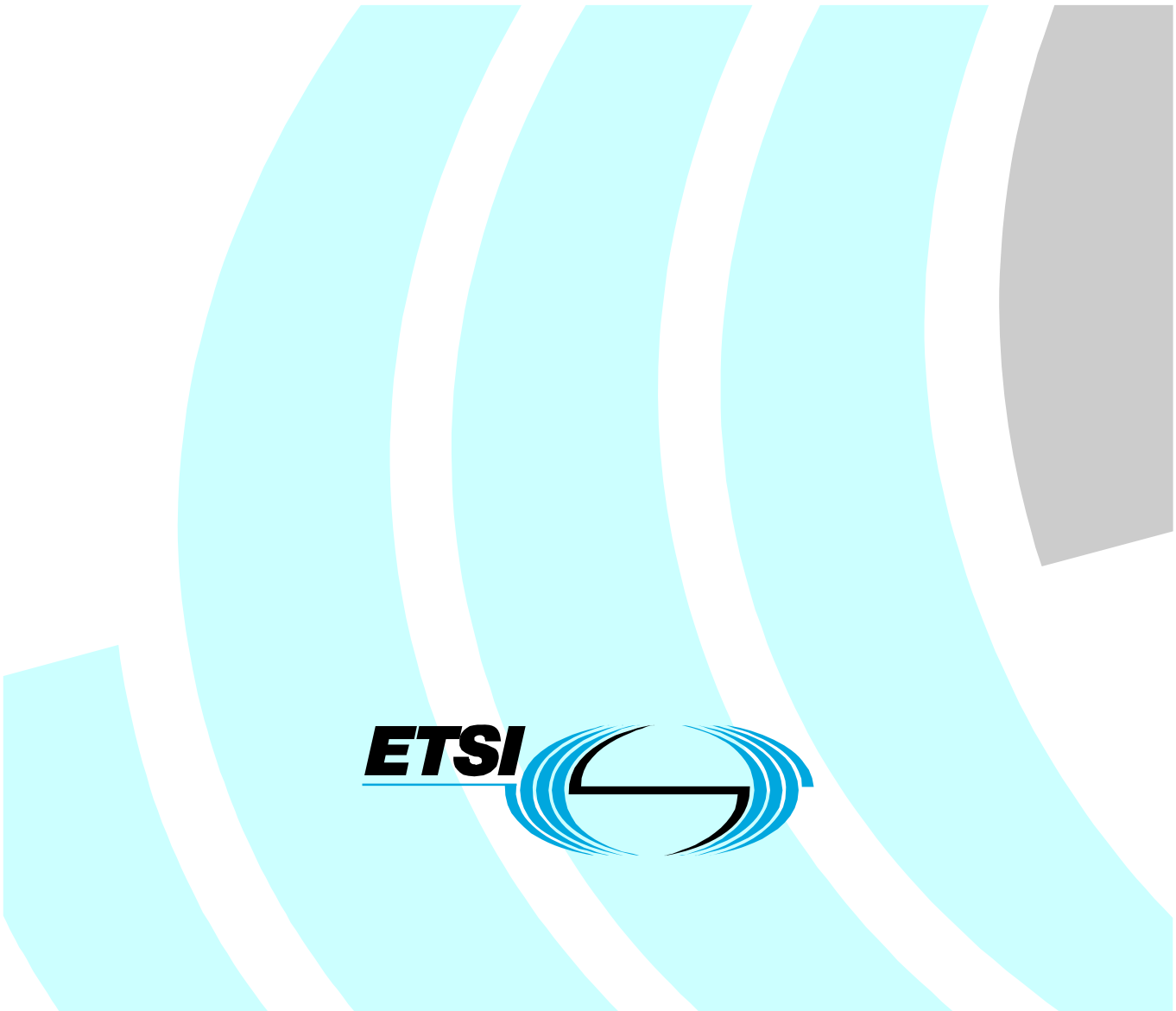
ETSI TS 102 656 V1.2.1 (2008-12)

Technical Specification

Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data



Reference
RTS/LI-00055

Keywords
handover, retention, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

Introduction

The EU Directive on Data Retention of 2006 [1] describes data to be retained from telecommunication systems and services. The Directive describes what data should be available for international (EU) exchange under mutual legal assistance treaties. The Directive therefore can also be seen as the mandatory set of data to be retained on a national basis.

The multi CSP, multi LEA and multinational aspect of the data retention resolution creates the need for a standardized requests and the delivery of the data. The present document describes similar to the requirements for lawful interception in TS 101 331 [2] the law enforcement needs for the request and delivery and related aspects of retained data.

The definition of a handover interface for the request and delivery should allow the technical facilities to be provided:

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

1 Scope

The present document gives guidance for the delivery and associated issues of retained data of telecommunications and subscribers. It provides a set of requirements relating to handover interfaces for the retained traffic data and subscriber data by law enforcement and other authorized requesting authorities. The requirements are to support the implementation of Directive 2006/24/EC [1] of the European Parliament and of the Council of 15 March 2006 on the retention of data.

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

The present document gives the requirements for the delivery of Retained Data (in line with TS 101 331 [2] for LI).

NOTE: Reading the present document it should be taken in account that:
This is an ETSI document and will not only apply to countries falling under the Directive (not only EU countries). Limitations in what data to be retained are a national issue. The present document and the Handover specification are not mandatory.
Where necessary the present document will clarify functionality of the Directive. The Directive text sometimes seems to combine issues from a telecom perspective. The Directive text might use ambiguous wording from a telecom perspective. Additional issues could be added to fulfil national requirements.

2 References

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

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

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

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

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

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

2.2 Informative references

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

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

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

Cell ID: identity of the cell from which a mobile telephony call originated or in which it terminated (Directive art. 2e)

Communication Service Provider (CSP): generic description covering Access Provider, Service Provider and Network Operator

Data: traffic data and location data and the related data necessary to identify the subscriber or user (Directive art. 2a)

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

lawful authorization: permission granted to an LEA under certain conditions to request specified telecommunications retained data and requiring co-operation from a network operator/service provider/access provider

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 an interception subject

quality of service: quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications 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

request criteria: identity associated with a retained data to be delivered

target identity: identity associated with a retained data to be delivered

telecommunications: any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo optical system

telephone service: calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services) (Directive art. 2c)

unsuccessful call attempt: communication where a telephone call has been successfully connected but not answered or there has been a network management intervention. (Directive art. 2f)

user: any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service (Directive art. 2b)

user ID: unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service (Directive art. 2d)

3.2 Abbreviations

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

CSP	Communication Service Provider
DSL	Digital Subscriber Line
EU	European Union
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HI	Handover Interface
HLR	Home Location Register
ID	IDentity
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISO	International Organization for Standardization
LEA	Law Enforcement Agency
LI	Lawful Interception
VLR	Visited Location Register
WLAN	Wireless Local Area Network

4 User (LEA) requirements

4.1 Introduction

This clause presents the user requirements related to the retained data of telecommunications 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) complies with the appropriate national requirements. A lawful authorization may specify a subset of requirements to be delivered on a case-by-case basis, this is based on the national regulation for different LEAs.

4.2 General requirements

a) The obligation of the Communication Service Provider (CSP) as to which data shall be retained and delivered is subject to national laws.

b) The obligation of the CSP as to which period the data shall be retained subject to national laws (see Directive art 7.b).

c) The CSP will be able to provide data of subscriber and subscriber related traffic data that was generated or processed within the retention period within its telecommunications system (also see Directive art. 3.2).

d) The CSP will be able to provide data received from other networks that was generated or processed (originated, terminated or forwarded) within the retention period within its telecommunications system.

e) The present document relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services (Directive Consideration 13).

f) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those providers, there is no obligation to retain them. There is no intention to harmonize the technology for retaining data, the choice of which is a matter to be resolved at national level (Directive Consideration 23).

NOTE 1: The retention of data applies to the use of services. This applies to subscribers, visitors, etc. of the service.

NOTE 2: The retention of data applies to all calls or services including those from roaming scenarios, e.g. mobile roaming records (ISO spec).

4.3 Requests

a) The requests for retained data can apply to:

   1) data generated or processed in association with communication or communication attempts (typically unsuccessful calls) (in accordance with particular national requirements);

   2) subscriber data.

b) The requests for retained data will be based on the request criteria defined in clause 4.4.

c) The request shall not require the CSP to make any subjective decisions, to use any judgement or discretion. In other words, requests shall be such that it is immediately clear whether a particular record matches the request.

d) The requests will be done by lawful authorization.

e) A lawful authorization can contain a combination of:

   1) a single request based on a single request criterion;

   2) multiple requests based on an aggregation of single request criteria;

   3) a request based on a range of request criteria.

NOTE: A request that conforms to the ETSI standard should not be assumed to be lawful under all jurisdictions. The delivery interface is not required to provide such a guarantee. It is assumed that national and international procedures are also in place to assure that the request is lawful.

4.4 Request for retained data

a) The request criteria for retained subscriber data shall contain the time stamp or time window and can be based on:

   1) a service or network identifier:

      i. network or service address (for example E.164, IP address, email, uri);

      ii. equipment identifier (for example IMEI, Directive art. 5.1.e);

      iii. network element (for example base station Global CellID); or

2) a name:

A name identifying for example the subscriber or registered user of the CSP; or

3) an address:

The address can be a subscriber address, billing address, directory address etc. known to the CSP.

b) The request criteria for retained data in association with communication or communication attempts shall be based on a time window and can be based on:

1) a number, the source, destination and or intermediate identity (influenced by users, IMSI, IMEI); or

2) location information (e.g. a base station identification, xDSL address, geographical grid reference).

NOTE 1: The base station identification can be the direct cell-id or other coordinates (GPS, zip, etc) that correlate to the associated cell-ids.

NOTE 2: As new services evolve, the standard should not exclude other items as the basis of requests for subscriber or communication information.

NOTE 3: The intermediate identities particularly apply to Call forwarding and email exploders.

NOTE 4: Which questions are legal and the elements they contain are in accordance with particular national requirements.

4.5 Delivery

a) In accordance with the relevant lawful authorization a CSP shall ensure that:

1) the entire data set specified in the lawful authorization is delivered;

2) the resultant generated from the request shall not be retained after successful delivery to the LEA;

3) a record of the received requests is kept to make audit trails possible (Directive art. 7 and 9).

b) The CSP will be able to provide data in such a way that any data that does not fall within the scope of the lawful authorization shall be excluded by the CSP.

c) All data provided as a result at the handover interface shall be given a unique correlation to the request and lawful authorization.

d) The CSP will provide information on known omissions in correlation with the data provided to the LEA (e.g. unavailable data in certain periods, start of retention).

4.6 Content of delivery

The data to be retained will be defined by national law. No content of communications shall be delivered. The delivery mechanism shall support (Directive art. 5 and other input):

a) data necessary to trace and identify the source of a communication:

1) network or service number(s) (for example E.164, IMSI, IP address, email address, uri);

2) equipment identifier (for example IMEI);

3) network element (for example base station CellID);

4) the name(s) and address(es) of the subscriber or registered user(s) and user ID(s) and national elements (for example user, account, directory).

b) data necessary to identify the destination of a communication:

1) network or service number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed (for example E.164, IMSI, IP address, email, uri);

2) equipment identifier (for example IMEI);

3) network element (for example base station Global CellID);

4) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID(s) and national elements (for example user, account, directory) of the intended recipient of the communication.

c) data necessary to identify the date, time of start and end or duration of a communication depending on the service:

1) the date and time of the start and end of the communication;

2) the date and time of the log-in and log-off of the service, based on a certain time zone.

NOTE 1: The most accurate time is desirable, preferably synchronized with a common time reference.

d) data necessary to identify the type of communication depending on the service:

1) supplementary services, teleservices and bearer services used and their associated parameters as available;

2) information relating to status;

3) Internet service used.

e) data necessary to identify users' communication equipment or what purports to be their equipment depending on the service:

1) calling and called numbers;

2) IMSI of the calling and called party, (the relevant IMSI which meets the search request will be provided, to get the second ID an additional request might be necessary);

3) IMEI of the calling and called party, (the relevant IMEI which meets the search request will be provided, to get the second ID an additional request might be necessary);

4) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

5) in the case of pre-paid anonymous services, the date and time of the credit updates and the location label (Cell ID) from which the service was activated (national option);

6) the calling telephone number for dial-up access;

7) the Digital Subscriber Line (DSL) or other end point of the originator of the communication.

NOTE 2: Several requesting steps might be needed.

f) data necessary to identify the location of mobile communication equipment:

1) the location label (e.g. Cell ID) at the start of the communication;

2) data identifying the geographic location of cells by reference to their location labels (e.g. Cell ID) during the period for which communications data are retained;

3) physical or IP address for WLAN communication (the physical address could be a postcode).

g) data of attempted communication (in accordance with particular national requirements);

h) data of established communication;

i) data of not successful established communication (in accordance with particular national requirements);

NOTE 3: It is not required to retain data relating to unconnected calls (Directive art. 3).

j) data on the status and updates (e.g. in the access network) (like logged on independent of communication) (in accordance with particular national requirements);

k) data on the service or service parameter and updates (like Supplementary Services independent of communication, e.g. forwarding) (in accordance with particular national requirements);

NOTE 4: It is advised to retain samples of cell-ids at regular time intervals during cellular telephony communication. The sampling interval is to be set to a value that is large enough to avoid massive storage of location data, but short enough to allow tracing of how the handset has moved during a communication session. A suitable value might for instance be GSM/GPRS idle mode location HLR/VLR update timers.

l) data on change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on based on national requirements. This might be on a periodic basis.) (this is for particular national requirements);

m) the conditions mentioned above also apply to multi-party or multi-way (in accordance with particular national requirements).

NOTE 5: Multi-party and multi-way particularly applies to conference call and email exploder.

4.7 Location information

Data on location information may be available in a number of forms:

a) the geographic, physical or logical location of the target identity, when telecommunications activity (involving communication or a service) is taking place;

b) the geographic, physical or logical location of the target identity, irrespective of whether telecommunications activity (involving communication or a service) is taking place or not (in accordance with particular national requirements);

c) the geographic, physical or logical location of an identity temporarily associated with a target service because of successful telecommunication or an unsuccessful attempt to establish telecommunication (in accordance with particular national requirements);

d) the geographic, physical or logical location of an identity permanently associated with a target service (in accordance with particular national requirements).

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

4.8 Availability constraints

a) A CSP shall make the necessary arrangements to fulfil his obligation to enable to retain and deliver data from the point in time when the telecommunication installation commences commercial service.

NOTE 1: The above requirement applies accordingly to the introduction of modifications to the telecommunication installation or to new operational features for existing telecommunications services to the extent of their impact on existing data retention and delivery capabilities.

b) When a lawful authorization is presented a CSP shall co-operate without undue delay (Directive art. 8).

c) After a lawful authorization has been issued, the results shall be delivered as soon as possible (service level agreement are a national issue).

d) CSP will retain data in such a way that the data retained and any other necessary information relating to such data can be delivered upon request to the competent authorities without undue delay (Directive art. 8).

NOTE 2: The above requirements c) and d) should also be seen with the technical background of the amount of data which had to be handled and delivered. As consequence out of this the response on a request could take a while.

4.9 Information transmission and information protection requirements

The obligations incumbent on service providers concerning measures to ensure data quality and their obligations concerning measures to ensure confidentiality and security of processing of data apply in full to data being retained (Directive Consideration 16).

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

a) the need to protect information on which and how many requests are or were made on retained data and the periods during which the information was requested;

b) the restriction to a minimum of staff engaged in implementation and operation of the handling of requests;

c) the result of a request for retained data shall be delivered through a handover interface;

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

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

f) the requested data shall only be transmitted to the LEA as indicated in the lawful authorization when mutual authentication over the hand over interface has been furnished;

g) authentication and proof of authentication shall be implemented subject to national laws and regulations;

h) if no dedicated routes are used, proof of authentication shall be furnished for each communication set-up;

i) confidentiality measures to protect the transmission of the results may be required. The use of encryption shall be possible;

j) in order to prevent or trace misuse of the technical functions integrated in the telecommunication installation, requests shall be fully recorded, including any application caused by faulty or unauthorized input. The records, which are subject to national regulation, shall cover all or some of:

   1) the request criteria of the request;

   2) the time or time window of the request;

   3) the delivery address of the result of the request;

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

   5) a reference to the lawful authorization.

k) the CSP shall ensure that the records as a result of a request are tamper-proof and only accessible to specific nominated staff;

l) all national regulations, procedures and processes shall be followed and are not replaced or superseded by requirements in the present document.

4.10 Internal security

The CSP shall configure the technical arrangements in his data retention installation so as to enable the processing of requests for retained data in accordance with applicable national laws. Staff enabling the process will be subject to the relevant national security regulations.

4.11 Technical handover interfaces and format requirements

a) The delivered information shall be delivered according to an open format and encoding.

b) These handover interfaces need to be implemented in those networks where required by national laws.

c) The configuration of the handover interface shall ensure that it provides the requested data set.

d) The configuration of the handover interface shall ensure that the quality of service meets national requirements (bandwidth, delay configurations, etc). The data volumes required over the interface are to be decided on a national basis although there shall be an expectation that the interface will not solely be used for requests resulting in the delivery of individual records.

e) The configuration of the handover interface shall be implemented with standard, generally available transmission paths, protocols and coding principles.

f) Each request shall be uniquely associated with the resulting data set delivered over the handover interface.

g) The correlation associating data within one data set shall be unique.

h) The network layers used for the hand over interfaces will be according to national law.

i) The hand over interface will support reporting for example fault, not available, not applicable, unclear reporting. It shall be possible to detect when transfer of information is unavailable or unsuccessful. The protocols adopted shall be resilient to transmission impairment.

j) The hand over interface shall support architectures with trusted third parties at the providers and/or law enforcement side.

4.12 Temporary obstacles to transmission

a) When transmission to law enforcement, in exceptional cases, is not possible the results shall be delivered as soon as the connection has been re-established.

b) Prevention of the delivery of requested data is not permitted.

4.13 Identification of the request criteria

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 data set, CSP with the LEA shall ensure that the data set can be delivered on the basis of these characteristics.

b) In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear determination of the data set to be delivered.

4.14 Multiple requests

a) The CSPs shall be able to handle the number of requests in accordance to national agreements.

b) The hand over interface shall be able to handle the number of requests in accordance to national agreements.

c) With multiple requests the CSPs shall take precautions to safeguard the identities of the requesting agencies and ensure the confidentiality of the investigations.

d) The multiple requests may require information according to different lawful authorizations.

e) The arrangements made in the retained data system and the hand over interface shall be set up, according to requirements, and configured so as to enable the elimination, without undue delay, of potential bottlenecks when several requests are handled concurrently.

Annex A (informative): Administrative requirements

A.1 Non disclosure

A.1.1 CSP

a) Information on the manner in which data retention is implemented in a given telecommunication installation shall not be made available to unauthorized persons.

b) Information relating to request criteria, target identities and target services to which requests have been issued shall not be made available to unauthorized persons.

c) National non-disclosure regulations and procedures shall be followed and are not superseded or replaced by requirements in the present document.

d) 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 data by the service provider or access provider, if required;

   2) any network operator involved in the provision of data is given no more information relating to operational activities than is strictly necessary to allow the request to be handled;

   3) no other service provider or access provider is involved in the provision of data, 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 data is given no more information relating to operational activities than is strictly necessary to allow the request to be handled.

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

A.1.2 Manufacturers or 3rd party providers

The CSP shall agree confidentiality on the manner in which data retention is implemented in a given installation with the manufacturers of his technical installations, subject to meeting the national regulations and procedures.

Annex B (informative): Categories of retained data sets

B.1 Introduction

In the present document three categories of retained data are specified:

- Mandatory set according to EU directive.
- Extended data set according to ETSI.
- National options and extensions to data sets.

B.2 Mandatory set according to EU directive

In the EU directive for data retention a number of parameters are specified per service and technology category. Apparently not all of these can be collected in a single place at the same time. Availability of data also depends on how the networks are set up and interconnected.

Regardless of such case-by-case limitations, the set of parameters in the EU directive should be considered as a minimum requirement. As far as possible, limitations should be specified and agreed on in order to clarify what is required from case to case.

B.3 Extended data set according to ETSI

In the course of work within TC LI on a handover interface specification, it is likely that a number of additional parameters will be defined. It would then be up to national regulations to decide how much of this is to be required as a minimum in addition to the set that is required by the EU.

B.4 National options and extensions to data sets

It is likely that special conditions on national levels will call for additional data to be retained. This may be introduced for instance as national options in the standardized set or as extensions in the data definitions.

Annex C (informative): Change Request History

Status of the present document Requirements of Law Enforcement Agencies for handling Retained Data		
Date	**Version**	**Remarks**
October 2007	1.1.1	First publication of the TS after approval by ETSI/TC LI16 (2-4 October 2007, Berlin) Version 1.1.1 prepared by Koen Jaspers (PIDS) (rapporteur)
December 2007	1.1.2	Re-published due to editorial correction on the title
October 2008	1.2.1	Included Change Request: TS102656CR001 (cat F) on Corrections of specific references, definitions and text This CR was approved by TC LI#19 (30 September - 2 October 2008 in Prague). Version 1.2.1 prepared by Koen Jaspers (PIDS) (rapporteur)

History

Document history		
V1.1.1	November 2007	Publication
V1.1.2	December 2007	Publication
V1.2.1	December 2008	Publication