the course of a stateful transaction (e.g. invocation of a supplementary service during an ISDN voice call).

— IRI_End

An IRI record identifying the end of a stateful transaction (e.g. call clear in an ISDN voice call).

— IRI_Report

An IRI record that provides signalling information that is not directly related to a stateful transaction.

Annex A
(informative)

LI requirement for EU/EFTA

This annex is provided to illustrate the regional requirements that apply in the EU/EFTA.

Operators subject to the authorization directive, i.e. those considered as communications service providers (CSP) in the context of the EU Framework Directive and the ECN&S regime, are required to support LI from statements made in the EU privacy directive EC/2002/58 [11]. In particular, Article 5 states:

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

In addition, ETSI SR 002 211 [2] identifies those aspects of standardization that are required to ensure compliance with the European Framework Directive. In some instances, the right to privacy can be withheld, as suggested in Article 5(2) of the privacy directive [see Article 5(1)]. Provisions for the lawful interception of traffic and for retention of signalling data are allowed to contain exceptions, as defined in Article 15(1) of the privacy directive:

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Annex B
(informative)

LI requirement for the United States of America (USA)

This annex is provided to illustrate the regional requirements that apply in the USA.

In the USA, the 1968 *Omnibus Crime Control and Safe Streets Act*, *Title III*[12] and the *Foreign Intelligence Surveillance Act (FISA)*[13] apply for LI.

NOTE 1 The US Congress passed the *Communications Assistance for Law Enforcement Act* (*CALEA*)[14] in 1994 to provide broad guidelines to network operators on how to assist the LEAs in setting up interceptions and the types of data to be delivered.

NOTE 2 The US Congress has extended the basic provisions above within the USA *Patriot Act*[15] to specifically cover terrorist activity and not general criminal activity.

Annex C
(informative)

LI requirement for Australia

This annex is provided to illustrate the regional requirements that apply in Australia.

The *Telecommunications (Interception and Access) Act* of 1979 [12] requires any entity that provides carriage services (a *carrier*) to provide an interception and delivery capability. The *carrier* is required to provide interception and delivery of intercepted communications to a delivery point, unless an exemption applies. Where a ministerial determination exists, the interception capability may be defined in a relevant international standard. A *carrier* is required to submit an *Interception Capability Plan* outlining the *carrier's* plan to provide interception and delivery capabilities.

Bibliography

[1] ETSI ES 201 158, *Telecommunications security — Lawful Interception (LI) — Requirements for network functions*

[2] ETSI SR 002 211, *Electronic communications networks and services — Candidate list of standards and/or specifications in accordance with Article 17 of Directive 2002/21/EC*

[3] ETSI TR 102 528, *Lawful Interception (LI) Interception domain Architecture for IP networks*

[4] ETSI TS 102 232-1, *Lawful Interception (LI) — Handover Interface and Service-Specific Details (SSD) for IP delivery — Part 1: Handover specification for IP delivery*

[5] ETSI TS 102 232-2, *Lawful Interception (LI) — Handover Interface and Service-Specific Details (SSD) for IP delivery — Part 2: Service-specific details for E-mail services*

[6] ETSI TS 102 232-3, *Lawful Interception (LI) — Handover Interface and Service-Specific Details (SSD) for IP delivery — Part 3: Service-specific details for internet access services*

[7] ETSI TS 102 232-4, *Lawful Interception (LI) — Handover Interface and Service-Specific Details (SSD) for IP delivery — Part 4: Service-specific details for Layer 2 services*

[8] ETSI TS 102 232-5, *Lawful Interception (LI) — Handover Interface and Service-Specific Details (SSD) for IP delivery — Part 5: Service-specific details for IP Multimedia Services*

[9] ETSI TS 102 232-6, *Lawful Interception (LI) — Handover Interface and Service-Specific Details (SSD) for IP delivery — Part 6: Service-specific details for PSTN/ISDN services*

[10] COM 96/C329/01, *European Union Council Resolution COM 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications*

[11] EU privacy directive EC/2002/58

[12] *The Omnibus Crime Control and Safe Streets Act of 1968* (Pub.L. 90-351, June 19, 1968, 82 Stat. 197, 42 U.S.C) (USA)

[13] *The Foreign Intelligence Surveillance Act of 1978* ("FISA" Pub.L. 95-511, 92 Stat. 1783, enacted October 25, 1978, 50 U.S.C.) (USA)

[14] *The Communications Assistance for Law Enforcement Act (CALEA)* (USA)

[15] *The USA PATRIOT Act* [*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law Pub.L. 107-56)*] (USA)

[16] *Telecommunications (Interception and Access) Act,* 1979 (Australia)

ICS 03.220.01; 35.240.60

Price based on 13 pages