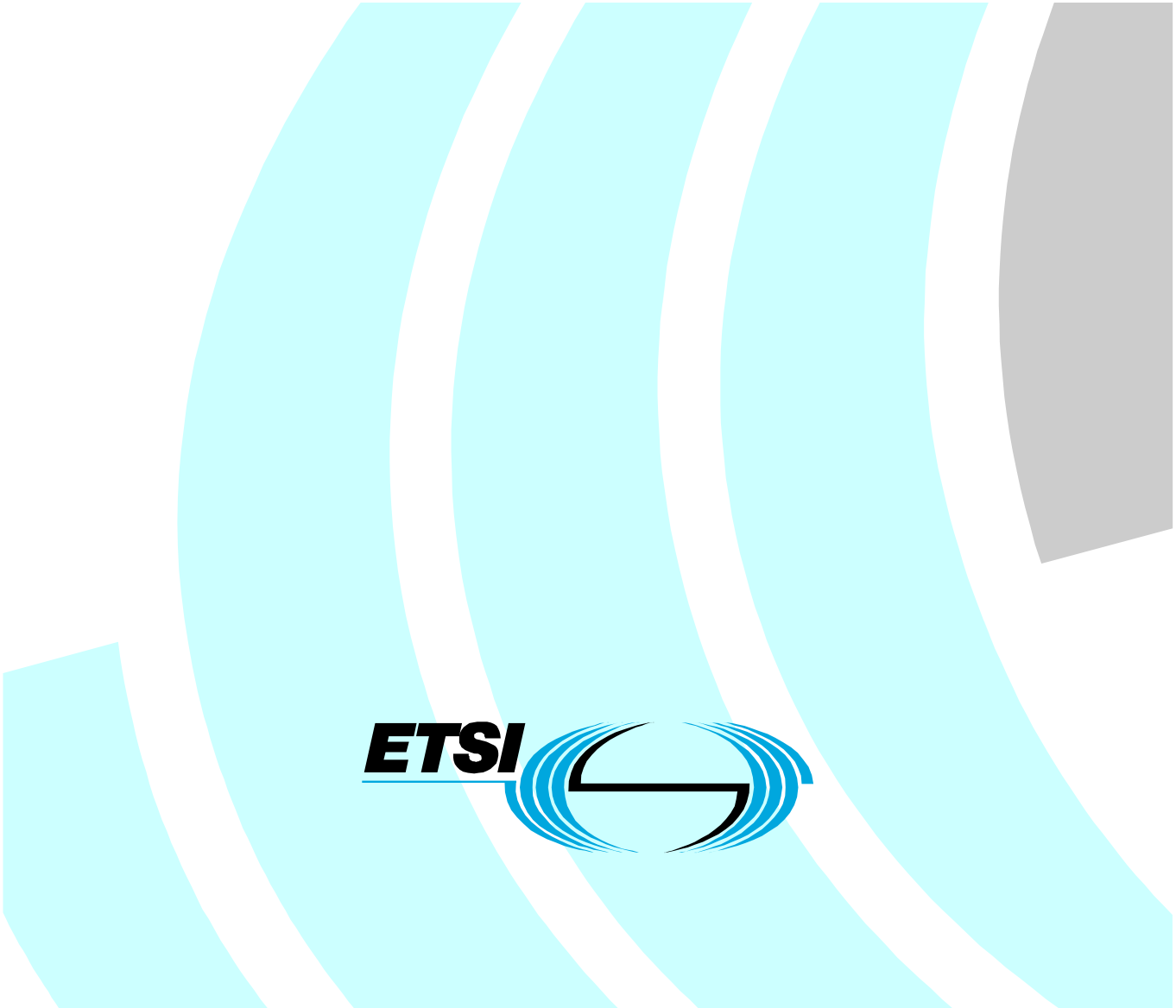
ETSI DTS/LI-00033 V0.4.03.1 (2007-64)

Technical Specification

OUTCOME TC LI RAP 165

Retained Data;
Handover interface for the request and delivery of retained data



Reference
RTS/LI-00033

Keywords
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).

1 Scope

The present document contains handover requirements and a handover specification for the data that is identified in EU Directive 2006/24/EC on retained. data [1]. The handover requirements from DTS/LI-00039 [3] are derived from the requirements contained in and implied by the EU Directive and by other national legislations. The present document considers both the requesting of retained data and the delivery of the results.

The present document defines an electronic interface. An informative annex describes how this interface may be adapted for manual techniques. Apart from in annex X, the present document does not consider manual techniques

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

[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] TS 101 232-01: “Handover interface for the lawful interception of telecommunications traffic IP Delivery”

[3] DTS/LI-00039

[4]

3 Definitions and abbreviations

3.1 Definitions

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

Handover Interface A (HI-A): the administrative handover interface comprising of Requests of information and their responses.

Handover Interface B (HI-B): the data handover interface comprising the retained data transmission of information.

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

number: any address (E.164, IP, email, uri) used for routing in a network or in a service on a user level or network/service level.

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 for information: a request from a **requesting authority** to a CSP for data retained.

Response to request of information: a response from the CSP to the **requesting authority** acknowledging or rejecting a **request for information**

Retained Data Record: a set of data elements for a specific subscriber/user related to a specific service transaction (Details to be determined).

Requesting Authority: any entity possessing the necessary jurisdiction and authority pursuant to law to compel a service provider to deliver retained subscriber information or traffic data specified in a query.

Service Transaction: an instance of a service given by an CSP to a subscriber/user.

Service Transaction Record: a set of data elements describing a service transaction (details to be determined).

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

Transmission of information: the transmission of retained data from the CSP to the **requesting authority**

3.2 Abbreviations

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

ADSL	Asymmetrical Digital Subscriber Line
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
RDH	Retained Data Handover
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 Overview of handover interface

4.1 Reference model

The generic Handover Interface adopts a two-port structure such that administrative request/response information (HIA) and Retained Data Information (HIB) are logically separated.

Figure 1 is the reference model for the request and transmission of retained telecommunications data.

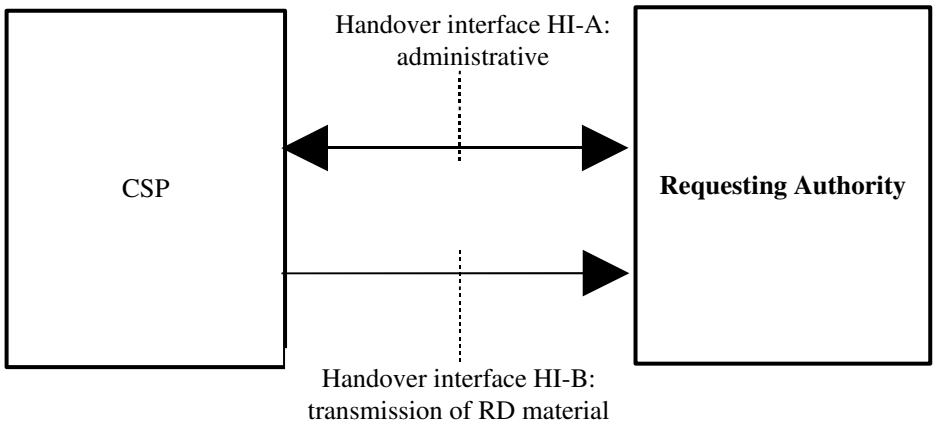


Figure 1: Functional Block diagram showing handover interface HI

4.2 Structure of document and applicable communication domains

The present document defines a framework that applies to all Retained Data. The present document defines a range of services (as shown in figure 2). The present document contains one annex for each service (Annex B onwards). For each service, the present document defines the "scope" of the service.

Services are defined:

1. On the basis of application-level functionality i.e. facilities the user may take advantage of in a uniform way, regardless of how it is implemented.
2. A service may also be defined as a transmission capability defined at the network level. Cf EC directive 2006/58 article 1 and article 5(c)(3)(ii).

NOTE: An example of an application-level service would be a telephony service offered either via CS or PS networks. An example of a network-level service would be a major operator offering routing or protocol conversion capabilities between local networks (belonging to, for instance, a company with interconnected local offices).

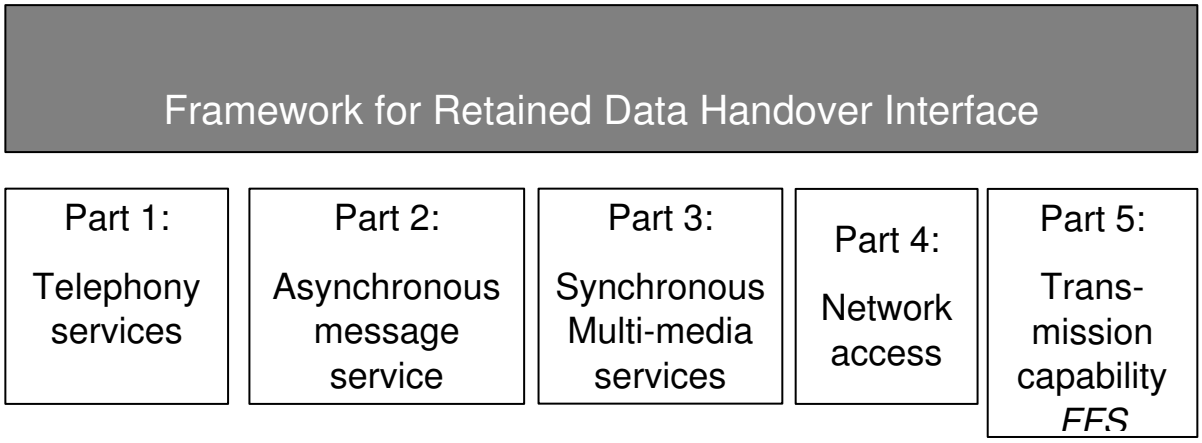


Figure 2: Framework structure

The present document is extensible: additional services may be added in future.

NOTE: When adding future services it is important to ensure that the service definitions are clear and distinct i.e. no overlap in the scope of the different services. However, it will be possible for services re-use common fields or structures from other services e.g. the present document has one definition of the structure for a person's name or address.

~~A framework structure is proposed similar to TS 102 232-01 [2], in which future services can be added as required, refer to Figure 2. It is proposed that each service be put into a separate Annex, although it could considered that separate standards be developed for each service (e.g. TS xxx xxx Part 1, Part 2, Part 3).~~

The framework defines the message procedures, the identifying and header information for each message, data exchange techniques, and security measures. Each service-specific standard will define the information that is available within that particular service.

EDITOR'S NOTE: Make it clear where each technology sits: PSTN/ISDN, GSM, GPRS, etc.

4.3 Breakdown into categories

Retained Data is broken down into the following categories:

- Subscriber data: information relating to a subscription to a particular service (e.g Name, Address)

  NOTE: Consider separating "personal information" (name, address) from "user identity" (phone number, email address), as one person may have multiple user identities.

- Usage data (or Traffic Data, Billing Data): information relating to usage of a particular service (e.g. Call Records)
- Equipment data: information relating to a device or handset.
- Network element data: information relating to a component in the underlying network infrastructure (e.g. location and identifier of a GSM base station) (for example, if this is not available from the usage data).
- Additional service usage: information relating to additional services used (e.g. DNS)

Each service shall break down its information into the categories listed above. There shall be no information outside of the above categories. For certain services, particular categories may not apply.

Future categories may be added a later date.

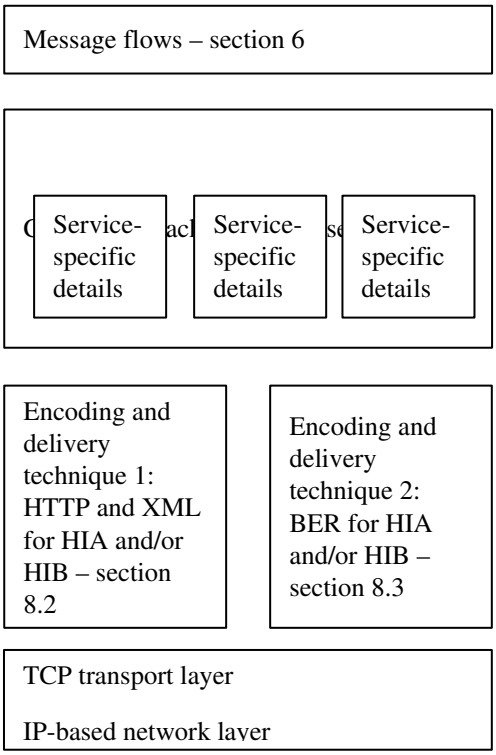
4.4 Handover Interface port 1 (HI-A) and Handover Interface port 2 (HI-B)

The Handover Interface port 1 (HI-A) shall transport various kinds of administrative, request and response information from/to the Requesting Authority and the organization at the CSP, which is responsible for Retained Data matters.

The Handover Interface port 2 (HI-B) shall transport the retained data information from the CSP to the Requesting Authority.

The HIA and HI-B interfaces may be crossing borders between countries. This possibility is subject to corresponding national law and/or international agreements.

4.5 Protocol stack used for the RDHI



6 Handover interface message flows

6.1 Successful delivery

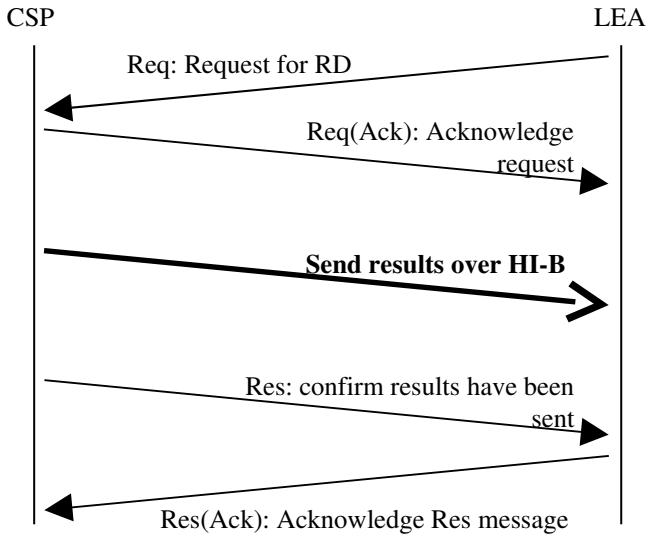
The following stages constitute a successful delivery:

- Request message (Req): The LEA sends a request for RD information
- Request acknowledgement (ReqAck): W~~ith no checking or validation, and w~~ithout undue delay, the CSP acknowledges it has received a message from the LEA. The CSP is now under obligation to work on the given request and the request is said to be "active".
- The CSP assembles a set of information that it believes to be a complete response (i.e. fully meets its obligation), and it is delivered over HI-B (the delivery address and other parameters for the delivery have

been agreed in advance or were specified in the Req). *If there are no records meeting the request criteria, a response shall still be sent, containing zero records.*

- Response (Res): The CSP signals over HI-A that the results have been delivered, and that the CSP considers the results to be complete.
- Response acknowledgement (ResAck): W~~ith no checking or validation, and w~~ithout undue delay, the LEA acknowledges it has received a Res message from the CSP. The CSP is now no longer under obligation to do further work on the given request and the request is no longer "active".

It may be that, after checking and validation, the LEA decides that the results from the CSP are not complete or accurate. This is handled under section 2.6.



NOTE 1: The HI-B and HI-A Response message may be combined at lower levels (see section x.x)

NOTE 2: The acknowledgements are required to be generated at an application level i.e. the CSP or LEA application is confirming receipt of the message. A transport level acknowledgement (e.g. TCP ACK) is not sufficient.

EDITOR'S NOTE: update for HTTP and check

6.2 Basic error situation

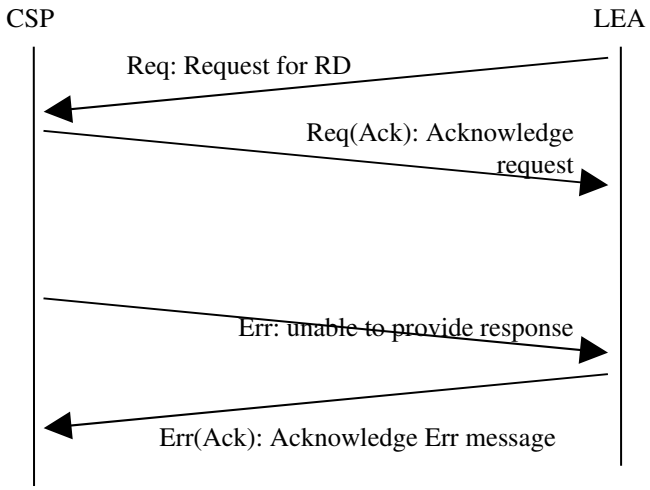
If the CSP is unable to process an active request for technical reasons (e.g. badly formatted request, authorisation not verified, unable to use the HI-B), then they shall send an error message as follows:

- Error (Err): The CSP sends an error message indicating that it is unable to provide a response to the request.

  NOTE: if the request is valid but creates no answers, then this is not an error condition.

- Error Acknowledgement (ErrAck): W~~ith no checking or validation, and w~~ithout undue delay, the LEA acknowledges it has received an Err message from the CSP. The CSP is now no longer under an obligation to do further work on the given request and the request is no longer "active".

The CSP is required to co-operate in resolving the error and it is likely that the request is re-issued (perhaps with some changes); however, from the point of view of the present document, all further messages will be handled manually or as a brand new request (see section 2.6).



6.3 Cancellation

The LEA may invoke a cancellation messages for any of its own active requests as follows:

- Cancel: For any active request, the LEA may issue a Cancel message.
- Cancel acknowledgement (CancelAck): W~~ith no checking or validation, and w~~ithout undue delay, the CSP acknowledges it has received the Cancel message. The CSP is now no longer under an obligation to do further work on the given request and the request is no longer "active".

NOTE: Only "active" requests may be cancelled. If the CSP receives a cancel message after responding, they may indicate this as an error to the LEA (see section 6.6)

6.4 Interim messages

An interim response is a message from the CSP to the LEA describing the current status of an active request. The use of interim responses is optional for agreement at a national level. The interim response includes some or all of the following information:

- A statement of the number of records found so far.
- A delivery of the information found so far.
- If agreed nationally, other information may be sent including estimates of how many records will be found or when they might be ready.

Interim responses are optional and are sent under conditions to be agreed nationally. Such conditions would typically be similar to the following:

- Time T has passed since the request.
- N records have been found that meet the request so far.
- The LEA chooses to make a request for an interim response.

There are therefore the following messages:

- Request for interim information (InterimReq): The LEA sends a request for an interim response, stating whether they want the delivery of records found so far or just the number.
- If delivery is required, then it is sent over HI-B. All records that are sent now shall then not be re-sent as part of the final delivery.
- Interim response message (InterimRes): The CSP sends an InterimResponse message containing the required information. If delivery is required, the InterimRes message shall be sent after the delivery is complete. Delivery of an interim response shall not generate a Res(Ack) from the LEA.

6.5 Error conditions

Many other error situations are possible. It might be the case that the LEA does not consider the “complete” answer from the CSP to be complete. It might be the case that the LEA cannot understand certain parts of the answer. In order to resolve these situations, it will be necessary for the LEA and CSP to discuss the matter person-to-person and this is not covered by the present document. Once any problems have been resolved, if the original request is still relevant, the request should be re-sent by the LEA (using a new request number i.e. completely independent of the previous request).

7 Definition of the elements for Retained Data messages

7.1 Information elements present in each message

The following table summarises the fields that shall be present in each of the messages defined in section 6. Those fields marked M are mandatory.

Message name	**Message abbreviation**	**Basic header info (section 7.2)**	**Other information (section 7.3)**	**A retained data request (section 7.5)**	**A retained data response (section 7.4)**
Request	Req	M	Optional:	M	-

			delivery information Optional: priority information		
Request acknowledgement	ReqAck	M	-	-	-
Error	Err	M	Error information	-	-
Error acknowledgement	ErrAck	M	-	-	-
Cancel	Cancel	M	-	-	-
Cancel acknowledgement	CancelAck	M	-	-	-
Interim request	InterimReq	M	Type of request, request number	-	-
Interim response	InterimRes	M	Request number, response number, status info.	-	-
Response	Res	M	-	-	-
Response acknowledgement	ResAck	M	-	-	-
HI-B message	-	M	Record number	-	M

7.2 Basic header information

7.2.1 RequestID

Each request (and its response) should have a RetainedDataRequestID, which distinguishes that request from any other on an international level. To do this, the request ID must contain:

- a country code (to indicate the country of the body making the request);
- an LEA code (assignable within the given country to distinguish between different LEAs);
- a unique reference number (assignable by the LEA). [LEAs will need to ensure they have warrants or other authorisation held against each request reference number].

7.2.2 CSP Identifier (CSPID)

A CSP ID shall be agreed on a national basis. CSP IDs shall not be repeated within the same country (i.e. shall not be repeated within the same country code, as given in the request ID). The LEA and CSP shall agree a CSP ID before any RDHI requests are made. Each request shall contain the CSP ID. If a CSP receives a request which does not have their own CSP ID, they shall signal an error (see section 6.3). The CSP ID shall be included in all further HI-A and HI-B messages.

NOTE1: it is not a NetworkElement ID and does not refer to exactly where in any network the info came from.

NOTE2: If there is already a scheme of identifiers defined that is unique for CSPs in a given country, it is recommended that this is re-used.

For further study: A given CSP may be related to other CSPs (e.g. owns them, carries their traffic, they are different parts of the same company). Subject to agreement between LEA and CSP, the LEA may make retained data requests against other related CSPs. In this case, the LEA shall indicate “Additional CSPs” to be included in the search, through a list of extra CSP IDs. In this case, the response shall indicate from which CSP the data came (FFS).

7.2.3 Timestamp

The time the message was created shall be included in the message.

Timestamps shall either be given in UTC-Z time, or the difference from UTC-Z time shall be specified. All timestamps shall contain the time and date.

7.3 Other information

7.3.1 Information in interim requests

An interim request message shall contain:

- Request type: whether it is required that the records found so far are delivered, or whether just a summary is required.
- Request number: Each InterimReq message shall be given a request number by the LEA, which shall increment for each interim request made against the particular Req in question. The first InterimReq sent against a given Req shall have request number equal to 0.

7.3.2 Information in interim responses

An interim response message shall contain:

- Number of records found so far
- For further study: Estimate of how the processing is progressing (estimated total number of records matching the request, estimate of the time when the response will be complete).
- If the response was generated in response to an interim request from the LEA, then the response shall quote the request number stated in the interim request.
- Response number: each response shall be given a response number by the CSP, which shall increment for each interim response sent. The first shall be given response equal to zero. This number is independent of the request number.

7.3.3 Record number

Each retained data record delivered against a particular Req shall be given a record number. The record number shall start at 0 and shall increment for each record delivered against the original Req. The record number counts independently even if some results are sent in various interim responses.

NOTE: The combination of Request ID and Record Number gives a particular record a globally unique number.

7.3.4 Error information

The error message shall contain a textual message giving as many details as possible of the error, and contact details (if appropriate) for a person who will be able to assist in resolving the error.

7.3.5 Delivery information

Delivery information shall either be agreed in advance between the CSP and LEA, or it shall be given in the HI-A request.

FOR FURTHER STUDY. NOTE SECURITY CONCERNS OF GIVING DELIVERY ADDRESSES IN HI-A.

7.3.6 Request priority

In some situations it may be useful to signal a priority with a request. This is for use at a national level. The present document makes no statement about how to treat requests of a different priority, how to manage queues of requests or how to manage the use of priority considerations.

EDITOR'S NOTE: add 8-character string to header structure to allow priority.

7.4 Retained Data response

7.4.1 General

The response is a set of records that meet the request criteria.

The response will be a "flat" sequence with no additional structure to them (e.g. not a "tree" of information in which certain records refer back to other records within the same response).

The records in a response will all be from the same “service” (see 4.2) and from the same “category” see (4.3)

7.4.2 Volatile information

Certain information changes over time and is called volatile (e.g. Cell IDs are volatile whereas latitude/longitude is not). Volatile information shall have a time associated with it, indicating the time of the observation.

1. The present document supports the transmission of “translated” data i.e. the volatile information converted into a permanent form.
2. The present document supports the querying of historical data, asking what the value of the volatile data was at a given time.

It is a national issue to agree which method(s) to use. It is mandatory that the value of volatile data can be ascertained by the LEA.

If a request is made for volatile information over a range of times (rather than just a specific time) then the response may contain multiple records that match the request. All record falling within the time period shall be sent.

7.4.3 Unavailable parameters

If parameters are not able to be filled in by the CSP, a default answer shall be populated. It is not acceptable to leave out the parameter altogether / make it optional.

7.5 Retained Data requests

7.5.1 Information contained within a request

A request for retained data, along with the headers defined in 7.1, 7.2 and 7.3, shall state:

- The service to which the request applies (the services are as defined in Annex B onwards).

  NOTE: for enquiries across multiple services, send a separate request for each service.
- The category of data (“Traffic”, “Subscriber”, etc).
- A set of “request parameters” that define which records are required.
- The request parameters shall include a time window.

Each “request parameter” shall be one of:

- A specified value for a given field
- A list of values for a given field
- A range for a given field (e.g. lower and upper bounds for integers, or a value containing wildcards for strings. See section 7.5.2 regarding when it is proportionate and legal to use ranges such as wildcards).

7.5.2 Statement about proportionality and legality

The request structure defined in section 7.5.1 permits a broad range of requests. Some of the requests that are possible under this structure will not necessarily be legal in all jurisdictions or proportionate in all situations. The goal of the present document is to define a structure that (at a technical level) allows a wide range of requests to be transmitted. Just because a request can be constructed within the framework in 7.5.1, it does not mean it is automatically a legal request. It is a national issue to establish whether or not a request is legal and proportionate.

NOTE: Some requests may be unexpectedly difficult depending on the implementation of databases on the operator side. For example, searching for a range of phone numbers (e.g. 01111100000 to 01111199999) would not be simple if phone numbers were stored in an encrypted format (it would then require each of the 100,000 numbers to be encrypted and requested independently). Searching for a range of values on a parameter could be time-consuming if the parameter was not normally used as a key or searched field under the database design. Such considerations should be taken into account when evaluating whether a request is "proportionate".

8 Data exchange techniques

8.1 General

Two data exchange techniques are presented: "HTTP" and "direct TCP".

The ***HTTP*** technique is intended to be used by those organisations who are not familiar with ASN.1. It is based on simple, reliable protocols for which software is easily available.

The ***direct TCP*** option provides a compact and direct data exchange mechanism, and may be more suitable for more rapid or large data exchanges.

It is acceptable to use one technique for HI-A and another for HI-B.

NOTE: It would be unusual to use direct TCP for HI-A at the same time as HTTP for HI-B.

The choice of technique is to be agreed by LEA and CSP. All LEAs shall support the HTTP technique, and no CSP shall be forced to use direct TCP if they deem this impractical (e.g. if they have no experience of ASN.1).

8.2 Web services

8.2.1 Basic information

The web service technique uses XML encoding derived from the XML schema in Annex A. It uses HTTP (on top of the standard TCP/IP stack).

The CSP runs a HTTP server, and the LEA acts a HTTP client.

8.2.2 Request

- The Request for RD (called *Req* in the message flows in section 6 of RDHI draft) is sent from LEA to CSP as a HTTP POST with the request details attached.
- The Acknowledgement (called *ReqAck*) is sent as a HTTP OK.

8.2.3 Interim updates

- Interim messages can be sent from LEA to CSP as HTTP POST, stating that an interim update is required.
- The reply is sent from CSP to LEA as part of a HTTP OK.

8.2.4 Results

FOR FURTHER STUDY

EDITOR'S NOTE: HTTP does not easily support the server (CSP) sending messages out without a Request from the LEA. So no Res message can be sent spontaneously. This is a significant problem. There are a number of options:

- *CSP must wait for a request from the LEA, and then the CSP can respond with the results i.e. the LEA polls for the results.*
- *CSP could also run a web client, and LEA a web server. Then messages could be sent in the opposite direction.*
- ~~*Use a raw TCP technique such as TD007.*~~
- ~~*Use a "notification" technique, outside of the HTTP protocol to inform the LEA that they should ask for the results. THIS IS CURRENTLY THE PREFERRED OPTION.*~~
- ~~*"Hold open" the HTTP connection to send a (multi-part?) reply down the connection. This may work for very quick responses (in which the response can be sent* within *a few seconds of the request) but otherwise is not very suitable.*~~

The LEA can ask for results in one of the following ways (FOR FURTHER STUDY).

- Option 1: LEA asks for a list of available results (call this an "INDEXLIST" message, sent as HTTP GET). The CSP returns a list of results that are ready. The LEA can then request individual files to be delivered using HTTP GET commands.e
- Option 2: For each outstanding Request, the LEA can ask for the results for that Request (by reference to its RequestID) using HTTP GET. The CSP would reurn an error (e.g. File Not Found) for those requests not yet ready.

8.2.5 Errors

Additionally, it is difficult for this technique to signal an error from the CSP without a request from the LEA. The same possible solutions (from 8.2.4) apply.

8.3 Direct TCP data exchange

The direct TCP mechanism uses BER encoding derived from the ASN.1 in Annex A. The direct TCP option uses TS 102 232 Part 1 data exchange details (section 6) on top of the standard TCP/IP stack.

The notes on errors in TS 102 232 Part 1 section 6.2.2 do not apply to RDHI.

~~10 Performance and quality~~

~~10.1 Timing~~

~~10.2 Quality~~

11 Security aspects

SECTION 11 IS FOR FURTHER STUDY

This clause will give an informative overview of the security properties and mechanisms that can be used to meet possible security requirements for the transportation of Lawful Intercepted data.

11.1 Security properties

A secure communication channel has the following properties:

- confidentiality;
- integrity;
- authentication;
- availability.

Confidentiality means that it is impossible to interpret the data by eavesdropping on the communication link.

Integrity means that any alteration or mutilation of the transported data is immediately detected.

Authentication means that the communicating parties have verified and confirmed each other's identities.

Availability means that the communicating parties have made agreements about up- and downtimes of the systems. In case of irregularities, alarm messages should be sent through another communication channel. Because of the nature of the transported data, confidentiality can be an issue. Retained data can also be confidential or secret by law and appropriate measures need to be taken to prevent eavesdropping by unauthorized third parties.

Integrity can be an issue when retained data is used as evidence in a criminal investigation. It must be provable that the data is unaltered during the transportation of the data

In the process of retained data it is very important to know that the LEMF is receiving the data from a real MF and the MF needs to be sure that it is sending its data to a real LEMF. If this verification of identity does not take place, retained data might end up in the wrong place or the LEMF is processing data that is originating from an unauthorized source.

The process of requesting retained data takes place within defined parameters. In case of any irregularities, appropriate actions need to be taken. Irregularities can be a sign of a breach of security, loss of data or detection of interception.

11.2 Security mechanisms

This clause will give an overview of possible mechanisms to achieve the properties as described above. Technical details are to be decided during the process of implementation.

Confidentiality can be achieved by using encryption. A common technique is to use a symmetric encryption algorithm. A symmetric algorithm is an algorithm where both communicating parties use the same key for encryption and decryption. This key must be exchanged in a secure way.

Integrity can be achieved using hashing algorithms. These algorithms generate a unique fingerprint of the transported data. When the transported data is altered, the fingerprint does not match anymore and appropriate actions can be undertaken (like retransmission of data).

Authentication can be achieved using cryptographic techniques. A common technique is to use asymmetric encryption. In this technique, both parties have two keys: A public key and a private key. Data encrypted with one key can only be deciphered with the other. If party X encrypts something using the public key of party Y then party Y is the only one able to decrypt this data using his private key. If party X encrypts something using his private key then this data can only be deciphered using his public key. By combining these properties, both parties can make sure that they are communicating with the right party.

Annex A (normative): Data fields

A.1 Introduction to data fields

Regardless of what data exchange technique is adopted for the request and delivery of retained data a common data dictionary is necessary. This list of parameters must be consistent, extensible and maintainable.

The NWO/AP/SvP and Requesting Authority will use this standard data dictionary.

The present document defines the format of data to be transferred across the RDHI. In Annex A, a number of data elements are identified; they fall into two areas:

- The elements marked MANDATORY are those that are essential in order to meet the requirements (e.g. explicitly required by the EU Data Directive, or necessary to meet the transport requirements).
- It is for national agreement to determine the situations in which the elements marked OPTIONAL are stored or delivered. The present document does not address the circumstances in which it is required, technically feasible or legal to store or deliver such elements. The present document states that if such an element is present on the handover interface, then it shall be delivered in the format specified in Annex A.

EDITOR'S NOTE: It is anticipated that a large proportion of the elements will fall into the second category i.e. that the present document is defining a superset of the available retained data information.

A.2 Choice of data modelling language

The structure of the data is defined in ASN.1. A XML schema (derived from the ASN.1) is also given in the present document. If data exchange takes place using XML, then the XML schema shall be used.

EDITOR'S NOTE: The XML schema will only be created once the ASN.1 is stable.

EDITOR's NOTE: It is likely that an automated tool will initially be used to create the XML schema from the ASN.1, but the translation will need to be checked and finished by hand as automatic translation may not be accurate.

EDITOR'S NOTE: If there are discrepancies between the ASN.1 and XML schema in a given version of the present document, then, when creating the subsequent version, it should be assumed that the ASN.1 is correct and the XML schema is to be changed. However, for implementation against a given version of the present document, it is only necessary that XML conforms to the XML schema and BER-encoded data conforms to the ASN.1 specification.

A.3 ASN.1 definitions

A.3.1 General remarks on ASN.1

Put Retained Data definitions alongside LI in the overall ASN.1 tree.

EDITOR's NOTE: See also Rap16TD013a1 for further suggestions for parameters. See Rap16TD004r1 for further suggestions (neither of these documents is yet agreed by any meeting).

Section A.3.2 contains the top levels of the ASN.1 tree. The ASN.1 details for each service are listed in Annex B onwards.

It is recommended to copy IRI parameters from LI standards wherever appropriate. Where a parameter is copied, it is essential that it has the same meaning and same format in both LI and RD standards. It is not recommended to IMPORT parameters from LI standards.

EDITOR'S NOTE: All the LI parameters listed in Rap16TD008 can be included, although note that nothing should be copied from LI standards about timestamp accuracy or resolution.

A.3.2 Top level of ASN.1

```
RetainedData DEFINITIONS ::=
BEGIN

-- Top level defintions for retained data of PSTN/ISDN telephony
```

Write an ASN.1 definition of the Retained Data header here.

A retained data request will contain Retained Data header plus a single RetainedData Request record (see 7.5)

A retained data response will contain a Retained Data header plus multiple RetainedDataRecords.

```
RetainedDataRecord ::= CHOICE
{
    telephonyRecord      [1] TelephonyRecord,
    messageRecord        [2] MessageRecord,
    multiMediaRecord     [3] MultiMediaRecord,
    networkAccess        [4] NetworkAccessRecord,
    transmission         [5] TransmissionRecord,

        -- other services will be included as they are implemented
    ...
}
```

```
TelephonyRecord::= CHOICE
{
    telephonySubscriber      [1] TelephonySubscriber,
    telephonyServiceUsage    [2] TelephonyServiceUsage,
    telephonyDevice          [3] TelephonyDevice,
    telephonyNetworkElement  [4] TelephonyNetworkElement,
    ...
}
```

And so on, a MessageRecord is a choice of MessageSubscriber, MessageServiceUsage, etc.

EDITOR'S NOTE: Re-use structures across different services wherever possible. For example, TelephonySubscriber can consist of a "Person" and a "telephonySubscription" and the "Person" structure can be re-used for all services.

Annex B (normative): Service-specific details for telephony services

B.1 Scope

A telephony service is a facility, which offers the user a capability to:

- Dial E164 numbers
- Get a dial tone and outgoing/incoming ringing tones
- Conduct conversation with one or more other parties
- Hang up
- Answer when the phone rings
- Use a basic set of value-added services (including SMS).

For further study – define the technologies that are included within this service.

B.2 ASN.1 definitions for telephony

```
-- Definitions of Subscriber Data
```

```
TelephonySubscriber::= SEQUENCE
{
    subscriberID                [1] TelephonySubscriberId,
        -- Unique identifier for this subscriber, e.g. account number
    subscriberName              [2] SubscriberName,

-- NAMES AND ADDRESSES ARE “VOLATILE” AND SHOULD BE TREATED AS DESCRIBED IN 7.4.4.

    registeredAddress           [3] ContactDetails,
        -- Address the account is registered at (i.e. an installation address)
    contactAddress              [4] ContactDetails OPTIONAL,
        -- Contact address, if different from the registered address

-- ADDRESS INFORMATION TO BE UPDATED AS PER RAP16TD11

    billingDetails              [6] BillingDetails,
    subscribedTelephonyServices     [7] SEQUENCE OF SubscribedTelephonyServices,
        -- A subscriber (or account) may have more than one service listed
        -- against them.
    ...
}
```

```
TelephonySubscriberId  ::= OCTET STRING
        -- Unique identifier for this subscriber, e.g. account number
```

```
SubscribedTelephonyServices::= SEQUENCE
{
    serviceID               [1] OCTET STRING,
        -- Unique identifier for this service within the operator
    providerID              [2] OCTET STRING,
        -- Unique identifier for the service provider
    timeSpan                [3] TimeSpan OPTIONAL,
        -- Start and end data, if applicable, of the subsription
    registeredNumber        [4] PartyNumber OPTIONAL,
        -- telephone number registered for this service
    serviceType             [5] TelephonyServiceType OPTIONAL,
    ...
}
```

```
SubscriberName ::= SEQUENCE
{
    salutation          [1] OCTET STRING OPTIONAL,
    surname             [2] OCTET STRING OPTIONAL,
            -- The non-chosen or inherited name of an individual.
    surnamePrefix       [3] OCTET STRING OPTIONAL,
            -- any prefix before the surname, e.g. “von”, “van der”.
    middleNames         [4] OCTET STRING OPTIONAL,
            -- That part of the name excluding forename, separable and preceding the surname.
    firstname           [5] OCTET STRING OPTIONAL,
            -- The firstname or initials.
    ...
}
```

```
ContactDetails ::= SEQUENCE
{
    address             [1] AddressInformation OPTIONAL,
    emailAddress        [2] OCTET STRING OPTIONAL,
    contactNumber       [3] SEQUENCE OF PartyNumber OPTIONAL,
            -- several numbers (work, home, mobile) may be given for a single subscriber
    dateOfBirth         [4] GeneralizedTime OPTIONAL,
    gender              [5] ENUMERATED
    {
            male(0),
            female(1),
            ...
    } OPTIONAL,
    ...
}
```

```
BillingDetails ::= SEQUENCE
{
    billingAddress      [1] AddressInformation,
    paymentDetails      [2] PaymentDetails,
    ...
}
```

```
PaymentDetails ::= NULL
    -- For further study.
```

```
AddressInformation ::= SEQUENCE
{
    addresseeName       [1] SubscriberName,
    flatNumber          [2] OCTET STRING OPTIONAL,
    buildingName        [3] OCTET STRING OPTIONAL,
    buildingNumber      [4] OCTET STRING OPTIONAL,
    streetName          [5] OCTET STRING OPTIONAL,
    postalCode          [6] OCTET STRING OPTIONAL,
            -- Postal code. Example: 2289AC.
    poBox               [7] OCTET STRING OPTIONAL,
            -- PO box or Response number
    city                [8] OCTET STRING OPTIONAL,
    country             [9] OCTET STRING OPTIONAL,
            -- Country code as defined in ISO 3166-1 [17].
    ...
}
```

```
TelephonyServiceType    ::= ENUMERATED
{
    private (0),
    privatePABX (1),
    publicPayphone (2),
    ...
}
```

```
-- Definitions of Service Usage Data
```

```
TelephonyServiceUsage   ::= SEQUENCE
{
    partyInformation                    [1] SEQUENCE OF TelephonyPartyInformation,
            -- This parameter provides the concerned party (Originating, Terminating
            -- or forwarded party), the identity(ies) of the party and all the information
            -- provided by the party.
    communicationTime                   [2] TimeSpan,
            -- Time and duration of the communcation
```

```
    eventInformation                    [3] SEQUENCE OF TelephonyEventInformation OPTIONAL,
        -- A list of events that occurred during this service usage
    endReason                           [4] INTEGER OPTIONAL,
        -- Q.850 cause code for call termination
    communicationType                   [5] TelephonyCommunicationType OPTIONAL,
    bearerService                       [6] TelephonyBearerService OPTIONAL,
    smsInformation                      [7] SmsInformation OPTIONAL,
    ...
}
```

```
TelephonyPartyInformation           ::= SEQUENCE
{
    partyRole                   [1] TelephonyPartyRole,
    partyNumber                 [2] PartyNumber,
    subscriberID                [3] TelephonySubscriberId OPTIONAL,
    deviceID                    [4] TelephonyDeviceID OPTIONAL,
    locations                   [5] SEQUENCE OF TelephonyLocation OPTIONAL,
        -- List of cell locations used by this party during the service usage
    ...
}
```

```
TelephonyCommunicationType ::= ENUMERATED
{
    telephonyFixedCS (0),
    telephonyWirelessCS (1),
    sMS (2),
    ...
}
```

```
TelephonyBearerService ::= ENUMERATED
{
    speech (0),
    data (1),
    fax (2),
    ...
}
```

```
SmsInformation ::= SEQUENCE
{
    smsEvent     [1] ENUMERATED
    {
        shortMessage (1),
        shortPartMessage (2),
        compositeMessage (3),
        notificationMessage (4),
        ...
    } OPTIONAL,
    smsType      [2] ENUMERATED
    {
        deliverSCtoMS (1),
        deliverReportMStoSC (2),
        statusReportSCtoMS (3),
        commandMStoSC (4),
        submitMStoSC (5),
        submitReportSCtoMS (6),
        reservedMTIValue (7),
        ...
    } OPTIONAL,
    smsStatus   [3] ENUMERATED
    {
        delivered (0),
        expired (1),
        deleted (2),
        replaced (3),
        submitted (4),
        incomplete-submission (5),
        incomplete-delivery (6),
        undeliverable (7),
        passed-on (8),
        ...
    } OPTIONAL,
    smsCmRefNr      [4] OCTET STRING (SIZE(1..2)) OPTIONAL,
    smsNumOfSM      [5] INTEGER (0..65535) OPTIONAL,
    smsNotifInd     [6] BOOLEAN OPTIONAL,
    smsProtocolId   [7] OCTET STRING (SIZE(1)) OPTIONAL,
    ...
}
```

```
TelephonyEventInformation ::= SEQUENCE
{
    time            [1] GeneralizedTime OPTIONAL,
            -- time when the event occurred
    type            [2] TelephonyEventType OPTIONAL,
            -- type of event
    party           [3] TelephonyPartyRole OPTIONAL,
            -- party to which the event is related
    location        [4] TelephonyLocation OPTIONAL,
    ...
}
```

```
TelephonyEventType ::= ENUMERATED
{
    handover (1),
    hold (2),
    retrieve (3),
    suspend (4),
    resume (5),
    ect (6),
    mpty (7),
    mptyHold (8),
    mptyRetrieve (9),
    mptySplit (10),
    uus1 (11),
    uus2 (12),
    uus3 (13),
    serviceSpeech (14),
    serviceFax (15),
    confBeginSeizure (16),
    confAdd (17),
    confSplit (18),
    confIsolate (19),
    confReattach (20),
    confDrop (21),
    confBeginActive (22),
    tpyInvoke (23),
    tpyPrivateComm (24),
    ...
}
```

```
TelephonyLocation  ::= SEQUENCE
{
    telephonyNetworkID  [1] TelephonyNetworkID,
            -- ID of the network element location (e.g. Cell ID)
    timeSpan            [2] TimeSpan,
            -- Time span that this location was valid for
    ...
}
```

```
TelephonyPartyRole ::= ENUMERATED
{
    originating-Party(0),
    terminating-Party(1),
    forwarded-to-Party(2),
    originalCalled (3),
    redirecting (4),
    connected (5),
    userProvidedCalling (6),
    roaming (7),
    translated (8),
    singlePersonalNumber (9),
    smsOriginator (10),
    smsRecipient (11),
    smsOriginatorTrn (12),
    smsRecipientTrn (13),
    ...
}
```

```
-- Device Data definitions
```

```
TelephonyDevice ::= SEQUENCE
{
    telephonyDeviceID   [1] TelephonyDeviceID, OPTIONAL
            -- Unique identifier for this telephony device (e.g. IMEI for a handset)
    imei                [2] OCTET STRING (SIZE (8)) OPTIONAL,
```

```
    ...
}

TelephonyDeviceID ::= OCTET STRING
    -- A unique identifier for the telephony device. For example, the IMEI number
    -- of a mobile handset

-- Network Data definitions

TelephonyNetworkElement ::= SEQUENCE
{
    telephonyNetworkID   [1] TelephonyNetworkID,
    location             [2] TelephonyLocation OPTIONAL,
    ...
}

TelephonyNetworkID ::= OCTET STRING
    -- Unique identifier for this network element: e.g. a Cell ID


-- General definitions

TimeSpan    ::= SEQUENCE
{
    startTime        [1] GeneralizedTime,
    endTime          [2] GeneralizedTime OPTIONAL,
    ...
}

PartyNumber::= [1] OCTET STRING
    -- E164 address of the node in international format. Coded in the same format as
    -- the calling party number parameter of the ISUP (parameter part: EN 300 356 [5])

END
```

Annex C: Service-specific details for asynchronous message services (normative)

C.1 Scope

Messages handling is an asynchronous form of communication where there is an intermediate storage of messages from where they can be downloaded or viewed (webmail). This includes e-mail, webmail but excludes chat, which is synchronous.

The facilities a user will expect to find are:

- Post a message to recipient's server
- Retrieve messages from own server
- Store messages in server (IMAP)

Note that SMS is handled under "telephony services".

For further study

C.2 ASN.1

Annex D: Service-specific details for synchronous multi-media services (normative)

D.1 Scope

This service consists of any interactive or synchronous service beyond the “telephony service” in Annex B. The designation “multi-media” indicates sound, pictures, video and may be extended to include future media forms. The services related to MMS today are:

- Media files over GPRS
- Streaming video over packet
- Chat

For further study

D.2 ASN.1

Annex E: Service-specific details for network access services (normative)

E.1 Scope

Network access is typically provided by ISPs, possibly through an intermediate access provider, such as Cable-TV or ADSL. This may be taken as a generic capability to access public networks with a variety of protocols, but in current practice only Internet access would be of interest for data retention.

User facilities are:

- Access to the Internet, after some sort of authentication

For further study

E.2 ASN.1

Annex F: Service-specific details for transmission services (normative)

F.1 Scope

This is typically a service offered between networks and thus transparent to the end-user. An ISP may for instance contract with a cable-TV operator to be able to offer access.

User facilities may be one or several of:

- Broadband access from customer premises to an interconnection point
- Non-transparent protocol conversion (i.e. excluding conversions or translations that are internal to the CSP in question).
- User authentication (eg through DHCP relay option 82)

Typically the information to be stored would consist of an identifier for the end-point of the service offered by the operator in question. *For further study.*

F.2 ASN.1

F.3 Notes

EDITOR'S NOTE: Rap16TD10 contains notes on WLAN services. It was agreed to be a useful starting point.

Annex X: Manual techniques (informative)

Introduction

Manual techniques can include:

- Use of phone, fax or email for HI-A or HI-B
- Use of physical storage media (e.g. DVD) for HI-B

For all manual uses, the following principles are recommended:

- The message flows (section x) should be broadly followed although acknowledgements may be unnecessary or not practical
- It is strongly recommended that the content of the messages should follow the messages defined in section x.x.
- Lower layers (encoding, transport, etc) (section x and x) in general would not be followed. Where appropriate, consistent encoding schemes are recommended.

Annex Y: Suggested use cases (informative)

EDITOR'S NOTE: This annex maintains a list of questions that people would like the RD interface to support. This list is a free-for-all and informative with no guarantee that the questions will be supportable. But it will be a valuable set of use cases for us to use to "test" our proposals. It will be deleted before publication.

EDITOR'S NOTE: As agreed at Rap16 (Groningen), for security reasons the list of use cases will be maintained as an ongoing TD in the LI-ActiveMembers list. The starting point and first version of the use cases is LI-Rap16-TD009 from Stefan Bjornson. Further contributions are welcome.

Annex Z (informative): Change Request History

Status of the present document Handover interface for the request and delivery of retained data		
Date	**Version**	**Remarks**

History

Document history		
V0.0.1	September 2006	Initial draft
v0.1.0	December 2006	Outcome of TC LI Rap#14 -> TC LI#14 Tenerife
V0.2.0	February 2007	Outcome of TC LI#14; input to Rap15
V0.3.0	March 2007	Outcome of Rap15; input to TC LI#15
V0.3.1	April 2007	Outcome of TC LI#15; input to Rap16
V0.4.0	June 2007	Outcome of Rap16