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

Lawful Interception (LI);
Requirements of Law Enforcement Agencies

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/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.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 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.

Foreword

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.

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:

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;

b) the current geographic, physical or logical location of the target identity, irrespective of whether communications activity (involving communication or a service) is taking place or not;

c) the current geographic, physical or logical location of an identity temporarily associated with a target service because of successful communication or an unsuccessful attempt to establish communication (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);

d) the current geographic, physical or logical location of an identity permanently associated with a target service (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).

NOTE: This information is expected to be made available from normal network operation.

4.5 Time constraints

a) A CSP shall make the necessary arrangements to fulfil his obligation to enable the interception and delivery of the result of interception from the point in time when the communication installation commences commercial service.

b) The above requirement applies accordingly to the introduction of modifications to the communication installation or to new operational features for existing communications services to the extent of their impact on existing interception capabilities.

NOTE 1: It is a national implementation (issue for negotiation) whether the operator does this proactively or passively after request of the LEA.

c) When a warrant is presented a CSP shall co-operate immediately.

NOTE 2: If a warrant is received during an ongoing call, depending on the intercept implementation, some operational problems might be experienced.

d) After a warrant has been issued, provision of the results of interception of a target identity shall proceed on a real-time or near real-time basis. In the case of near real-time the LEA should be able to force real-time (by means of emptying any buffers involved) if necessary.

4.6 Non-disclosure

4.6.1 Communications Service Provider

a) Information on the manner in which interception measures are implemented in a given communication installation shall not be made available to unauthorized persons.

b) Information relating to target identities and target services to which interception is being applied shall not be made available to unauthorized persons.

4.6.2 Manufacturers

The CSP shall agree confidentiality on the manner in which interception measures are implemented in a given communication installation with the manufacturers of his technical installations for the implementation of interception measures.

4.7 Information transmission and information protection requirements

The technical arrangements required within a communication installation to allow implementation of the interception measures shall be realized with due care exercised in operating communication installations, particularly with respect to:

a) the need to protect information on which and how many target identities are or were subject to interception and the periods during which the interception measures were active;

b) the restriction to a minimum of staff engaged in implementation and operation of the interception measure;

c) ensuring the clear delimitation of functions and responsibilities and the maintenance of third-party communications privacy, interception and recording shall be carried out in operating rooms accessible only by authorized personnel;

d) the result of interception shall be delivered through a handover interface;

e) no access of any form to the handover interface shall be granted to unauthorized persons;

f) CSPs shall take all necessary measures to protect the handover interface against misuse;

g) the result of interception shall only be transmitted to the LEMF as indicated in the warrant when proof of the authority to receive of the LEMF, and proof of the authority to send of the interface, has been furnished;

h) authentication and proof of authentication which shall be implemented as subject to national laws and regulations;

NOTE: This can be particularly relevant for material used in evidence. Use of cloud or virtualized technologies may introduce additional threats or challenges to the assurance of evidence. Suggestions for cryptographic mitigations are provided in ETSI TS 103 307 [i.2].

i) if no dedicated routes to the LEMF are used, such proof shall be furnished for each communication set-up;

j) depending on certain interception cases, LEAs may require confidentiality measures to protect the transmission of the results of such interception. The use of encryption shall be possible;

k) in order to prevent or trace misuse of the technical functions integrated in the communication installation enabling interception, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input. The records, which are subject to national regulation, shall cover all or some of:

   1) the target identity of the target service or target services concerned;

   2) the beginning and end of the activation or application of the interception measure;

   3) the LEMF to which the result of interception is routed;

   4) an authenticator suitable to identify the operating staff (including date and time of input);

   5) a reference to the warrant;

l) the CSP shall ensure that the records are tamper-proof and only accessible to specific nominated staff.

4.8 Internal security

The CSP shall configure the technical arrangements in his communication installation so as to enable the processing of intercepted material in accordance with applicable national laws within the issuing jurisdiction. Staff enabling the process of interception will be subject to the relevant national security regulations.

Protecting information requires the use of isolation techniques or secure enclaves (e.g. where virtualization or cloud-based solutions are used).

It will require particular attention in virtualization or cloud-based solutions to create and maintain restrictions on staff access in hardware and in software.

4.9 Unchanged state of service, etc.

a) Interception shall be implemented and operated in such manner that no unauthorized person can detect any change from the unintercepted state.

NOTE: This requirement is particularly relevant in a virtualized context. The undetectability requirement applies to unauthorized persons with access to the hypervisors running on the host hardware, as well as the providers/vendors of the host hardware.

b) Interception shall be implemented and operated in such manner that no communicating parties can detect any change from the unintercepted state.

c) The operating facilities of the target service shall not be altered as a result of any interception measure. The operating facilities of any other service shall not be altered as a result of any interception measure.

d) The quality of service of the target service shall not be altered as a result of any interception measure. The quality of service of any communications service other than the target service shall not be altered as a result of any interception measure.

4.10 Technical handover interfaces and format requirements

a) The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure.

NOTE: If a warrant is received during ongoing communication, depending on the intercept implementation, some operational problems might be experienced.

b) These handover interfaces need to be implemented in those communication networks for which the interception capability is required by national laws.

c) The configuration of the handover interface shall ensure that it provides the results of interception.

d) The configuration of the handover interface shall ensure that the quality of service of the communications traffic provided at the handover interface is not inferior to that offered to the target service for each particular call.

e) The configuration of the handover interface shall be such that that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

f) Each interception target shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.

g) The correlation between the content of communication and intercept related information shall be unique.

h) LEAs require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

i) If CSPs initiate encoding, compression or encryption of communications traffic, LEAs require the CSPs to provide intercepted communications en clair.

j) LEAs require CSPs to be able to deliver the intercepted communications to the LEMF via packet data connections.

k) The LEMF/LEA will be informed of:

1) the activation of an intercept measure;

2) the deactivation of the intercept measure;

3) any change of the intercept measure;

4) the temporary unavailability of the intercept measure.

4.11 Independence of the Communications Service Provider

a) A CSP shall ensure that the configuration of the installation is such that he can implement and operate each ordered interception measure:

   1) without any involvement of third parties; or

   2) with the minimum of involvement of third parties if 1) is not practicable.

b) A service provider or access provider shall ensure that:

   1) any network operator whose network is used by the service provider or access provider can co-operate in the provision of interception by the service provider or access provider, if required;

   2) any network operator involved in the provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorized target services to be intercepted;

   3) no other service provider or access provider is involved in the provision of interception facilities, unless that service provider or access provider is involved in the co-operative provision of service;

   4) any service provider or access provider involved in the co-operative provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorized target services to be intercepted.

c) A CSP shall not rely on another CSP or jurisdiction to ensure LI activity can occur. For example, a serving network shall not share LI target identities with a home network in the case of roaming or vice versa.

d) In the majority of cases, national regulation shall require LI activity is performed entirely within a particular legal jurisdiction.

e) There is a general requirement of LEAs that services provided to their home countries from technical facilities outside those home countries can be intercepted, as if they had been provided from the home country.

NOTE: A draft set of requirements addressing this specific case is given in clause E.3.

4.12 Temporary obstacles to transmission

a) When transmission to the LEMF of the content of communication is, in exceptional cases, not possible the remainder of the results of interception (e.g. intercept related information) shall nevertheless be provided to the LEA (see also clause 4.3, item d)).

b) Prevention of the interception of the content of communication is not permitted.

4.13 Identification of the identity to be intercepted

a) Where the special properties of a given service, and the justified requirements of the LEAs, necessitate the use of various identifying characteristics for determination of the traffic to be intercepted, the CSP shall ensure that the traffic can be intercepted on the basis of these characteristics.

b) The identifiers for the determination of a target can be:

   1) the network access identifier;

   2) the equipment identifier; or

   3) the service level identifier.

c) The CSP shall be able to perform interception based on long term or permanent identifiers associated with a target's network access, service or equipment, as identified by the LEA. To achieve interception, the CSP may need to translate these into further associated identifiers, in order to identify the data to be intercepted.

NOTE: LEAs will continue to need to specify the target of interception using long-term identifiers, such as IMEI or IMSI, even if the network uses other derived or temporary identifiers to identify the correct traffic due to the concealment of long-term identifiers for privacy reasons.

d) In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear determination of the traffic to be intercepted.

4.14 Multiple interception measures

a) The CSP shall ensure that more than one interception measure can be operated concurrently for one and the same identity. Multiple interceptions may be required for a single target service to allow monitoring by more than one LEA. Multiple interceptions for a single target service may also be required by the same LEA. The maximum number of simultaneous interceptions against the same target is network specific and should be defined (by national agreement).

b) If multiple interceptions are active, CSPs shall take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.

c) The multiple interception measures may require information according to different warrant.

d) The arrangements made in a network for the technical implementation of interception measures shall be set up, according to requirements, and configured so as to enable the elimination, without undue delay, of potential bottlenecks in a regional or functional part of that network when several interception measures are operated concurrently.

Annex A (normative): Detailed requirements of law enforcement agencies for circuit switched oriented communications networks and services

A.0 Overview

This annex consists of the requirements detailed for circuit switched oriented communications networks and services.

A.1 Details on clause 4.3, item d)

d) The CSP, shall in relation to each target service provide intercept related information:

1) when a call set-up is attempted;

2) when a call is established;

3) when no successful call is established (when a call attempt fails);

4) on change of status (e.g. in the access network);

5) on change of service or service parameter (e.g. activation of call forwarding);

6) on change of location, see also clause 4.2, item b), bullet 6);

7) when a successful call is terminated.

8) on change of access network or access provider (e.g. when roaming).

A.2 Details on clause 4.4

NOTE: This information is expected to be made available from normal network operation. An example of geographic location might be a cell identity in mobile networks, an example of physical location might be a subscriber access number in a fixed network and an example of a logical location might be a UPT number associated with a physical location.

A.3 Details on clause 4.7, items i) and j)

The technical arrangements required within a communication installation to allow implementation of the interception measures shall be realized with due care exercised in operating communication installations, particularly with respect to:

i) where switched lines to the LEMF are used, such proof shall be furnished for each call set-up;

j) depending on certain interception cases (e.g. satellite interception), LEAs may require confidentiality measures to protect the transmission of the results of such interception. The use of encryption shall be possible.

A.4 Details on clause 4.10, items a) and h)

a) The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure.

NOTE 1: If a warrant is received during an ongoing call, depending on the intercept implementation, some operational problems might be experienced.

h) LEAs require the content of communication to be provided across the handover interface in an agreed format:

1) the content of communications relating to two communicating parties is placed in two separate communications channels (also known as stereo mode);

2) other configurations appropriate to the target service concerned.

NOTE 2: Migration of the installed base might lead to a national requirement to support mono mode (instead of stereo) for a certain period.

Annex B (normative): Detailed requirements of law enforcement agencies for packet oriented communications networks and services

B.0 Overview

This annex consists of the requirements specific for packet oriented communications networks and services.

These requirements will be used to derive specific packet network and or service requirements and furthermore to standardize handover interfaces.

The requirements described in this part are focussing on packet-oriented networks and services.

Although most packet networks or service will be based on IP the requirements will also apply to X.25 and other networks or services. For the handover interface the option of tunnelling, e.g. X.25 on IP is considered to be a usual approach.

In the telephony networks a migration from analogue to digital has taken place. This migration went from the higher network levels (trunks and switches) to the subscriber lines. A second wave in these networks is the move from circuit switched to packet switched. The present document will take this wave also in account (e.g. VoIP, TISPAN).

Packet oriented access techniques fixed (e.g. dial in, ADSL, cable modems) and mobile (e.g. GPRS, UMTS, and mobile satellite systems) will be covered by the present document.

B.1 Details on clause 4.3, items d) and e)

The CSP shall, in relation to each target service:

d) Intercept related information shall be provided:

   1) when an access network attach/detach is attempted;

   2) when an access network attach/detach is established;

   3) when no successful access network attach/detach is established;

   4) when a service attach/detach is attempted;

   5) when a service attach/detach is established;

   6) when no successful service attach/detach is established;

   7) on change of status (e.g. in the access network);

   8) on change of service or service parameter;

   9) on change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on, see also clause 4.2, item b), bullet 6));

   10) on change of access network or access provider (e.g. when roaming);

NOTE 1: In the present document, service should be taken to include so-called supplementary services of access networks.

e) Intercept related information 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 (e.g. dial in calling line number and called line number, access server identity);

3) details of services used and their associated parameters;

4) information relating to status;

5) timestamps;

6) location information (as described in clause 4.2, item b), bullet 6));

7) post dialled digits, if required, for voice/VoIP based communication (see clause D.2.1).

NOTE 2: To avoid a need for IRI reports per datagram exchange (e.g. packet) the target communication and the delivery of this communication to the LEMF has to have very little time difference.

EXAMPLE: In the case of GPRS, IRI reports need to (at least) be sent at attach/detach (attempts) to the network, PDP-context activation/deactivation or location updates.

B.2 Details on clause 4.4

An LEA may request location information relating to locations, in a number of forms:

a) the current geographic, physical or logical location of the target identity, when communications activity (involving a datagram exchange or a service) is taking place;

b) the current geographic, physical or logical location of the target identity, irrespective of whether communications activity (involving a datagram exchange or a service) is taking place or not;

c) the current geographic, physical or logical location of an identity temporarily associated with a target service because of successful communication or an unsuccessful attempt to establish communication;

d) the current geographic, physical or logical location of an identity permanently associated with a target service.

B.3 Details on clause 4.7, item i)

i) If no dedicated routes to the LEMF are used, such proof shall be furnished for each set-up of a datagram exchange.

B.4 Details on clause 4.10, item a)

a) The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure.

NOTE: If a warrant is received during an ongoing datagram exchange, depending on the intercept implementation, some operational problems might be experienced.

Annex C (normative): Advanced services

Growing integration of Internet type of services/applications into communication networks and services could give ambiguity on what services are expected to be interceptable.

Communication services offered to subscribers in the marketplace as individual services are required to have an interception capability. These services can be broken down into peer-to-peer services and communication services supported by a provider. A carrier is not expected to be able to understand or perform analysis on peer-to-peer services which do not utilize service capabilities offered by a provider. However, any communication service offered by a carrier, including those that are used to support peer-to-peer services should be interceptable by the carrier.

In those cases where the interception in the access does not provide all information additional LI functions are necessary.

Individual countries may have a different approach to interception of these services dependent on their own legislative provisions.

A list of events that are of interest to law enforcement has been provided in annex D for voice and messaging services. Not all events apply to all services and the specific availability of these messages will depend on what capabilities a carrier provides to its subscribers. The remote access to a message server is communication and therefore an integral part of the service.

The combination of services can lead to even new services. The example list in annex D is not limiting but should be used to give guidance on the interception requirements for new services. The requirements in this annex with the examples in annex D are not new requirements but explanations of the requirements in relation to some services.

The word "call" is also used for the message flow.

Annex D (informative): Examples of advanced services

D.0 Overview

The events in this annex are examples of events that should be delivered, when reasonably available, as CC and IRI if a target is intercepted. This is not an exhaustive list.

D.1 General capabilities

D.1.1 Registration/authorization events

Law Enforcement has identified the need to intercept and report the following registration and authorization events:

- Address Registration;
- Address De-registration;
- Mobility Authorization;
- Mobility De-authorization.

D.1.2 Communication content events

Law Enforcement has identified the need to intercept and report the following communication content:

- Content Delivery Start;
- Content Delivery Change;
- Content Delivery Stop;
- Content Unavailable.

D.1.3 Feature management events

Law Enforcement has identified the need to intercept and report the following feature management:

- Feature Activation;
- Feature Deactivation;
- Feature Configuration.

D.1.4 Interception status events

Law Enforcement has identified the need to intercept and report the following interception status:

- Interception Activation;
- Interception Continuation;
- Interception Change;
- Interception Deactivation.

D.2 Voice capabilities

D.2.1 Call management events

Law Enforcement has identified the need to intercept and report the following call management:

- Call Origination;
- Call Termination Attempt;
- Call Answer;
- Call Release;
- Address Resolution;
- Call Admission Control;
- Media Modification;
- Signalling Events;
- Subject Signalling;
- Network Signalling;
- Post dialled digits.

D.2.2 Feature use events

Law Enforcement has identified the need to intercept and report the following feature use:

- Call Redirection;
- Party Hold;
- Party Retrieve;
- Party Join;
- Party Drop;
- Call Merge;
- Call Split.

D.3 Messaging capabilities

D.3.0 Overview

Message events could be accessed remote and handled on a server.

D.3.1 Message creation events

Law Enforcement has identified the need to intercept and report the following message creation events:

- Creation of message;
- Storing as draft message;
- Retrieving stored draft message;
- Sending of message;
- Deletion of draft message.

D.3.2 Message reception events

Law Enforcement has identified the need to intercept and report the following message reception events:

- Reception of message;
- Opening of message;
- Storing of message;
- Retrieving stored message;
- Deletion of message;
- Replying/forwarding message.

D.3.3 Automatic welcome or reply message management

Law Enforcement has identified the need to intercept and report the following Automatic welcome or reply message management events:

- Creation of automatic message;
- Modification of automatic message;
- Deletion of automatic message;
- Creation of condition for automatic message;
- Modification of condition for automatic message;
- Deletion of condition for automatic message.

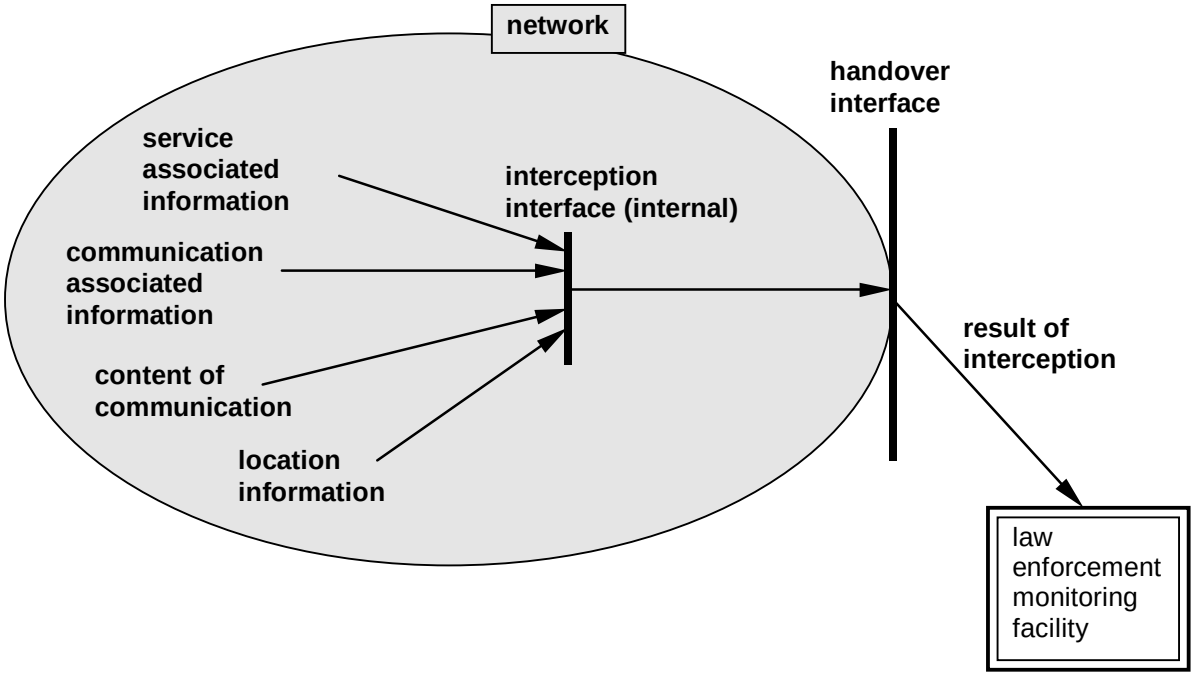
Annex E (informative): Explanatory diagrams

E.0 Overview

The diagrams provided in this annex are intended to be illustrative of the abstractions employed, and are not intended to limit the scope of the present document.

E.1 General network arrangements

The general arrangement for a network which is capable of providing interception facilities is as shown in figure E.1.



NOTE: An optional mediation device within the network may be required to convert the information according to national laws.

Figure E.1: General network arrangements for interception

Information relating to some target service is collected within the network at an interception interface. This information is then passed to an optional buffer, depending on specific circumstances, and then to a handover interface. From the handover interface information is then passed to the LEMF.

The information collected includes some or all of:

- the content of communication;
- communication associated data;
- service associated data;
- location information.

E.2 Service providers

A service provider is an entity which takes advantage of the connectivity offered by a network provider to offer some service which the network's connectivity on its own is otherwise incapable of providing. Depending on circumstance, a service provider may be part of the same organization which operates a network, or the service provider may belong to a different organization. The service provider relies on the co-operation of the network operator to deliver their service to their customer. The service provider may also provide some services with the assistance of other service providers.

The services which a service provider may offer are essentially unlimited. Possibilities include:

- voice storage services;
- personal numbers;
- card calling services.

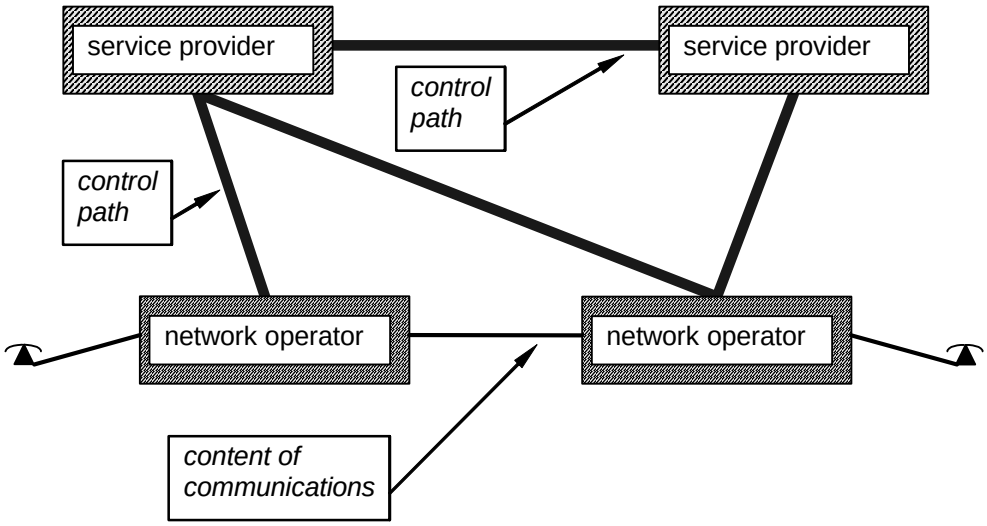


Figure E.2: Service provider relationship to a network operator

Figure E.2 shows that, in general, a service provider has no direct access to the content of communications.

E.3 Home country service from a foreign territory

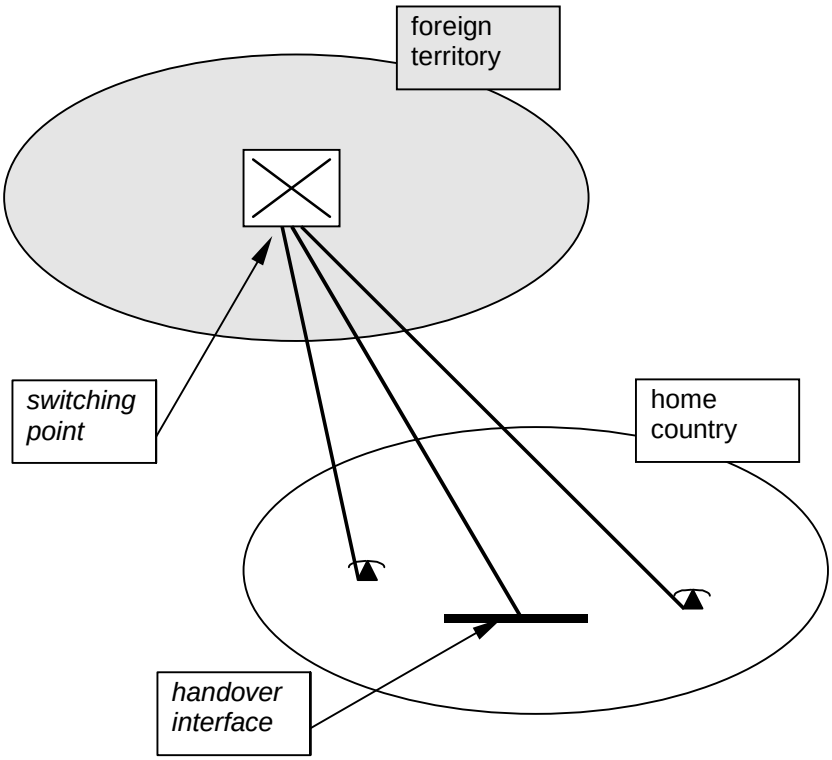


Figure E.3: Home country service, foreign territory switching

There may be a service provider involved, either in the home country or in a foreign territory, which need not be the same foreign territory that the switch point is located in.

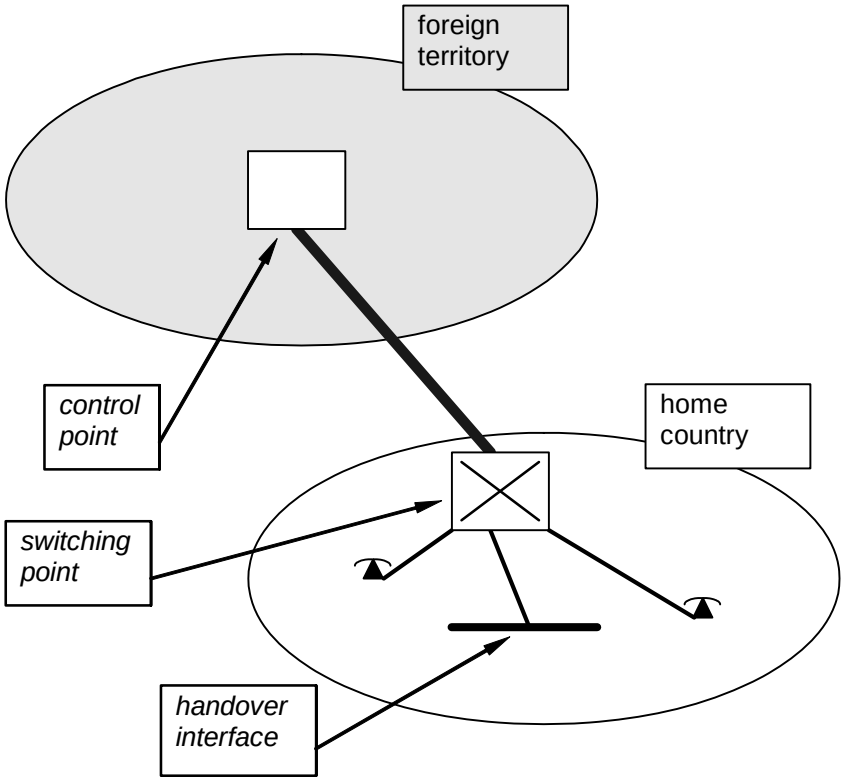


Figure E.4: Home country service, home country switching, foreign territory control

E.4 Identification of a target service

An LEA is concerned with a target as, generally, a specific person or persons. From the viewpoint of the CSP that target employs one or more target services. Associated with the target's use of each target service are one or more target identities. These relationships are shown in figure E.5.

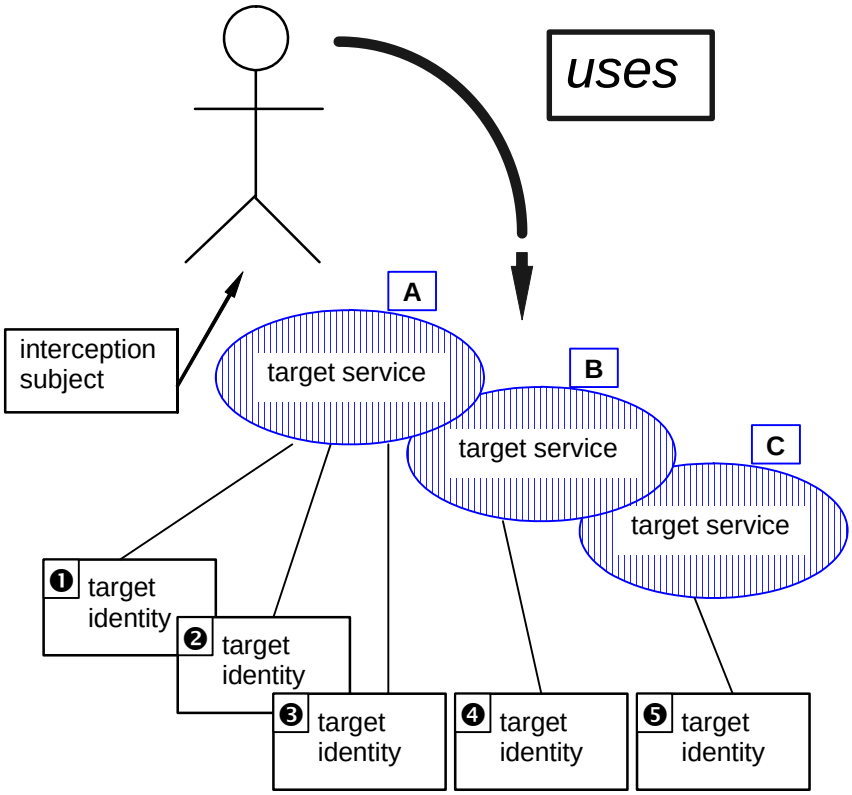


Figure E.5: Target service identification

A single target makes use of three services: A, B and C. When using service A, the target makes use of three identities: ❶❷❸. For service B, the target uses identity ❹. For service C, the target uses identity ❺.

The target identities for target service A could be three different e-mail addresses. Another target identity could be MSISDN, IMSI or IMEI in a mobile network.

Annex F (informative): Basic requirements for interception across national frontiers

As the communications market in Europe develops, more services will be provided across national frontiers, using terrestrial or satellite communication links. To address these circumstances further requirements will be necessary. Initial study suggests that at least the following are relevant.

A CSP providing service to a home country from a foreign territory including international space above earth including satellite operators and those providing service via satellite facilities has to make arrangements such that:

a) interception is possible relating to activity of a target identity within a specific national domain;

b) if the interception interface lies in a foreign territory, then arrangements (both technical and organizational) are made such that interception is possible as if the interception interface were located in the home country;

c) the act of interception is kept discreet;

d) any result of interception is kept confidential, possibly by the use of encryption;

e) any other party involved in the provision of interception facilities is aware of the least detail of operational activities possible;

f) observation of the networks and services involved will not disclose the act of interception;

g) observation of the networks and services involved will not disclose the identities involved in any activity relating to interception;

h) observation of the networks and services involved will not disclose any result of interception;

i) relating to each home country there has to be a legal entity on whom warrants can be served.

NOTE: The above requirements are subject to further review, particularly with regard to questions of extraterritoriality.

Annex G (informative): Change Request History

Status of the present document Requirements of Law Enforcement Agencies		
Date	**Version**	**Remarks**
May 2001	1.1.1	First publication of the TS after ETSI/SEC LI#28 (15 - 17 May 2001, Hamburg) approval.
May 2006	1.2.1	Included Change Request: TS101331CR001r3 (cat C) Adding advanced service information This CR was approved by TC LI#12 (9-11 May 2006, Lemesos)
February 2009	1.3.1	Included Change Request: TS101331CR002 (cat F) Inclusion of End Session IRI event This CR was approved by TC LI#20 (3-5 February 2009, Levi)
January 2014	1.4.1	Included Change Request: TS101331CR003r1 (cat B) Adding requirements on juridical domain This CR was approved by TC LI#35 (28-30 January 2014, Milan)
February 2017	1.5.1	Included Change Request: TS101331CR005r3 (cat C) on Clarifications of LI requirements This CR was approved by TC LI#44 (30 January - 1 February 2017 in Sophia Antipolis).
September 2020	1.6.1	Included Change Request: TS101331CR006r2 (cat F) Clarification on multiple interception measures This CR was approved by TC LI#55 (21 - 25 September 2020 e-meeting)
February 2021	1.7.1	Included Change Request: TS101331CR007r4 (cat F) Alignment of the terms target, warrant and CSP This CR was approved by TC LI#56 (15 - 19 February 2021 e-meeting)
June 2021	1.8.1	Included Change Request according temporary document LI(21)P57023r5 TS101331CR008r5 (cat B) Additional LEA Requirements This CR was approved by TC LI#57 (21 - 25 June 2021 e-meeting)

History

Document history		
Edition 1	December 1996	Publication as ETSI ETR 331 (withdrawn)
V1.1.1	August 2001	Publication
V1.2.1	June 2006	Publication
V1.3.1	October 2009	Publication
V1.4.1	February 2014	Publication
V1.5.1	March 2017	Publication
V1.6.1	October 2020	Publication
V1.7.1	March 2021	Publication
V1.8.1	July 2021	Publication