

ETSI TS 101 331 V1.8.1 (2021-07)



Lawful Interception (LI); Requirements of Law Enforcement Agencies (standards.iteh.ai)

[ETSI TS 101 331 V1.8.1 \(2021-07\)](https://standards.iteh.ai/catalog/standards/sist/d65874d8-72f5-45a8-9efe-3402e9b8f13c/etsi-ts-101-331-v1-8-1-2021-07)

<https://standards.iteh.ai/catalog/standards/sist/d65874d8-72f5-45a8-9efe-3402e9b8f13c/etsi-ts-101-331-v1-8-1-2021-07>

Reference

RTS/LI-00206

Keywords

lawful interception, security

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

<https://portal.etsi.org/TB/ETSI/DeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2021.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	9
3.3 Abbreviations	9
4 User (LEA) requirements	10
4.1 Overview	10
4.2 General requirements	10
4.3 Result of interception	12
4.4 Location information.....	12
4.5 Time constraints	13
4.6 Non-disclosure	13
4.6.1 Communications Service Provider	13
4.6.2 Manufacturers	13
4.7 Information transmission and information protection requirements	14
4.8 Internal security.....	14
4.9 Unchanged state of service, etc.	15
4.10 Technical handover interfaces and format requirements	15
4.11 Independence of the Communications Service Provider	16
4.12 Temporary obstacles to transmission	16
4.13 Identification of the identity to be intercepted.....	16
4.14 Multiple interception measures	17
Annex A (normative): Detailed requirements of law enforcement agencies for circuit switched oriented communications networks and services	18
A.0 Overview	18
A.1 Details on clause 4.3, item d)	18
A.2 Details on clause 4.4.....	18
A.3 Details on clause 4.7, items i) and j)	18
A.4 Details on clause 4.10, items a) and h).....	19
Annex B (normative): Detailed requirements of law enforcement agencies for packet oriented communications networks and services	20
B.0 Overview	20
B.1 Details on clause 4.3, items d) and e).....	20
B.2 Details on clause 4.4.....	21
B.3 Details on clause 4.7, item i).....	21
B.4 Details on clause 4.10, item a)	21
Annex C (normative): Advanced services	22

Annex D (informative):	Examples of advanced services.....	23
D.0	Overview	23
D.1	General capabilities	23
D.1.1	Registration/authorization events	23
D.1.2	Communication content events	23
D.1.3	Feature management events	23
D.1.4	Interception status events	23
D.2	Voice capabilities	24
D.2.1	Call management events.....	24
D.2.2	Feature use events	24
D.3	Messaging capabilities	25
D.3.0	Overview	25
D.3.1	Message creation events	25
D.3.2	Message reception events	25
D.3.3	Automatic welcome or reply message management	25
Annex E (informative):	Explanatory diagrams	26
E.0	Overview	26
E.1	General network arrangements.....	26
E.2	Service providers.....	27
E.3	Home country service from a foreign territory.....	28
E.4	Identification of a target service.....	29
Annex F (informative):	Basic requirements for interception across national frontiers	31
Annex G (informative):	Change Request History.....	32
History	https://standards.iteh.ai/catalog/standards/sist/d65874d8-72f5-45a8-9efc-3402e9b8f13c/etsi-ts-101-331-v1-8-1-2021-07	33

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

ITih STANDARD PREVIEW
(standards.itech.ai)

Foreword

ETSI TS 101 331 V1.8.1 (2021-07)
This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).
The present document replaces ETSI ETR 331 (1996) [i.1] (and earlier versions of the present document).

Modal verbs terminology

In the present document **"shall"**, **"shall not"**, **"should"**, **"should not"**, **"may"**, **"need not"**, **"will"**, **"will not"**, **"can"** and **"cannot"** are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"must" and **"must not"** are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Originally ETSI ETR 331 [i.1] was intended to incorporate into ETSI standards the EU Council Resolution of 1995 [1] on International User Requirements. In consequence, the original ETSI ETR 331 [i.1] concentrated on telephony networks such as PSTN, ISDN and GSM because these were the main communications networks. The introduction of TETRA, GPRS, UMTS and the increased usage of the Internet forced a change so that ETSI ETR 331 [i.1] has been replaced by the present document which focuses on the interpretation of ETSI ETR 331 [i.1] on specific technologies in the different annexes.

According to rules set by the laws of individual nations as well as decisions of the European Union, there is a need to lawfully intercept communications traffic and intercept related information in modern communications systems. With the aim of harmonising the interception policy in the member states, the Council of the European Union adopted a set of requirements in EU Council Resolution of 1995 [1], with the aim of feeding them into national legislation. The LEA requirements have to be taken into account in defining the abstract handover interface.

The definition of a handover interface for the delivery of the results of lawful interception should allow the technical facilities to be provided:

- with reliability;
- with accuracy;
- at low cost;
- with minimum disruption;
- most speedily;
- in a secure manner;
- using standard procedures.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ETSI TS 101 331 V1.8.1 \(2021-07\)](https://standards.iteh.ai/catalog/standards/sist/d65874d8-72f5-45a8-9efe-3402e9b8f13c/etsi-ts-101-331-v1-8-1-2021-07)

<https://standards.iteh.ai/catalog/standards/sist/d65874d8-72f5-45a8-9efe-3402e9b8f13c/etsi-ts-101-331-v1-8-1-2021-07>

1 Scope

The present document gives guidance for lawful interception of communications in the area of co-operation by Communications Service Providers (CSPs). It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies. Requirements with regard to communications services provided from areas outside national boundaries are not fully developed yet and therefore only some preliminary requirements have been annexed for information.

The present document describes the requirements from a Law Enforcement Agency's (LEA's) point of view.

Not all requirements necessarily apply in one individual nation.

These requirements need to be used to derive specific network requirements and furthermore to standardize handover interfaces.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://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.

The following referenced documents are necessary for the application of the present document.

- [1] European Union Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01).

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".
- [i.2] ETSI TS 103 307: "CYBER; Security Aspects for LI and RD Interfaces".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

access provider: company that provides a user of some network with access from the user's terminal to that network

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

call: logical association between several users (this could be connection oriented or connection less) capable of transferring information between two or more users of a communications system

NOTE: In this context a user may be a person or a machine.

communications: 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

Communications Service Provider (CSP): network operator, access provider or service provider who is obliged by law to perform a lawful action in response to a warrant (e.g. perform Lawful Interception)

content of communication: information exchanged between two or more users of a communications service, excluding intercept related information

NOTE: This includes information which may, as part of some communications service, be stored by one user for subsequent retrieval by another.

Handover Interface (HI): physical and logical interface across which the interception measures are requested from CSP, and the results of interception are delivered from a CSP to a law enforcement monitoring facility

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

intercept related information: collection of information or data associated with communication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data (e.g. service profile management by subscriber) and location information

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

NOTE: In the present document the term interception is not used to describe the action of observing communications by an LEA (see below).

interception interface: physical and logical locations within the CSP's communications facilities where access to the content of communication and intercept related information is provided

NOTE: The interception interface is not necessarily a single, fixed point.

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

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

Law Enforcement Monitoring Facility (LEMF): law enforcement facility designated as the transmission destination for the results of interception relating to a particular target

lawful authorization: permission granted to an LEA under certain conditions to intercept specified communications and requiring co-operation from a CSP

NOTE: 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 a target

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

quality of service: quality specification of a communications channel, system, virtual channel, computer-communications session, etc.

NOTE: 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.

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 CSP to an LEA

NOTE: Intercept related information has to be provided whether or not communication activity is taking place.

service provider: natural or legal person providing one or more public communications services whose provision consists wholly or partly in the transmission and routeing of signals on a communications network

NOTE: A service provider need not necessarily run his own network.

target: entity or entities, specified in a warrant, the lawful action applies to (e.g. whose communications are to be intercepted)

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

target service: communications service associated with a target and usually specified in a warrant for interception

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

warrant: formal mechanism to require lawful action from a LEA served to the CSP on given target identifier(s)

NOTE: Depending on jurisdiction a warrant is also known as: intercept request, intercept order, lawful order, court order, lawful order or judicial order (in association with supporting legislation).

3.2 Symbols

Void.

3.3 Abbreviations

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

ADSL	Asymmetrical Digital Subscriber Line
CC	Content of Communications
CSP	Communication Service Provider
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI	Handover Interface
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MSISDN	Mobile Station International ISDN number

PDP	Packet Data Protocol
PSTN	Public Switched Telephone Network
TETRA	TErrestrial TRunked RAdio
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunications
VoIP	Voice over IP

4 User (LEA) requirements

4.1 Overview

This clause presents the user requirements related to the lawful interception of communications with the LEA being the user. The relevant terms are defined in clause 3.1. These user requirements are subject to national law and international treaties and should be interpreted in accordance with applicable national policies.

The following list of requirements is a collection of items, where several requirements might not correspond to national laws and regulations of the individual countries. Implementation takes place if required by national law. The Handover Interface(s) (HIs) should be configured in such a way that it (they) will comply with the appropriate national requirements. A warrant will specify a subset of requirements to be delivered on a case-by-case basis.

The consequences and implications of these requirements contain clarifications for new developments (e.g. virtualized networks or 5G communications).

4.2 General requirements

- a) The obligation of the CSP as to which communications traffic shall be intercepted is subject to national laws.
- b) In accordance with the relevant warrant a CSP shall ensure that:
 - 1) the entire content of communication associated with a target identity being intercepted can be intercepted during the entire period of the warrant;
 - 2) any content of communication associated with a target identity being intercepted which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire period of the warrant;

NOTE 1: Interception at retrieval from storage is assumed to be performed by the provider of such services, if covered by the warrant for interception. This may not be always be possible, e.g. if a mailbox storage facility is located in another country. Access to the stored information by the LEA might be by a search warrant and not by interception as such.

- 3) the delivery of the intercept related information is reliable. If the intercept related information cannot be delivered immediately to the relevant LEMF, then the intercept related information shall be buffered until they can be delivered;
- 4) the delivery of the content of communication is reliable. If the content of communication cannot be delivered immediately to the relevant LEMF, then the content of communication shall be buffered if this is required by national laws;

NOTE 2: Buffering is assumed to take place according to normal routines and regularly installed facilities in the network for the type of communication being intercepted. If special measures for buffering are requested by the authorities, these would normally be provided external to the regular communication system, e.g. in mediation devices.

NOTE 3: Buffering is applied to prevent information loss due to disturbances or delays in the network or delivery mechanism. Buffering is not intended to overcome the exceptional case the LEMF is not available.

NOTE 4: Requirements for buffering to secure delivery of interception products should be based on analysis of total system reliability, including delivery nodes, delivery channels, the LEMF and any buffering devices that are used.

- 5) the CSP shall not monitor or permanently record the results of interception.
- 6) the CSP shall be able to deliver location information, as a choice, only at the beginning and end of a target's communications, during all phases of a target's communications, or independent of a target's communications. The exact method shall be able to be set on a per-intercept basis to satisfy a specific warrant.
- c) The ability to intercept communications shall be provided relating to the targets operating permanently within a communications system (e.g. a subscriber or account).
- d) The ability to intercept communications shall be provided relating to the targets operating temporarily within a communications system (e.g. a visiting mobile subscriber or a visiting subscriber using an access network to a home service). A visited network shall be able to process the interception of all services without home network assistance or visibility, using the identifiers provided by an LEA.
- e) The results of interception relating to a target service shall be provided by the CSP in such a way that any communications that do not fall within the scope of the warrant shall be excluded by the CSP.

NOTE 5: It is assumed that the intercepting system exercises best effort to exclude non-authorized interception patterns (e.g. transferred communication).

- f) All results of interception provided at the handover interface shall be given a unique identification relating to warrant.
- g) The LI requirements are not limited to communication of individuals. The LI requirement also applies to devices in IoT including CIoT.
- h) The results of interception relating to a target service shall be provided by the CSP in such a way that only information that falls within the scope of the warrant shall be delivered, while information that falls outside the scope of the warrant shall be excluded by the CSP. The following are some examples:
<https://standards.iteh.ai/catalog/standards/sist/d65874d8-72f5-45a8-9efc-3402e9b8f13c/etsi-ts-101-331-v1-8-1-2021-07>
 - 1) Target location information:
 - i) all location information is delivered or is excluded;
 - ii) location information only at the beginning and end of a communication is delivered while location information at other phases of communication is excluded;
 - iii) location information at all phases of a communication is delivered while location information outside communications phases is excluded; or
 - iv) location information independent of any communications is delivered.

The location information identified for exclusion shall be omitted from the results of interception delivered to the LEMF.

- 2) Content of communication:
 - For IRI-only intercepts, the content of communication of the target shall be omitted from the results of interception delivered to the LEMF.
- 3) Post dialled digits:
 - Depending on the requirements for IRI-only intercepts, post dialled digits from the target, associated with voice/VoIP communications (see Annex D.2.1) shall be excluded from the results of interception delivered to the LEMF.

NOTE 6: Information used for the IRI is expected to be part of standard network signalling procedures. No additional signalling is expected for the IRI.

4.3 Result of interception

The CSP shall, in relation to each target service:

- a) provide the content of communication (see also clause 4.2, bullet h));
- b) remove any service coding or encryption which has been applied to the content of communication (i.e. en clair) and the intercept related information at the instigation of the CSP;

NOTE 1: If coding/encryption cannot be removed through means, which are available in the network or service for the given communication, the receiving agencies should be provided with keys, etc. to access the information en clair, see clause 4.3, item c).

- c) provide the LEA with any other decryption keys whose uses include encryption of the content of communication, where such keys are available for NWO/SvP/AP;
- d) provide intercept related information when the following events occur:
 - 1) when communication is attempted;
 - 2) when communication is established;
 - 3) when no successful communication is established;
 - 4) on change of status (e.g. in the access network);
 - 5) on change of service or service parameter;
 - 6) on change of location (this can be related or unrelated to the communication (e.g. at the beginning and end of a target's communications) or at all times when the apparatus is switched on);
 - 7) when a successful communication is terminated;
 - 8) on change of access network or access provider (e.g. when roaming).

NOTE 2: In the present document, service should be taken to include so-called supplementary services.

- e) provide intercept related information that shall contain:
 - 1) the identities that have attempted communications with the target identity, successful or not;
 - 2) identities used by or associated with the target identity;
 - 3) details of services used and their associated parameters;
 - 4) information relating to status;
 - 5) time stamps;
 - 6) location information (see also clause 4.2, bullet b, item 6));
 - 7) post dialled digits (see also clause 4.2, bullet h)), for voice/VoIP based communication.
- f) apply the conditions mentioned above also to multi-party or multi-way communication if and as long as the target identity participates, or depending on national laws, even if the target identity is not participating but the multi-party/multi-way communication is associated with the target identity.

4.4 Location information

An LEA may request location information relating to locations (see also clause 4.2, item b), bullet 6)), in a number of forms:

- a) the current geographic, physical or logical location of the target identity (either at the beginning and end of a target's communications, or during all phases of a target's communications, or independent of a target's communications), when communications activity (involving communication or a service) is taking place;