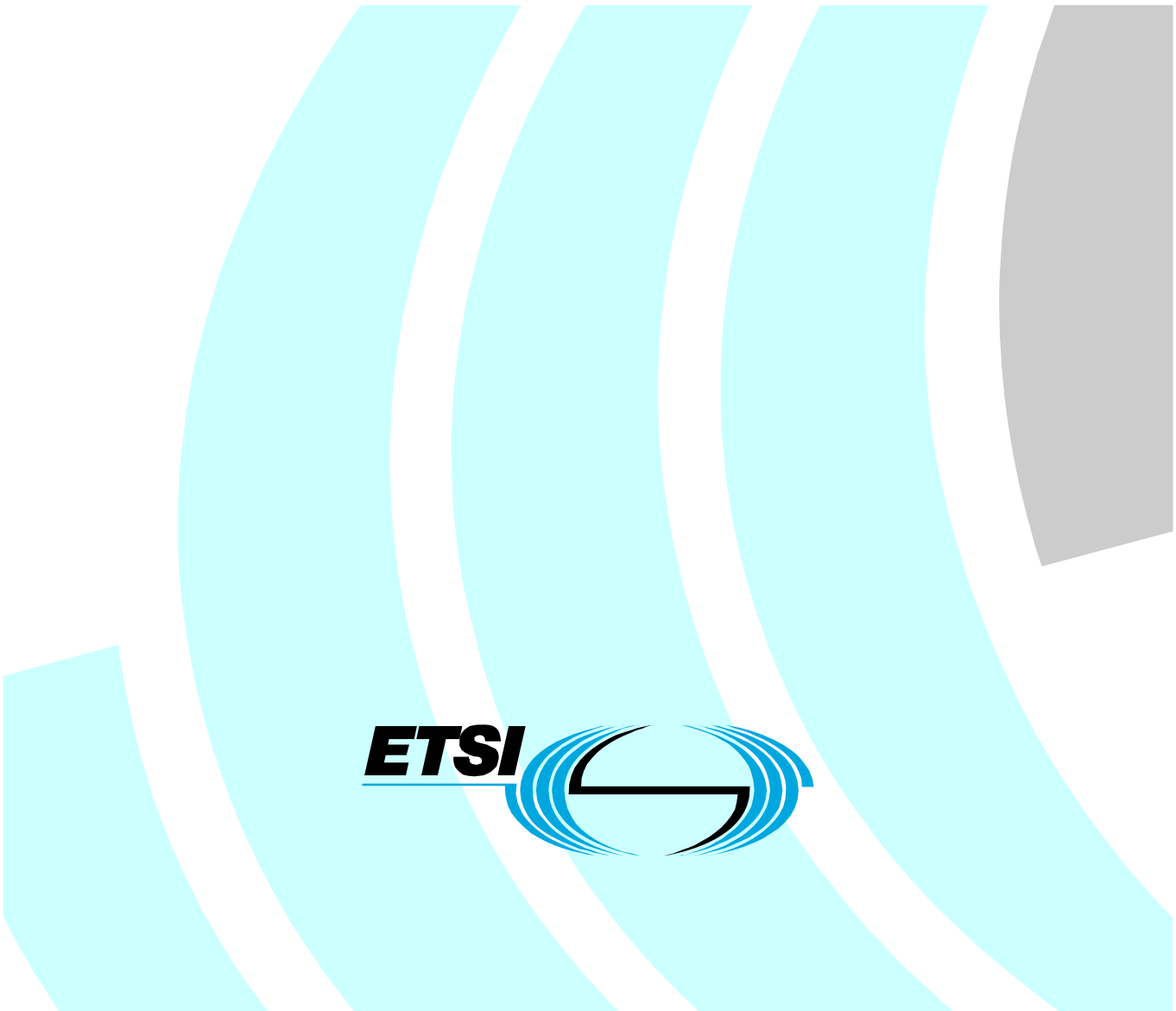
ETSI TS 102 657 V1.2.1 (2009-06)

Technical Specification

Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data



Reference
RTS/LI-00059

Keywords
handover, retention

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).

The ASN.1 module and XML schema are also available as an electronic attachment to the original document from the ETSI site (see details in clause A.3.1.2).

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 Data Retention [1]. The handover requirements from TS 102 656 [2] are derived from the requirements contained in and implied by the EU Directive [1] 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 I, the present document does not consider manual techniques.

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.

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 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[3] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[4] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

[5] ISO 4217: "Codes for the representation of currencies and funds".

[6] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[7] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".

[8] ETSI TS 100 974: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Application Part (MAP) specification (GSM 09.02)".

[9] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".

[10] ETSI TS 125 431: "Universal Mobile Telecommunications System (UMTS); UTRAN lub Interface Layer 1 (3GPP TS 25.431)".

[11] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[12] ETSI TS 101 109: "Digital cellular telecommunications system (Phase 2+); Universal Geographical Area Description (GAD) (3GPP TS 03.32)".

[13] FIPS PUB 186-2: "Digital Signature Standard (DSS)".

[14] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[15] IETF RFC 2818: "HTTP Over TLS".

[16] ETSI 123 040: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical Realization of Short Message Service (SMS) (3GPP TS 23.040)".

[17] IETF RFC 0793: "Transmission Control Protocol".

[18] IETF RFC 2581: "TCP Congestion Control".

[19] IETF RFC 2988: "Computing TCP's Retransmission timer".

[20] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[21] IETF RFC 0791: "Internet Protocol".

[22] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[23] IETF RFC 0822: "Standard for the format of ARPA internet text messages".

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:

Authorized Organization: any authority legally authorized to request or receive retained data e.g. a Law Enforcement Agency

Handover Interface A (HI-A): administrative handover interface comprising requests for information and their responses

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

lawful authorization: permission granted to an Authorized Organization 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

request: a request for retained data means a legal requirement for a Communications Service Provider (CSP) to disclose retained data in accordance with relevant national law

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

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

retained data record: set of data elements for a specific subscriber/user related to a specific service transaction

service transaction: instance of a service given by a CSP to a subscriber/user

service transaction record: set of data elements describing a service transaction (details to be determined)

transmission of information: 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	Asymmetric Digital Subscriber Line
APN	Access Point Name
ASN	Abstract Syntax Notation
BER	Basic Encoding Rules
CPE	Customer Premises Equipment
CS	Circuit Switched
CSP	Communication Service Provider
CSPID	CSP Identifier
DNS	Domain Name System
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSS	Digital Signature Standard
DVD	Digital Versatile Disc or Digital Video Disc
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI	Handover Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
ICCID	Integrated Circuit Card ID
ID	IDentifier
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security

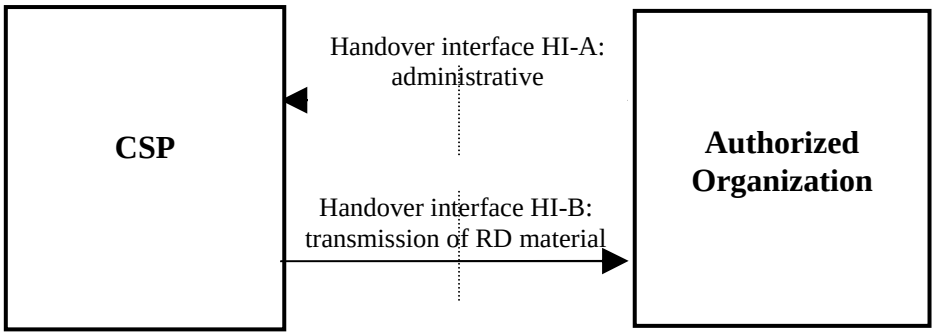
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LAN	Local Area Network
LI	Lawful Interception
MAC	Media Access Control
MSISDN	Mobile Subscriber ISDN number
MSN	Multiple Subscriber Numbers
NA	Network Access
NAS	Network Access Server
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PS	Packet Switched
PSTN	Public Switched Telephone Network
PUK	Personal Unblocking Key
RAI	Routing Area Identifier
RD	Retained Data
RDHI	Retained Data Handover Interface
SAI	Service Area Identifier
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
UTF	Unicode Transformation Format
UTM	Universal Transverse Mercator
WGS	World Geodetic System
XML	eXtensible Markup Language

4 Overview of handover interface

4.1 Reference model

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

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



NOTE 1: The term Authorized Organization covers any agency legally authorized to make RDHI requests (see clause 3.1).
NOTE 2: HI-B delivers data from CSP to the Authorized Organization. There may be related supporting lower level messages from the Authorized Organization to CSP on HI-B.

Figure 1: Functional diagram showing handover interface HI

Each of these two parties can be expanded to show some of their internal functions. This is not to proscribe how implementations of the present document must be organized, and is purely informational.

Within the CSP block, three internal CSP functions can be identified: an *administrative function to* manage the RD requests and responses; a *data collection function* to collect data from the various internal network elements and prepare the data for retention; a *data store management function* to index and store the data, execute queries, and manage the maximum retention period for RD.

Within the Authorized Organization block, two functions can be identified: an *issuing authority* responsible for initiating new RDHI requests; a *receiving authority* to accept the RDHI responses. In many situations, the authority issuing a request will also be the authority to receive the responses. However, the issuing authority may indicate a different delivery point for HI-B responses, in which case the issuing authority and receiving authority will be different.

These internal functions, and the interfaces between them, do not form a normative part of the present document.

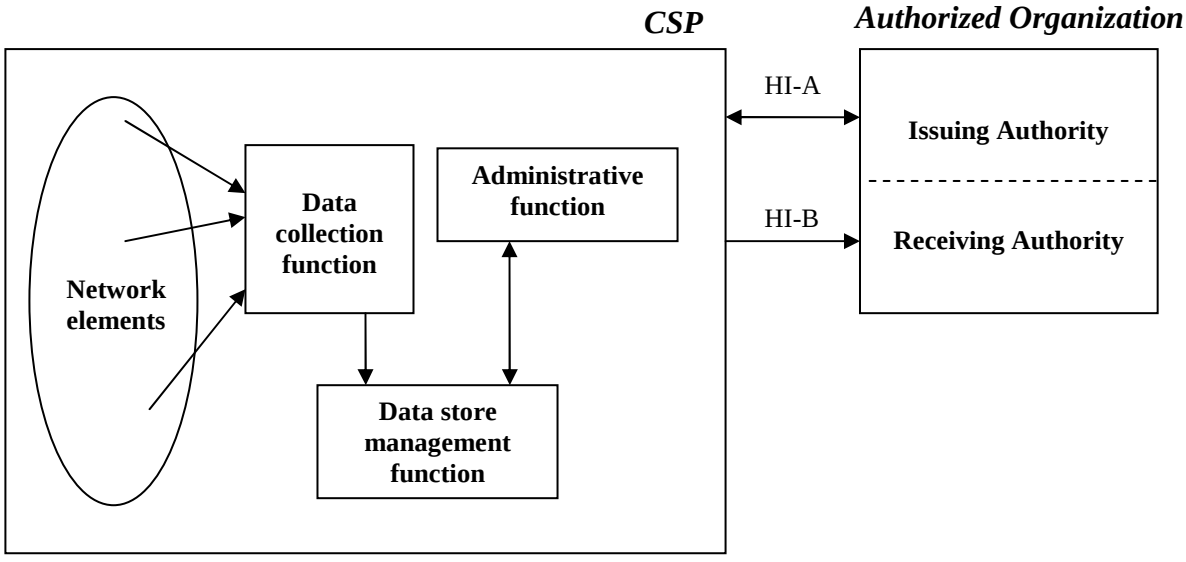


Figure 2: Functional model (informative)

A CSP or Authorized Organization may outsource some of its internal functions to a third party. It is a national option whether or not outsourcing is allowed, or whether conditions apply.

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 3). The present document contains one annex for each service (annex B onwards).

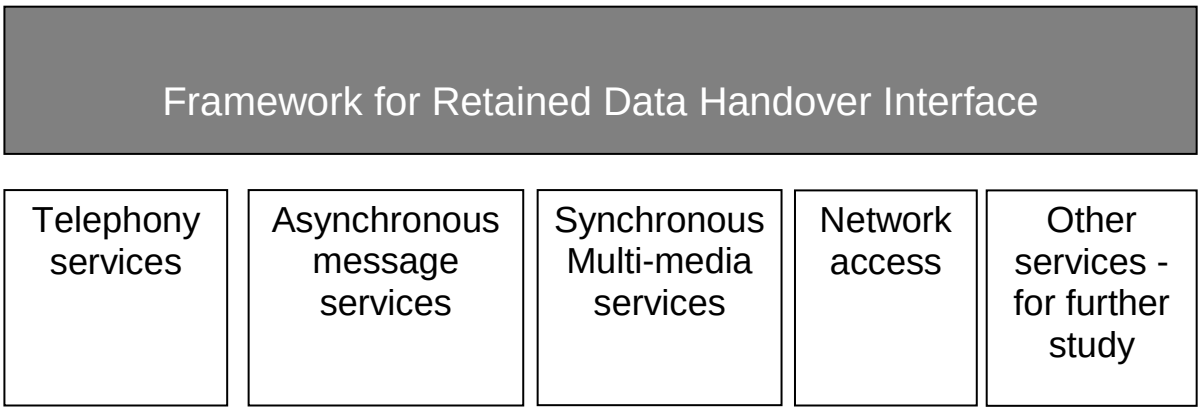


Figure 3: Framework structure

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

This handover interface does not mandate or require CSPs to create data by inspecting or analyzing communication content.

The scope of each service is as follows:

- Telephony services covers those services offering the facilities listed in clause B.1. It covers services that provides PSTN/ISDN functionality (either offered over PSTN/ISDN or emulated PSTN/ISDN (as defined in ES 282 002 [22]) over IP) including GSM/UMTS-CS and SMS.
- Asynchronous messaging services covers asynchronous communications involving the intermediate storage of messages, as defined in clause C.1. This includes e-mail, webmail but excludes chat, which is synchronous, and excludes SMS.
- Synchronous multimedia services are not covered by the present document. Specifically, the present document does not contain details for interactive or synchronous communication sessions beyond the telephony services.
- Network access services covers the services offering a capability to access public networks (typically the internet), including GPRS/UMTS-PS, as defined in clause E.1.

NOTE: Data about subscriber are common to all services, as shown in the type declaration *GenericSubscriberInfo*. Even if the interface specification includes a copy of subscriber records embedded within each type of service, these records may be stored in just one copy in the Retained Data repository on the operator side and with references to/from the subscribed-to services in order to reduce storage size.

The present document is extensible: additional services may be added in future. Common SIP/IMS calls/communications are not handled by the present document.

4.3 Categories of retained data

Retained Data is broken down into the following categories:

- Subscriber data: information relating to a subscription to a particular service (e.g. Name, Address).
- Usage data Information relating to usage of a particular service (e.g. Call Records).
- Equipment data: information relating to an end-user 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).

A more detailed breakdown of these categories is given in annex H.

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

4.5 Model used for the RDHI

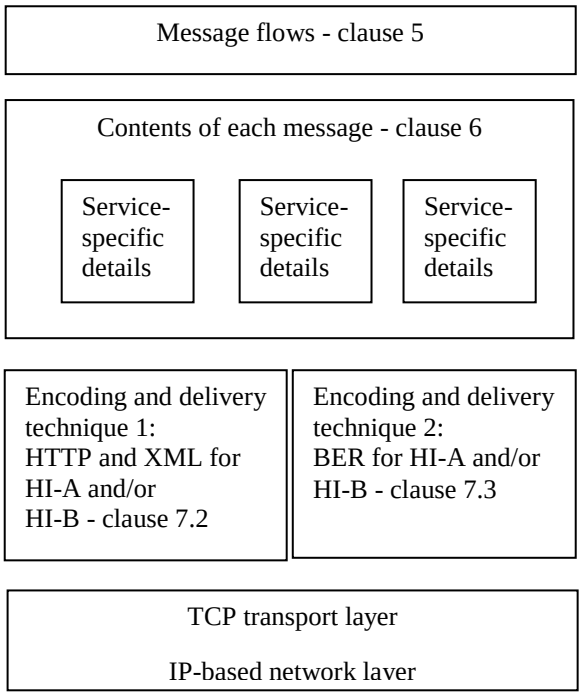


Figure 4: RDHI model

5 Handover interface message flows

5.1 Introduction

5.1.1 Summary of this clause

Clause 5 identifies the messages that shall be sent over the RDHI.

The following situations are covered (see clause 5.1.3): successful deliveries, cancelled deliveries, basic error situations and the delivery of results in stages.

The RDHI can operate in one of two modes (see clause 5.1.2). Clause 5.1 applies to both modes. Clause 5.2 covers the *General* mode, and clause 5.3 covers the *Authorized-Organization-initiated* mode.

Clause 5.4 covers addressing over HI-A and HI-B.

5.1.2 Message flow modes

RDHI message flows are defined for the following two situations:

- The *General* situation, where there is a transport mechanism that supports a full two-way transport of messages between Authorized Organizations and CSPs (see clause 5.2).
- The *Authorized-Organization-initiated* situation, where there is a transport mechanism in which the Authorized Organization initiates a communication and then the CSP responds i.e. the CSP is only able to send messages in response to an Authorized Organization message (see clause 5.3).

The remainder of clause 5.1 contains information that applies to both situations.

5.1.3 Delivery cases

Message flows for the following cases are covered:

- A successful complete delivery.
- A basic error at the CSP, signalling that no further results will be delivered for that request (see clause 5.1.4).
- The Authorized Organization cancels a request, signalling that no further results shall be delivered for that request (see clause 5.1.5).
- The delivery of some of the results before all results are ready (see clause 5.1.6).

5.1.4 "Active" requests and "closed" requests

It is essential that both parties are clear about when a request is active (i.e. the CSP is researching the answer) and when it is closed (i.e. the CSP is no longer expected to be working on the request). In order to do this, each message flow contains the following underlying steps:

- Authorized Organization submits a request to the CSP.
- CSP acknowledges it has received the request:
  - *The request is now said to be "active".*
- Either Authorized Organization or CSP signals to the other party that the request is ended (e.g. all results have been sent, an error has occurred).
- An acknowledgement is sent to confirm receipt of the message that ends the request:
  - *The request is now said to be "closed".*

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

5.1.5 Errors and failure situations

5.1.5.1 Error and failure types

The present document covers two varieties of mistake or failure:

1) ResponseFailed: If an Authorized Organization sends a request which the CSP cannot process, then the CSP sends a ResponseFailed message (see clause 5.1.5.2).
2) Errors: If one party makes a syntactical or protocol-level error (e.g. badly-formatted XML), the other party can return an error. The message with the mistake is then ignored (see clause 5.1.5.3).

It is possible that more detail is needed (beyond what is covered by the present document), e.g. it might be the case that the Authorized Organization does not consider the "complete" answer from the CSP to be complete. In order to resolve these situations, it will be necessary for the Authorized Organization 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 Authorized Organization (using a new request number i.e. completely independent of the previous request).

5.1.5.2 Request process failure feedback

If the CSP is unable to process an active request for technical reasons (e.g. authorization not verified, unable internal CSP error), then they shall send a response message marked as "FailureResponse". This terminates the request and shall be acknowledged. 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.

5.1.5.3 Other errors

If the CSP receives a message that is incorrectly formatted or out of order in the State diagram then they shall reply with an error message. The error message shall indicate, where possible, the request ID that was specified in the "bad" message. If the request ID is present in the error message, the Authorized Organization shall consider its previous message on that request ID to have been ignored.

Error messages should, if appropriate, include a short description of the error. There is no concept of an error acknowledgement for this sort of error.

5.1.6 Cancelling a request

The Authorized Organization may cancel any of its own *active* requests (as described in clauses 5.2.2 or 5.3.2), to signal that no further processing or delivery shall take place against that request.

Only "active" requests may be cancelled, see clause 5.1.4.

5.1.7 Delivery of results

By default, a *single shot* delivery approach shall be used. This means that the CSP gathers all the results meeting the request, and then they are delivered together with an indication that the results are "complete". This is acknowledged by the Authorized Organization and the request is closed.

Subject to national agreement, a *multi-part* delivery approach may be used. This means that results are delivered in a number of batches. The present document does not define the criteria which cause a batch of records to be sent (they may include: "after a certain time has elapsed", "once a certain number of records have been gathered", or may be based on other criteria); such criteria are agreed in advance outside of the message flows in the present document. Unless the CSP is certain that all results have been sent, it shall indicate that a batch of results is "incomplete"; such deliveries shall be acknowledged by the Authorized Organization as described in clauses 5.2.3 and 5.3.3, and the request remains active. Once the CSP is certain that there are no more results, it shall indicate that the results are "complete"; the Authorized Organization shall acknowledge this and the request is closed.

NOTE 1: The use of multi-part delivery is not to take place without permission in advance from the Authorized Organization concerned. In some situations, multi-part delivery creates additional complications at the CSP; the use of multi-part delivery is to take into account its technical feasibility at the CSP side.

NOTE 2: A CSP is considered to be certain that the result is complete if the data available in its own domain for the requested period has been sent. It is a national issue to deal with data received by the CSP from outside its domain after a "complete" message has been sent.

5.1.8 State diagram

The messages described in clauses 5.2 and 5.3 follow this state diagram.

Error messages are not shown in figure 5. The error message (and the message that contains the error) cause no change in state.

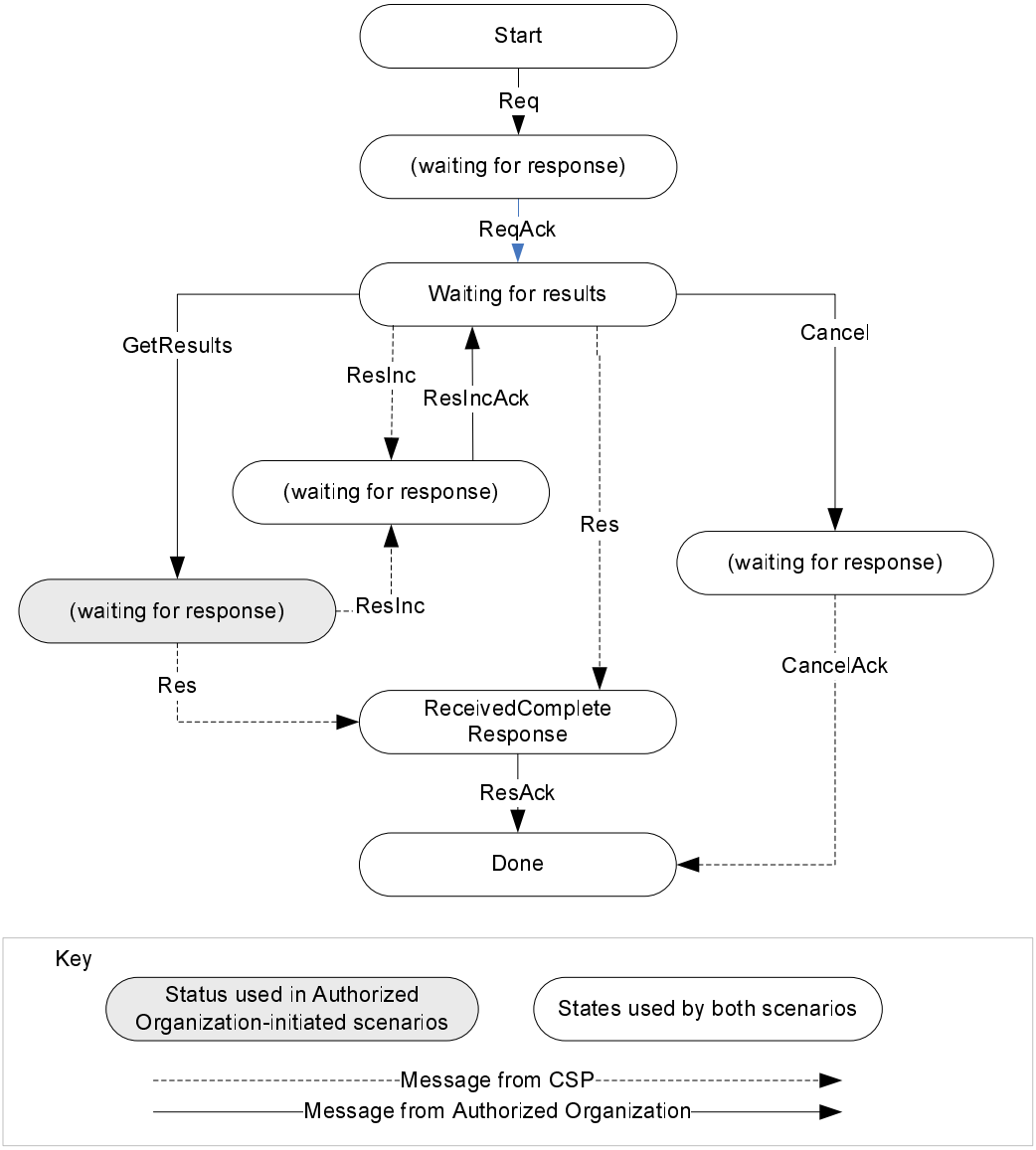


Figure 5: State diagram

The GetStatus message in clause 5.3 follows this figure, independent of the state of each request.

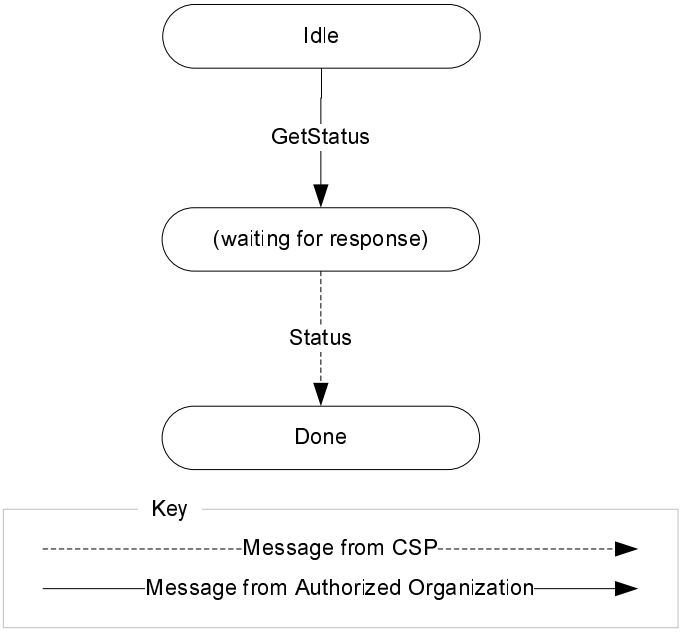


Figure 6: State diagram for GetStatus

5.2 Message flows for general situation

5.2.1 Delivery of a response

The following stages constitute the delivery of a response:

- Request message (Req):
  The Authorized Organization sends a request for RD information.

- Request acknowledgement (ReqAck):
  Without undue delay, the CSP acknowledges it has received a message from the Authorized Organization. The CSP is now under obligation to work on the given request and the request is 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 as a Res message:

  - If there are no records meeting the request criteria, a response shall still be sent, containing zero records. The Res message will have the "responseComplete" flag set.

  - If the request cannot be fulfilled for technical or procedural reasons (e.g. request exceeds authentication, or an internal CSP error), the Res message has the "responseFailed" flag set. This should contain details of why the request is unserviceable.

- Response acknowledgement (ResAck):
  Without undue delay, the Authorized Organization 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 closed (i.e. no longer active).

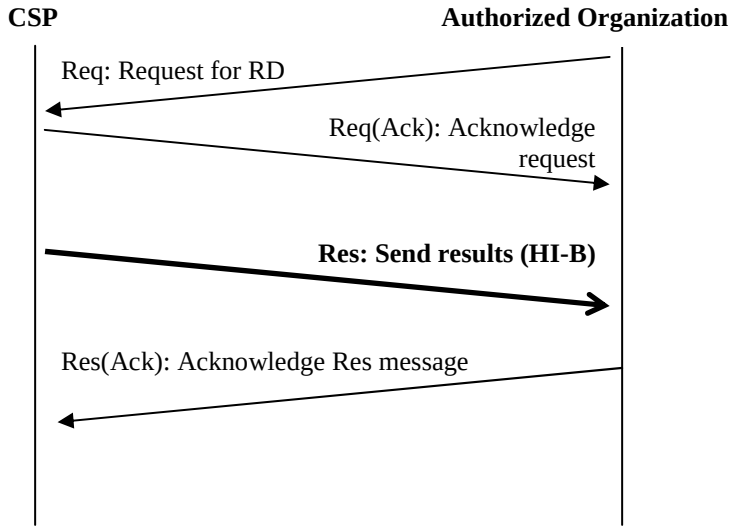


Figure 7: Message flow Successful delivery

5.2.2 Cancellation of request

Cancellation is an optional function and works as follows:

- Cancel:
  For any active request, the Authorized Organization may issue a Cancel message.
- Cancel acknowledgement (CancelAck):
  Without 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".
- Cancel rejection.
- The cancel messages after an already fully answered request will cause an error message to be returned (see clause 5.1.5.3).The CSP may choose to create an alarm in this situation (the alarm is not part of the handover interface).

If the optional function multi-part delivery is used, it is acceptable to send a Cancel message after some of the results have been received. After a Cancel message, no further results shall be sent, and a Cancel Acknowledgement shall be used.

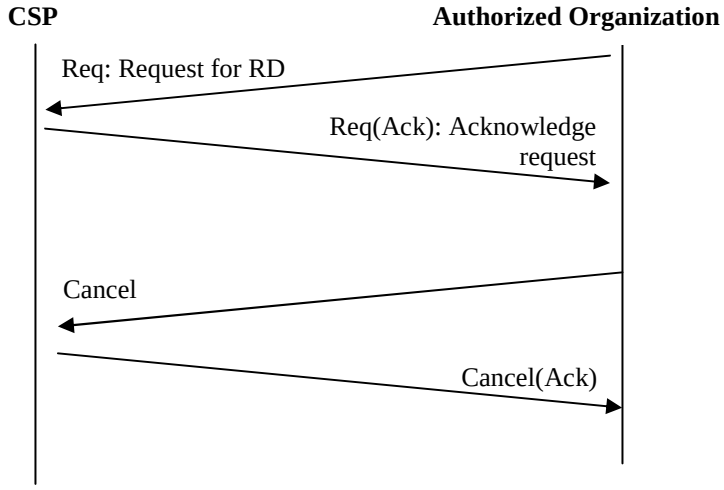


Figure 8: Message flow Cancellation by Authorized Organization

5.2.3 Multi-part delivery

As stated in clause 5.1.7, multi-part deliveries are a national option, only to be used by agreement at a national level.

Multi-part deliveries are made as follows:

- Request is made and acknowledged as usual.
- Incomplete sets of results are sent over HI-B according to agreed criteria (see clause 5.1.6). Each is flagged as "responseIncomplete".
- The Authorized Organization acknowledges each incomplete results message with a ResInc(Ack) message (this is a Res(Ack) message with type set to "AcknowledgeIncompleteResults").

NOTE: Partial results should also be acknowledged. It is important to the CSP, for legal reasons, that the Authorized Organization confirms that results were received. Such an acknowledgement does not imply that the CSP has fulfilled all of its obligations.

- There shall be no next partial delivery until the ACK has been received.
- The Authorized Organization acknowledges the final results message over HI-A.

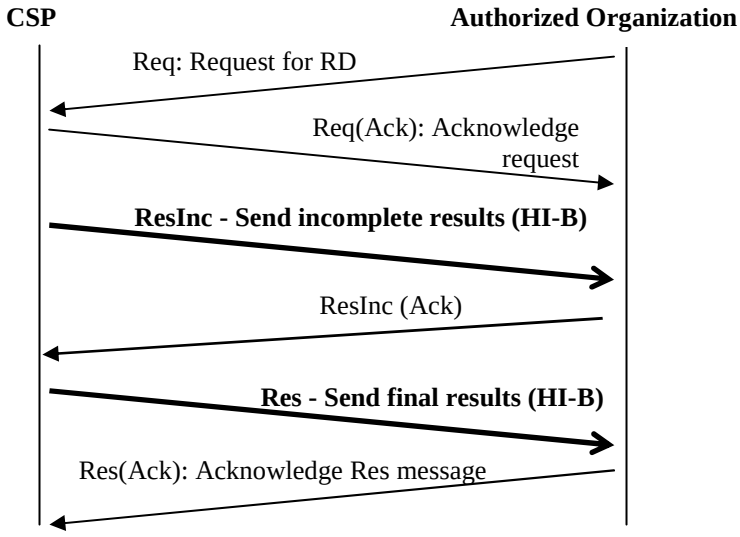


Figure 9: Message flow multi-part delivery

5.3 Message flows for Authorized-Organization-initiated scenario

5.3.1 Delivery of results or a failure response

The following messages are sent:

- **Request and acknowledge:**
  - Request message (Req):
    The Authorized Organization sends a request for RD information.
  - Request acknowledgement (ReqAck):
    Without undue delay, the CSP acknowledges it has received a message from the Authorized Organization. The CSP is now under obligation to work on the given request and the request is said to be "active".

- **Status messages (the use of Status Messages is optional, for discussion on a national basis):**

  - The Authorized Organization sends a GetStatusMessage request to the CSP. This message contains a list of RequestIDs for which the Authorized Organization requires status information. An Authorized Organization shall only make status requests about its own requests, not those from other Authorized Organizations.

  - Upon receiving the GetStatusMessage, the CSP sends a StatusMessage containing a collection of StatusResponses, one for each of the relevant RequestIDs. The StatusResponse for each RequestID contains a status flag which may be one of the values listed below. The GetStatus and Status messages do not change the status of any request, they only report on it:

    - ready - the records are ready to be collected by the Authorized Organization;
    - incompleteResultsReady - see clause 5.3.3;
    - notReady - the records are not yet ready for collection;
    - failureResponseReady - the request has failed. The Authorized Organization should issue a GetResults to find further details;
    - inDelivery - the records are currently being sent to the Authorized Organization;
    - invalidRequestID - no such request is outstanding.

- **Results messages:**

  - GetResults message:
    If there are results ready to be collected, the Authorized Organization sends a GetResults message to a CSP on HI-B, to initiate the delivery of results for a specific request ID.

NOTE 1: The Authorized Organization is expected to collect results reasonably promptly as soon as it is indicated they are ready.

  - The CSP shall respond with a Res message on HI-B, giving the results for the request ID in question. If the response has failed (as described in clause 5.1.4.2) then the response will have the responseFailed flag set, and further details are included. If the results are not yet available, then a "not ready" flag is set.

NOTE 2: An Authorized Organization should not make another GetResults request against a request ID until it has received reply to a previous one, or a predetermined time has passed.

  - If a Res message has been sent by the CSP, the Authorized Organization shall send a ResAck on HI-A without undue delay, and the request will no longer be active.

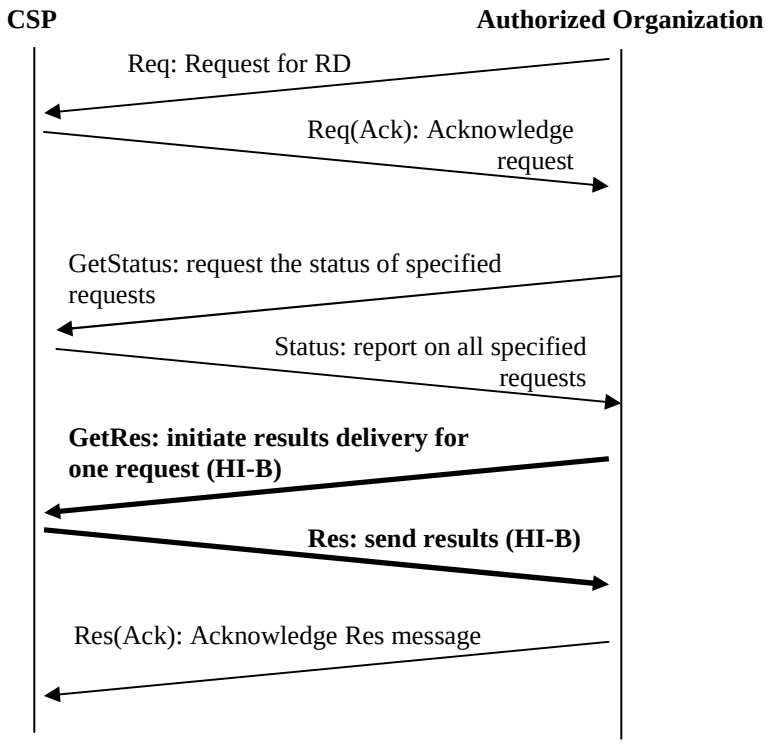


Figure 10: Delivery of results as initiated by the Authorized Organization

5.3.2 Cancellation of request

Exactly the same as clause 5.2.2.

5.3.3 Multi-part delivery

As stated in clause 5.1.7, multi-part deliveries are a national option, only to be used by agreement at a national level.

Multi-part messages work as follows:

- Request is made and acknowledged as usual.
- If a batch of responses is ready to send, then the CSP responds to a GetStatus message with the value "Incomplete results ready". As described in clause 5.1.7, the criteria for when such a batch is ready are outside the scope of the present document.
- The Authorized Organization may issue a getResults against a request that has been marked as "Incomplete results ready".
- The CSP shall return a response message containing the batch of responses. It is flagged as "ResultsIncomplete".
- The Authorized Organization shall acknowledge each incomplete results message with a ResInc(Ack) message (this is a Res(Ack) message with type set to "AcknowledgeIncompleteResults").
- While the CSP is waiting to collate the next batch of responses, it answers a GetStatus messages with a value of "notReady".
- When the next batch is ready, the status becomes "Ready" (for the final batch) or "IncompleteResultsReady" (for an incomplete set).
- The final batch of responses is flagged as "ResultsComplete". The Authorized Organization acknowledges the final results over HI-A.

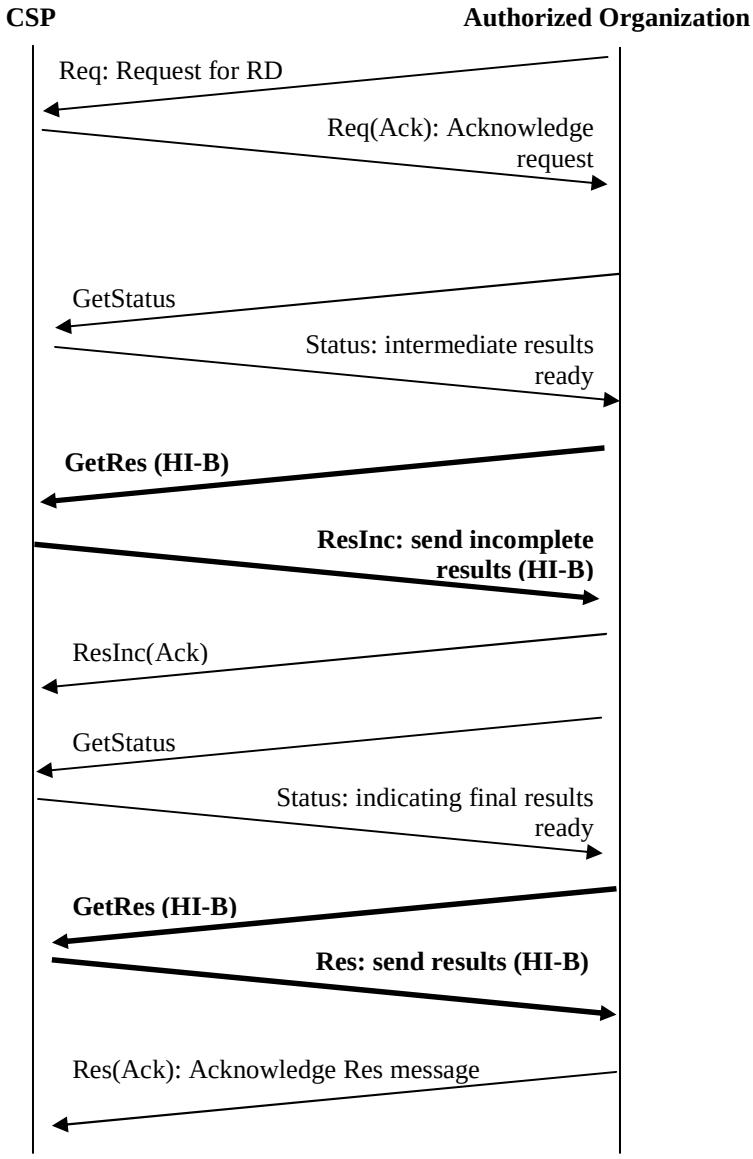


Figure 11: Delivery of results as initiated by the authorized organization in case of multi-part delivery

5.4 HI-A and HI-B addressing

The Authorized Organization and the CSP can use multiple addresses for messages sent over HI-A and HI-B. The set of addresses used must be prearranged between the Authorized Organization and the CSP. The messages below can contain delivery points. These are used to avoid mentioning specific addresses.

When the Authorized Organization initiates any kind of request, the CSP must return the corresponding acknowledgement and/or response to the address from which the request originated. However, when submitting an RDHI request, the Authorized Organization can indicate a different delivery point to which HI-B data must be sent. If no explicit delivery point is specified, the HI-B responses must be sent to the point from which the RDHI request originated.

6 Definition of the elements for retained data messages

6.1 Header information

6.1.1 Use of header information

All of the information in clause 6.1 is required on all messages unless stated otherwise.

6.1.2 RequestID field specification

Each message shall have a RequestID. The Request ID distinguishes that request from any other on an international level. To do this, the request ID shall contain:

- a country code (to indicate the country of the body making the request);
- an Authorized Organization code (assignable within the given country to distinguish between different Authorized Organizations);
- a unique reference number (assignable by the Authorized Organization). Authorized Organizations will need to ensure they have warrants or other authorization held against each request reference number. For a GetStatusMessage or StatusMessage the reference number shall not be present in the RequestID (instead there is a list of reference numbers in the body of the message).

6.1.3 CSP Identifiers

6.1.3.1 Use of CSP identifiers

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 Authorized Organization 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 clause 5.1.5). The CSP ID shall be included in all further HI-A and HI-B messages.

NOTE 1: It is not a NetworkElement ID and does not refer to exactly where in any network the info came from.

NOTE 2: 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.

6.1.3.2 Third Party CSP Identifier

Where a CSP is holding data on behalf of another CSP, the thirdParty_CSPID shall be used to indicate that an Authorized Organization is making a Retained Data Request over the HI-An interface, relating to a third party CSPs for which the CSP specified in the CSPID field is retaining data. Similarly a CSP disclosing data over the HI-B interface shall use the thirdParty_CSPID field to indicate that the data being disclosed does not relate to a subscriber owned by the CSP specified in the CSPID field.

The thirdParty_CSPID shall be agreed on a national basis and shall follow the same rules and format as for the CSPID field.

The thirdParty_CSPID an OPTIONAL parameter. However the thirdParty_CSPID shall be included in all HI-A and HI-B messages where the initial Authorized Organization Retained Data request message specified a thirdParty_CSPID.

If a thirdParty_CSPID is included in the Retained Data Request, the CSP specified in the CSPID field shall only disclose data relating to that thirdParty_CSPID and not any other data it holds (e.g. Data specifically belonging to the CSP specified in the CSPID field) or any other thirdParty_CSPID.

6.1.4 Timestamp

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

All timestamps shall contain the time and date, and an indication of the time zone.

6.2 Retained Data response

6.2.1 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 clause 4.2) and from the same "category" (see clause 4.3).

6.2.2 Additional information in response messages

6.2.2.1 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 the results are sent in a number of responses (see clause 5.1.7).

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

6.2.2.2 Response status

Every response shall have a ResponseStatus. The status will define whether it is complete or incomplete (see clause 5.1.7). In addition, for Authorized-Organization-initiated situations, it possible to indicate a status of Unavailable (see clause 5.3.3).

In case of a request that cannot be fulfilled by CSP for technical or procedural reasons (see clause 5.2.1), it is possible to indicate a status of failed response.

6.2.3 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 Authorized Organization.

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.

6.2.4 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.

There may be scenarios where an Authorized Organization requires parameters that are not available at the CSP (e.g. local loop unbundling, where the information is owned by another CSP and is therefore outside the control of the CSP to which the request was sent). In these scenarios, the CSP is not obliged to communicate with any other CSP to fetch information that they do not own. However, where the CSP has additional information that would assist the Authorized Organization, this should be communicated in the additionalInformation parameter.

A CSP may omit fields in the response for which data is held by another CSP. The format of the additionalInformation field is left to national implementation. CSPs and Authorized Organizations should agree beforehand on the format and wording of the information returned in these circumstances.

6.3 Retained Data requests

6.3.1 Information contained within a request

A request for retained data, along with the headers defined in clause 6.1, shall consist of a set of query records containing request criteria. A request may only ask for data from one service (see clause 4.2) and one category (see clause 4.3). For enquiries across multiple services or categories, a request shall be sent for each service and category.

The request shall list one or more request criteria. Each request criteria shall be one of the following types:

- Equal To: A specified value for a given field.
- Range: A range for a given field (e.g. lower and upper bounds, using the lessThan or greaterThan operators).
- Member of: A list of values for a given field.

The CSP shall return all records from the stated service and category that match all of the listed criteria.

EXAMPLE: A query record of type **telephonyServiceUsage** with the parameter **partyNumber** filled in with a specific phone number and **communicationTime** between T1 and T2 will return all telephonyServiceUsage records which contain that phone number and communicationTime in the interval T1 toT2.

Annex G gives examples of how common use-cases can be expressed using this formalism.

6.3.2 Format of a request

A request message shall contain a full set of valid header information, as defined in clause 6.1.

A request message shall contain a sequence of criteria, as described in clause 6.3.1. Each criterion shall be expressed as a RequestConstraint parameter. The RequestConstraint parameter contains a RetainedDataRecord (or a sequence of RetainedDataRecords in the case of IsAMemberOf), specifying a field and a value. The choice of RequestConstraint parameter defines the type of criteria, and will be one of the following:

- Equals: The value of the specified field of returned records shall equal the value given.
- LessThan: The value of the specified field of returned records shall be less than the value given. Only valid for numeric types such as GeneralizedTime or Integer.
- GreaterThan: The value of the specified field of returned records shall be greater than the value given. Only valid for numeric types such as GeneralizedTime or Integer.
- StartsWith: The value of the specified field of returned records shall start with the value given. Only valid for string types such as UTF8String.
- EndsWith: The value of the specified field of returned records shall end with the value given. Only valid for string types such as UTF8String.
- IsAMemberOf: The value of the specified field of returned records must be equal to one of the values given. The different permissible values are given as a sequence of RetainedDataRecords, each with a different permissible value set in the field of interest.

Multiple RequestConstraints of the same type shall be put in the same RetainedDataRecord to indicate multiple criteria. Values for all of the criteria must be from the same service and category (see clause 6.3.1). All records from this service and category which satisfy all criteria shall be returned.

NOTE: When using the IsAMemberOf constraint one needs to specify a RetainedDataRecord for each set of fields to be used. For example: in order to query about all records of calls which happened to be in either of the cells in the group: {cell1, cell2}, and be made by either of the phone numbers in the group: {phone1, phone2, phone3}, then it will need six instances of RetainedDataRecord in the SEQUENCE of the IsAMemberOf constraint. These six instances will be as follows: {cell1 and phone1}, {cell1 and phone2}, {cell1 and phone3}, {cell2 and phone1}, {cell2 and phone2}, {cell2 and phone3}. In effect these instances are a decomposition of the outer product of the two sets.

6.3.3 Additional information in requests

6.3.3.1 Priority of a request

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.

6.3.3.2 Maximum hits

A request may specify an upper bound on the number of results, by populating the MaxHits parameter in the request.

It is a national issue to discuss details of how MaxHits are used, and what further action to take when MaxHits is exceeded. It is a national issue to discuss how to handle MaxHits with partial deliveries.

If the MaxHits parameter is present, and if the CSP identifies more results meeting the request than the MaxHits value, then the CSP shall treat this as a ResponseFailed (i.e. send a ResponseMessage with ResponseStatus set to responseFailed) with the string "Maximum hits exceeded" in the information field of the FurtherInformation structure.

6.4 Error messages

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 (see clause 5.1.5.3).

7 Data exchange techniques

7.1 General

Two data exchange techniques are presented: "HTTP" and "direct TCP". The choice of technique is a national option.

The data exchange techniques for HI-A and HI-B may be different. For instance XML encoding may be used for HI-A, while ASN.1 BER encoding may be used for HI-B. This is a matter for agreement between CSP and Authorized Organization on case-by-case basis.

7.2 HTTP data exchange

7.2.1 Basic configuration

The HTTP data exchange technique uses XML encoding. It uses HTTP [14] (on top of the standard TCP/IP stack).

The HTTP data exchange can be configured as a:

- single client/server configuration;
- mutual client/server configuration.

In a single client/server configuration the initial initiative for data exchange shall be taken by the party with the client. In the mutual client/server configuration both parties can take the initiative to exchange data.

7.2.2 Single client/server

In the single client/server configuration the CSP runs a HTTP server, and the Authorized Organization acts a HTTP client. The HTTP technique is intended to be used with the Authorized-Organization-initiated message flows in clause 5.3. The details in clause 7.2.4 also apply to the single client/server model.

The Authorized Organization and CSP shall agree on a common URI format. A single URI shall be used for all HTTP requests.

7.2.3 Mutual client/server

In the mutual client/server configuration both CSP and Authorized Organization run a HTTP server and both CSP and Authorized Organization act as a HTTP client. The HTTP technique is intended to be used with the general message flows in clause 5.2. The details in clause 7.2.4 also apply to the mutual client/server model.

The Authorized Organization and CSP shall agree on a common URI format. The URIs used for the data exchange shall be agreed.

7.2.4 Details common to both single and mutual cases

The HTTP specification mentions several mandatory and optional features. Some features can be useful, while others raise security concerns. Therefore, the following points should be noted.

The POST method shall be used for all requests.

Some HTTP header fields are less useful within the RDHI, or will complicate the handover protocol without adding clear benefits. In particular, headers to do with negotiation of content or language, range-limiting of requests, cache control, and conditional retrieval should be avoided. The CSP and Authorized Organization shall not send header fields unless there is a clear need for those headers.

Proxies can be useful and may be used. However, caching of whatever form shall not be used. The header "Cache-control: no store" may be used to ensure this behaviour. Special care should be taken with the logs kept by proxy servers.

Most requests and responses contain an XML message as their entity-body. Such entity bodies shall specify a content type of text/xml.

It is not acceptable to rely on HTTP status codes as a substitute for RDHI messages. For example, an Authorized Organization may not consider a blank HTTP 200 (OK) as a Req(Ack) message; it must also carry a full and well-formed RDHI Req(Ack) message as its payload.

The use of gzip is recommended.

7.3 Direct TCP data exchange

The direct TCP mechanism uses BER encoding derived from the ASN.1 in annex A. The direct TCP option uses data exchange details on top of the standard TCP/IP stack.

The direct TCP technique shall be used with the General message flows in clause 5.2.

7.3.1 Transport layer

7.3.1.1 Introduction

Clause 6.4 of TS 102 232-1 [3] describes a transport layer that is based on the Transport Control Protocol. TCP is implemented according to RFC 0793 [17], RFC 2581 [18], RFC 2988 [19] and clause 4.2 of RFC 1122 [20]. According to the interface described in clause 4.1 the CSP is the TCP sender and the Requesting Authority is the TCP receiver or contrariwise.

7.3.1.2 TCP settings

The source and destination port numbers shall be within the dynamic port range for TCP. The value of the source port number is chosen by the TCP sender. The allocation of the destination port number is outside the scope of the present document.

TCP "keep-alive" (RFC 1122 [20]) should not be used.

7.3.2 Network layer

The Network layer implements the Internet Protocol according to RFC 0791 [21].

7.3.3 Delivery networks

The choice of the network will be made on a national basis for legal and pragmatic reasons.

8 Security Measures

8.1 General

The use of security measures for RDHI is recommended. The following security measures are optional and may be adopted (in full or in part) on a national basis.

The present document makes a distinction between connection level security and application level security.

NOTE: Connection level security measures are not independent of application level security measures. The XML/HTTP ecosystem has certain techniques, measures, and toolkits (for example for digital signatures) that have been proven to work together well.

8.2 Connection Level Security

The present document considers the electronic interfaces for HI-A and HI-B between the Authorized Organization and CSP as connections. Most practical implementations of such secure connections are at the hardware level, and sometimes at the software level. For securing these connections the following security measures need to be enforced:

- Mutual authentication.
- Confidentiality.

- Integrity.

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

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 can be detected.

ASN.1 and XML are used as HI-A and HI-B interface definition languages. For ASN.1 the recommended security methods are either IPSec or TLS. For XML the recommended security methods are either IPSec or HTTPS [15]. Whatever method is used, authentication, confidentiality and integrity are to be enforced on these connections - for both HI-A and HI-B.

8.3 Application Level Security

Connection level security enables a secure means of connection between Authorized Organization and CSP. Such measures validate and ensure that on the other side of the link there is a trusted equipment or application belonging to the correct entity (Authorized Organization or CSP). However, due to the sensitive nature of retained data, additional security measures are recommended at the application level (for both the ASN.1 and XML methods), similar in some respect to the security measures in TS 102 232-1 [3].

The recommended application level security measures are:

- **Digital signature on RDHI requests for HI-A, by an Authorized Organization entity:**
  Such an entity might be a person authorizing RDHI requests on HI-A (e.g. an Authorized Organization officer or some other person authorized by law or regulation to authorize RDHI requests), or some other entity defined by national law or regulation.
  The process involves the Authorized Organization computing a hash over the entire set of fields in the request (including the time stamp). Then the hash is digitally signed with the entity's private key. The signed hash and the entity's certificate (validating its public key) are sent in the request to the CSP. In effect, the request may be viewed as comprising two parts - one part is composed of the request fields without the signature and certificate, and the other is the signature (of the hash of the first part) and the certificate.
  The CSP may choose to validate the request by computing the request's hash and verifying that it matches the one signed by the Authorized Organization. The CSP may choose to validate the certificate as well. The generation of certificates and the nature of the assigning authority are out of scope of the present document.
  The CSP may choose just to keep the requests with their associated signatures and certificates for audit trail and any other validation or official procedure.

- **Digital signatures on RDHI responses for HI-A, by the CSP:**
  The CSP signs the HI-A responses in exactly the same manner as the Authorized Organization signs the requests, i.e. signing the hash of the entire set of fields (including the time stamp) and sending the signed hash and its certificate (validating its public key) with the set of fields. Such digital signatures may serve the Authorized Organization in judicial procedures to show that responses coming from the CSP are certified by the CSP. This is especially recommended in case the CSP works in such a manner where each request (although electronically sent) is approved by a person.

- **Hashing and digital signatures on HI-B:**
  For the purpose of the Authorized Organization providing court evidence that the retained data is truly CSP originated, the HI-B information is hashed, and these hashes are digitally signed. The HI-B information sent with the hashes and the CSP certificate (validating its public key). The Authorized Organization should keep the digitally signed hashes and certificates together with the data.

For a technical description of these security measures see clause 8.4.

8.4 Technical Security Measures

8.4.1 General

NOTE: Connection level security measures are not independent of application level security measures. The XML/HTTP ecosystem has certain techniques, measures, and toolkits (for example for digital signatures) that have been proven to work together well.

8.4.2 Connection Level

The level and implementation of for example the TLS, IPSec and HTTPS security mechanisms are a matter of national regulations.

8.4.3 Application Level

8.4.3.1 Hashes

This is an area for national implementations.

8.4.3.2 Digital Signatures

All digital signatures in the present document are DSS/DSA signatures according to FIPS PUB 186-2 [13].

8.4.3.3 HI-B Non-Repudiation

In order to allow the authorities to verify the authenticity of the received data, hashes over the HI-B data may be sent. This verification may be used when the collected data is planned for evidential purposes.

SHA-1 hash are computed and signed by DSS/DSA Signature. The digitally signed hashes are created for:

- the entire HI-B data when sent in ***one*** bulk/message/transaction as a consequence of one HI-A request; or
- a part of HI-B data when sent in ***one*** bulk/message/transaction as a consequence of one HI-A request.

The digitally signed hash is always sent with its data, and not in subsequent transfers, for simplicity. This way there is an association of one digitally signed hash to one data transfer, and no hash coverage lapses occur. It is assumed that one HI-B bulk/message/transaction pertains to only one HI-A request.

In the case of multi-part HI-B transmissions, the RecordNumber (which starts from zero for each HI-B set of responses) will be used in a sequential consecutive manner to number the records sent. Each subsequent HI-B transmission will start with the next sequential RecordNumber. This is to ensure that the Authorized Organization is able to make sure that the entire information has been received. The "Res" response (as opposed to the "ResInc") will indicate the last HI-B transmission for a specific request. The "Res" response will include RecordNumber as well conforming to this scheme.

8.4.3.4 Digital Signatures and Message Structure

The RetainedDataMessage defined in clause A.3.2.1 contains the RetainedDataDigest. Although the use of digest is optional (yet recommended), the RetainedDataMessage shall always be used for all messages. When the digest is not used, the retainedDataDigest will not be populated.

When the digest is used, the RetainedDataHeader and RetainedDataPayload will be each separately BER encoded. The BER encoded fields will be used to populate their appropriate place in the message. A hash will be computed over the combined BER encoded fields (RetainedDataHeader and RetainedDataPayload, in this order). The hash will be digitally signed and be used to populate the retainedDataDigest field.

For this purpose, two separate ASN.1 definition modules have been provided in annex A.

Annex A (normative): Data fields

A.1 Summary

A.1.1 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 CSP and Authorized Organization shall use the present document data dictionary.

The present document does not supersede the EU Data Retention Directive [1] or national legislation.

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

- Those elements that are required to meet technical delivery requirements are marked ***MANDATORY (M)***.
- Some elements are explicitly required to be retained by the EU Data Retention Directive [1], but their availability depends on network and other technical properties (e.g. if held by a third party). These are marked as ***CONDITIONAL (C)***.
- It is for national agreement to determine the situations in which the elements marked ***OPTIONAL (O)*** are stored or delivered. The present document does not address the circumstances in which it is required to 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.

The tables in clauses B.2, C.2, etc., assign each element M, C or O according to these definitions. Some of the lowest-level parameters are not listed in the tables in B.2, C.2, etc.: they are defined only in the ASN.1 in clauses B.3, C.3, etc. Such elements have the same status (M, C or O) as their parent.

NOTE 1: It is up to national legislation to decide whether and under what conditions the elements marked as Optional are required. Also, national legislation may decide for each Conditional field its status when the condition is not met.

NOTE 2: In the formal ASN.1 listing, the word OPTIONAL is used as defined in the ASN.1 language, and is therefore not directly linked to the definition above.

A.1.2 Choice of data modelling language

The structure of the data is defined in ASN.1. An 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.

A.1.3 Overview

The data structure is broken down in the following way:

- Message headers e.g. identifying information that is present on all messages (definitions in clause 6 and ASN.1 in clause A.3.2).
- Common fields i.e. parameters that might be used in more than one type of service (definitions in clause A.2 and ASN.1 in clause A.3.3).
- Service-specific fields i.e. parameters that are only used in relation to one particular service (There is one annex for each service. Parameter definitions are in clauses B.2, C.2, etc. and ASN.1 in clauses B.3, C.3, etc.).

A.2 Parameter definition for common fields

A.2.1 RetainedDataHeader

A.2.1.1 Parameters

The RetainedDataHeader structure is populated as per clauses 5 and 6. The parameters are as follows.

Table A.1: RetainedDataHeader parameters

Field name	Value	M/C/O (see clause A.1.1)
requested	See clause 6.1.2	M
cSPID	See clause 6.1.3	M
timestamp	See clause 6.1.4	M
thirdPartyCSPID	See clause 6.1.3.2	O

A.2.1.2 RequestID parameters

The RequestID structure uniquely identifies a request. See clause 6.1.2.

Table A.2: RequestID parameters

Field name	Value	M/C/O (see clause A.1.1)
countryCode	See clause 6.1.2.	M
authorisedOrganisationID	See clause 6.1.2.	M
requestNumber	See clause 6.1.2.	O

A.2.2 RetainedDataPayload

A.2.2.1 RequestMessage parameters

The use of the RequestMessage structure is described in clauses 5 and 6.3.2. The parameters are as follows.

Table A.3: RequestMessage parameters

Field name	Value	M/C/O (see clause A.1.1)
requestPriority	See clause 6.3.3.1.	O
requestParameters	See clause 6.3.2.	O
deliveryPointHIB	See clause 5.4.	O
maxHits	See clause 6.3.3.2.	O
nationalRequestParameters	Defined on a national basis.	O

A.2.2.2 RequestAcknowledgement parameters

The use of the RequestAcknowledgement structure is described in clause 5. The parameters are as follows.

Table A.4: RequestAcknowledgement parameters

Field name	Value	M/C/O (see clause A.1.1)
suggestedCompletionTime	Indicative time for expected completion of query.	O

A.2.2.3 ResponseMessage parameters

The use of the ResponseMessage structure is described in clauses 5 and 6.2. The parameters are as follows.

Table A.5: ResponseMessage parameters

Field name	Value	M/C/O (see clause A.1.1)
responseStatus	See clause 6.2.2.2.	O
responsePayload	Required if responseStatus is responseComplete or responseIncomplete (see table A.6).	O
nationalResponsePayload	Defined on a national basis.	O

Table A.6: ResponseRecord parameters

Field name	Value	M/C/O (see clause A.1.1)
recordNumber	See clause 6.2.2.1.	O
recordPayload	See clause 6.2.	O
additionalInformation	See clauses 6.2.2.2 and 6.2.4.	O
nationalRecordPayload	Defined on a national basis.	O

A.2.2.4 GetStatusMessage parameters

The use of the GetStatusMessage structure is described in clause 5. The parameters are as follows.

Table A.7: GetStatusMessage parameters

Field name	Value	M/C/O (see clause A.1.1)
requestNumbers	See clause 5.3.1.	O

A.2.2.5 StatusMessage parameters

The use of the StatusMessage structure is described in clause 5. The parameters are as follows.

Table A.8: StatusMessage parameters

Field name	Value	M/C/O (see clause A.1.1)
statusResponse	See clause 5.3.1.	O

Table A.9: StatusResponse parameters

Field name	Value	M/C/O (see clause A.1.1)
requestNumber	See clause 5.3.1.	O
requestStatus	See clause 5.3.1.	O

A.2.2.6 ErrorMessage parameters

The use of the ErrorMessage structure is described in clauses 5 and 6.4. The parameters are as follows.

Table A.10: ErrorMessage parameters

Field name	Value	M/C/O (see clause A.1.1)
additionalInformation	See clause 6.4.	O

A.2.3 GenericSubscriberInfo

A.2.3.1 Parameters

The GenericSubscriberInfo structure encapsulates common subscriber information in a generic way. This structure is used in multiple service-specific annexes.

If the subscriber is an organization or business, then information can be stored in OrganizationInfo. If the subscriber is an individual, then information can be stored in IndividualInfo. It is a matter for national implementations to decide which structure is appropriate for each service and subscriber.

A.2.3.2 OrganizationInfo parameters

The OrganzationInfo field contains the following parameters.

Table A.11: OrganizationInfo parameters

Field name	Value	M/C/O (see clause A.1.1)
name	Name of the organization.	C
contactDetails	Address and contact details for point of contact.	C
nationalRegistrationID	Provides a unique reference for this organization (e.g. a tax registration number). The format of this field is for national agreement.	O

A.2.3.3 IndividualInfo parameters

The IndividualInfo field contains the following parameters.

Table A.12: IndividualInfo parameters

Field name	Value	M/C/O (see clause A.1.1)
name	Name of the individual.	C
contactAddress	Address and contact details for individual.	C
dateOfBirth	Date of birth.	O
gender	Gender.	O
identificationNumber	Provides a nationally-unique reference number. The format of this field is for national agreement.	O
authenticationInfo	Records how the individual authenticated themselves with the service provider (e.g. passport, utility bill etc). The format of this field is for national agreement.	O

A.3 ASN.1 definitions

A.3.1 General

A.3.1.1 ASN.1 syntax tree

Figure A.1 shows the object identifier tree from the point of view of retained data handling.

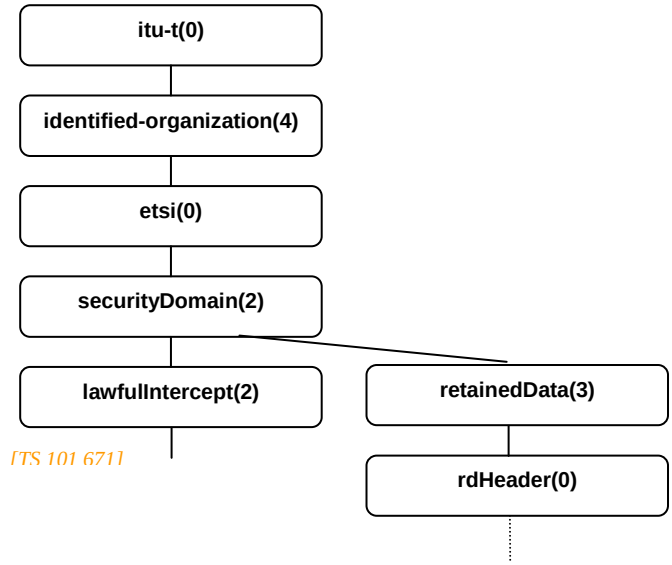


Figure A.1: Object identifier tree

A.3.1.2 General remarks on ASN.1

Clause A.3.2 contains the top levels of the ASN.1 module. 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.

The ASN.1 definitions are contained in an .asn file (TS 102 657, RDMessage, ver2.asn) which accompanies the present document.

A.3.2 ASN.1 Definitions for message headers

A.3.2.1 Message wrappers

```
RDMessage {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) retainedData(3) rdHeader(0)
version2(2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- ============================
-- Object Identifier definitions
-- ============================
```

```
-- RetainedData DomainId
retainedDataDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) retainedData(3)}
```

```
-- rdHeader
rdHeaderId OBJECT IDENTIFIER ::= {retainedDataDomainId rdHeader(0) version2(2)}
```

```
-- ====================================
-- Top level definitions for RDHI wrapper
-- ====================================
```

```
RetainedDataMessage ::= SEQUENCE
{
    rdHeaderId              [0] OBJECT IDENTIFIER,
    retainedDataHeader      [1] RetainedDataHeader,
    retainedDataPayload     [2] RetainedDataPayload,
    retainedDataDigest      [3] OCTET STRING OPTIONAL,
        -- The digitally signed hash of the combined fields above (retainedDataHeader and
        -- retainedDataPayload)
    ...
}
```

A.3.2.2 Message headers

```
-- ============================================================================
-- Definitions for Retained Data header information, present in every message
-- ============================================================================
```

```
RetainedDataHeader ::= SEQUENCE
{
    requestID       [1] RequestID,
    cSPID           [2] CSPID,
    timeStamp       [3] GeneralizedTime,
    thirdPartyCSPID [4] CSPID OPTIONAL,
    ...
}
```

```
CSPID ::= UTF8String
    -- Unique identifier for the CSP that issued the request
```

```
RequestID ::= SEQUENCE
{
    countryCode                 [1] CountryCode,
    authorisedOrganisationID    [2] AuthorisedOrganisationID,
    requestNumber               [3] RequestNumber OPTIONAL,
        -- all messages except GetStatusMessage and StatusMessage have a request number
        -- (see clause 6.1.2)
    ...
}
```

```
CountryCode ::= UTF8String (SIZE(2))
-- A country code as per ISO 3166-1 [4]
```

```
AuthorisedOrganisationID::= UTF8String
-- A unique identifier for an Authorized Organization issuing a Retained Data request
```

```
RequestNumber ::= UTF8String
-- Unique within a given country and Authorized Organization
```

```
-- ================================================
-- Definitions for Retained Data payload information
-- ================================================
```

```
RetainedDataPayload ::= CHOICE
    -- Payload can be a request, response, error or acknowledgement
{
    requestMessage          [1] RequestMessage,
    requestAcknowledgement  [2] RequestAcknowledgement,
    responseMessage         [3] ResponseMessage,
    responseAcknowledgement [4] ResponseAcknowledgement,
    errorMessage            [5] FurtherInformation,
    cancelMessage           [6] CancelMessage,
    cancelAcknowledgement   [7] CancelAcknowledgement,
    getstatusMessage        [8] GetStatusMessage,
    statusMessage           [9] StatusMessage,
    getResultsMessage       [10] GetResultsMessage,
    ...
}
```

```
-- ================================================
-- Definitions of Request message and acknowledgement
-- ================================================
```

```
RequestMessage ::= SEQUENCE
{
    requestPriority             [1] RequestPriority,
    requestParameters           [2] RequestConstraints,
    deliveryPointHIB            [3] DeliveryPointHIB OPTIONAL,
        -- pre-arranged set of delivery address(es) of that specific Authorized Organization
    maxHits                     [4] INTEGER OPTIONAL,
        -- Maximum number of records to be returned.
        -- On a national basis maximum numbers could be considered
        -- In case of maxHit a responseFailed message is sent and no data is sent
        -- (see clause 6.3.3.2)
    nationalRequestParameters   [5] NationalRequestParameters OPTIONAL,
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national requirements
    ...
}
```

```
DeliveryPointHIB ::= UTF8String
```

```
RequestConstraints ::= SEQUENCE
{
    equals                  [1] RetainedDataRecord OPTIONAL,
    notEqualTo              [2] RetainedDataRecord OPTIONAL,
    lessThan                [3] RetainedDataRecord OPTIONAL,
        -- For numerical values
    lessThanOrEqualTo       [4] RetainedDataRecord OPTIONAL,
        -- For numerical values
    greaterThan             [5] RetainedDataRecord OPTIONAL,
        -- For numerical values
    greaterThanOrEqualTo    [6] RetainedDataRecord OPTIONAL,
        -- For numerical values
    startsWith              [7] RetainedDataRecord OPTIONAL,
        -- For strings
    endsWith                [8] RetainedDataRecord OPTIONAL,
        -- For strings
    isAMemberOf             [9] SEQUENCE OF RetainedDataRecord OPTIONAL,
    ...
}
```

```
RequestPriority ::= OCTET STRING
    -- Priority considerations are a matter for national implementation
    -- This standard makes no statement regarding how such priorities are represented or used
```

```
RequestAcknowledgement ::= SEQUENCE
{
    suggestedCompletionTime     [1] GeneralizedTime OPTIONAL,
        -- Indicative time that results will be ready
        -- Purely informational, not binding for either party
    ...
}
```

```
-- ==================================================
-- Definitions of Response message and acknowledgement
-- ==================================================
```

```
ResponseMessage ::= SEQUENCE
{
    responseStatus              [1] ResponseStatus,
    responsePayload             [2] SEQUENCE OF ResponseRecord OPTIONAL,
        -- Clause 6 explains use of this field
        -- A responseUnavailable message shall not have a responsePayload (see clause 5.3.3)
        -- The responseComplete and responseIncomplete message shall have a responsePayload
        -- If there are no responses, the responsePayload is present but has zero entries
    nationalResponsePayload     [3] NationalResponsePayload OPTIONAL,
        -- to be defined on a national basis
        -- only to be used in case the present document cannot fulfil the national requirements
    ...
}
```

```
ResponseStatus  ::= CHOICE
{
    responseComplete    [1] NULL,
        -- No further results to come
    responseIncomplete  [2] NULL,
        -- There may be further results to come
    responseUnavailable [3] NULL,
        -- See clause 6.3.3
    responseFailed      [4] FurtherInformation,
        -- See clauses 6.2.2.2 and 6.3.3.2
    ...
}
```

```
ResponseRecord  ::= SEQUENCE
{
    recordNumber                [1] INTEGER,
    recordPayload               [2] RetainedDataRecord,
    additionalInformation       [3] AdditionalInformation OPTIONAL,
         -- see clause 6.2.4
    nationalRecordPayload       [4] NationalRecordPayload OPTIONAL,
    ...
}
```

```
AdditionalInformation ::= SEQUENCE
{
    contactInformation      [1] UTF8String OPTIONAL,
        -- Name or address of operator or person who may have further information
    otherInformation        [2] UTF8String OPTIONAL,
    ...
}
```

```
RetainedDataRecord ::= CHOICE
{
    telephonyRecord     [1] TelephonyRecord,
    messageRecord       [2] MessageRecord,
    networkAccess       [3] NetworkAccessRecord,
        -- Other services will be included (like multimedia) as they are implemented
    ...
}
```

```
ResponseAcknowledgement ::= CHOICE
{
    -- Acknowledges a response has been sent
    acknowledgeCompleteResults      [1] NULL,
    acknowledgePartialResults       [2] NULL,
    ...
}
```

```
-- ================================================
-- Definitions of an error message and acknowledgment
-- ================================================
```

```
FurtherInformation ::= SEQUENCE
{
    information         [1] UTF8String,
    contactInformation  [2] UTF8String OPTIONAL,
    ...
}
```

```
-- ================================================
-- Definitions of a cancel message and acknowledgement
-- ================================================
```

```
CancelMessage ::= NULL
    -- Cancels an active request
```

```
CancelAcknowledgement ::= NULL
    -- Acknowledges the receipt of a cancel message (no other information required)
```

```
-- ================================================
-- Definitions of status request and response messages
-- ================================================
```

```
GetStatusMessage ::= SEQUENCE
{
    requestNumbers      [1] SEQUENCE OF RequestNumber,
    ...
}
```

```
StatusMessage ::= SEQUENCE
{
    statusResponse      [1] SEQUENCE OF StatusResponse,
    ...
}
```

```
StatusResponse ::= SEQUENCE
{
    requestNumber   [1] RequestNumber,
    requestStatus   [2] RequestStatus,
    ...
}
```

```
RequestStatus ::= CHOICE
{
    ready                       [1] NULL,
    incompleteResultsReady      [2] NULL,
    failureResponseReady        [3] NULL,
    notReady                    [4] NULL,
    error                       [5] FurtherInformation,
    inDelivery                  [6] NULL,
    invalidRequestID            [7] NULL,
    ...
}
```

```
-- ========================================
-- Definitions of status get results messages
-- ========================================
```

```
GetResultsMessage ::= NULL
    -- No further information required (the RequestID is given in the header)
```

```
-- ====================
-- National parameters
-- ====================

NationalRequestParameters ::= SEQUENCE
{
    countryCode     [1] UTF8String (SIZE (2)),
        -- Country Code according to ISO 3166-1 [4],
        -- the country to which the parameters inserted after the extension marker apply.
    ...
        -- In case a given country wants to use additional national parameters according to its law,
        -- these national parameters should be defined using the ASN.1 syntax and added after the
        -- extension marker (...).
        -- It is recommended that an version indicator is included in the national parameters
        -- definition.
}

NationalResponsePayload ::= SEQUENCE
{
    countryCode     [1] UTF8String (SIZE (2)),
        -- see comment in NationalRequestParameters
    ...
}

NationalRecordPayload ::= SEQUENCE
{
    countryCode     [1] UTF8String (SIZE (2)),
        -- see comment in NationalRequestParameters
    ...
}
```

A.3.3 ASN.1 definitions for common fields

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

```
-- ============================================
-- Definitions for Generic Subscriber Information
-- ============================================

GenericSubscriberInfo ::= SEQUENCE
{
    organizationInfo    [1] OrganizationInfo OPTIONAL,
    individualInfo      [2] IndividualInfo OPTIONAL,
    ...
}
```

```
OrganizationInfo ::= SEQUENCE
{
    name                    [1] UTF8String OPTIONAL,
        -- name of the organization
    contactDetails          [2] ContactDetails OPTIONAL,
        -- address, and name/phone number of a point of contact
    nationalRegistrationID  [3] UTF8String OPTIONAL,
        -- e.g. social security number
    ...
}
```

```
IndividualInfo ::= SEQUENCE
{
    name                    [1] PersonName OPTIONAL,
    contactAddress          [2] ContactDetails OPTIONAL,
    dateOfBirth             [3] GeneralizedTime OPTIONAL,
    gender                  [4] ENUMERATED
    {
        male(0),
        female(1),
        ...
    } OPTIONAL,
    identificationNumber    [5] UTF8String OPTIONAL,
    authenticationInfo      [6] AuthenticationInfo OPTIONAL,
    ...
}
```

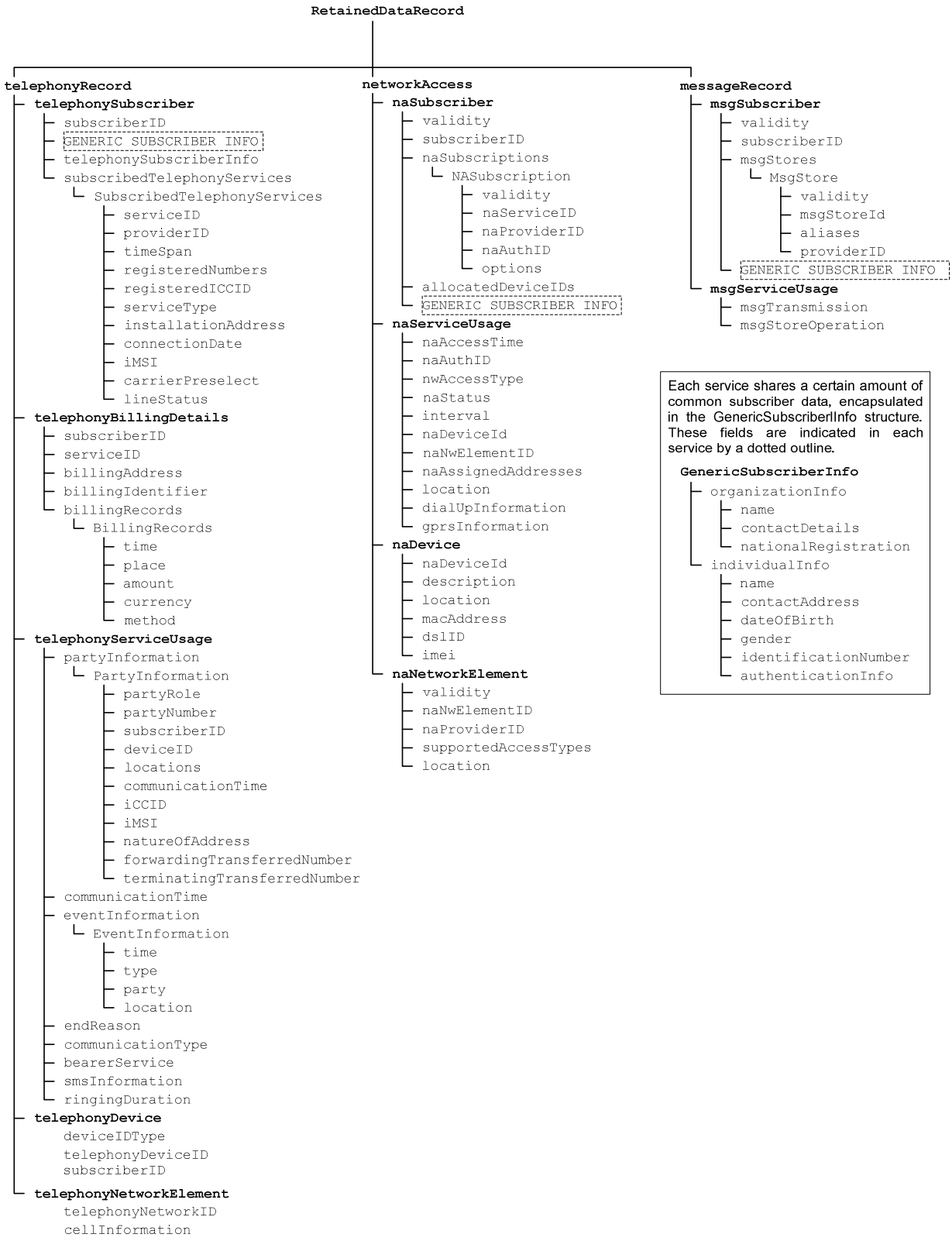
```
PersonName ::= SEQUENCE
{
    salutation              [1] UTF8String OPTIONAL,
    surname                 [2] UTF8String OPTIONAL,
        -- the non-chosen or inherited name of an individual, e.g. "Arend"
    surnamePrefix           [3] UTF8String OPTIONAL,
        -- any prefix before the surname, e.g. "von", "van der"
    surnameSuffix           [4] UTF8String OPTIONAL,
        -- any suffix after the surname, e.g. "Jr", "III"
    middleNames             [5] UTF8String OPTIONAL,
        -- that part of the name excluding forename, separable and preceding the surname
    firstname               [6] UTF8String OPTIONAL,
        -- the first name or initials, e.g. "Peter"
    ...,
    secondsurname           [7] UTF8String OPTIONAL,
        -- a second surname is used in several countries
    secondsurnamePrefix     [8] UTF8String OPTIONAL,
    secondsurnameSuffix     [9] UTF8String OPTIONAL
}
```

```
ContactDetails ::= SEQUENCE
{
    address         [1] AddressInformation OPTIONAL,
    emailAddress    [2] UTF8String OPTIONAL,
    contactNumber   [3] SEQUENCE OF PartyNumber OPTIONAL,
        -- several numbers (work, home, mobile) may be given for a single subscriber
    ...
}
```

```
AddressInformation ::= SEQUENCE
{
    flatNumber      [1] UTF8String OPTIONAL,
    buildingName    [2] UTF8String OPTIONAL,
    buildingNumber  [3] UTF8String OPTIONAL,
    streetName      [4] UTF8String OPTIONAL,
    poBox           [5] UTF8String OPTIONAL,
        -- PO box or Response number
    postalCode      [6] UTF8String OPTIONAL,
        -- Postal code. Example: 2289AC
    region          [7] UTF8String OPTIONAL,
    province        [8] UTF8String OPTIONAL,
    language        [9] UTF8String OPTIONAL,
    city            [10] UTF8String OPTIONAL,
    country         [11] CountryCode OPTIONAL,
        -- Country code as defined in ISO 3166-1 [4]
    validity        [12] TimeSpan OPTIONAL,
        -- time from which the address was registered
    ...
}
```

```
AuthenticationInfo ::= SEQUENCE
{
    authenticationType      [1] UTF8String OPTIONAL,
        -- the type of document used to authenticate, e.g. passport, driver's license
    authenticationNumber    [2] UTF8String OPTIONAL,
        -- the number of the document used to authenticate
    ...
}
```

A.3.4 Schematic representation of top level ASN.1



NOTE: This figure should be regarded only as an aid to understanding. In the event of a discrepancy between this figure and the text of the ASN.1 specification the ASN.1 specification is the leading one.

Figure A.2: Schematic representations of the major ASN.1 structures for three services

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

B.1 Scope

Telephony services covers those services offering the facilities listed below. It covers services that provide PSTN/ISDN functionality (either offered over PSTN/ISDN or emulated PSTN/ISDN over IP) including GSM/UMTS-CS and SMS.

A user may expect a service that offers the capability e.g. to:

- Dial telephone 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.

B.2 Telephony fields

B.2.1 General

This clause describes the fields and parameters of the Telephony ASN.1 definitions given in clause B.3. This clause should be read in conjunction with the notes in the ASN.1 definitions themselves and the definitions in clause A.1.1.

B.2.2 Telephony Subscriber

B.2.2.1 Subscriber ID

SubscriberID is a unique identifier for a particular subscriber within a CSP, for example an account number. The format and content of this field is for CSPs to determine. The only requirement is that the subscriber ID is unique for each subscriber within the CSP.

Table B.1: TelephonySubscriber parameters

Field name	Value	M/C/O (see clause A.1.1)
`subscriberID`	A unique identifier for a particular subscriber within a CSP.	C

B.2.2.2 GenericSubscriberInfo

Common information such as name and address is stored the GenericSubscriberInfo structure. This is defined the service-independent annex A.

B.2.2.3 TelephonySubscriberInfo

Information about the subscriber which is specific to telephony services is contained in the TelephonySubscriberInfo structure. This is for further study.

B.2.2.4 SubscribedTelephonyServices

B.2.2.4.1 Description

There shall be a SubscribedTelephonyService structure for each subscription the subscriber holds. The parameters are as follows.

Table B.2: SubscribedTelephonyServices parameters

Field name	Value	M/C/O (see clause A.1.1)
serviceID	A unique identifier within the operator for the service or tariff subscribed to.	O
providerID	A unique identifier for the service provider. The format of this field is to be determined by national agreement.	O
timeSpan	Time over which the subscription was held. If the subscription is active, the endTime shall not be populated.	O
registeredNumbers	The telephone number(s) assigned to the subscriber as part of this subscription, if applicable (multiple e.g. in GSM for voice/fax/data, ISDN MSNs).	O
serviceType	The type of service subscribed to.	O
installationAddress	The installation address for the subscriber's equipment, if applicable.	O
billingDetails	Details of the subscribers billing history - see clause B.2.2.4.2.	O

B.2.2.4.2 BillingDetails

The BillingDetails structure gives information about the subscribers billing history for a particular subscription. The parameters are as follows.

Table B.3: BillingDetails parameters

Field name	Value	M/C/O (see clause A.1.1)
billingAddress	The billing address for this subscription.	O
billingIdentifier	A unique identifier for billing purposes. The format of this field is for CSPs to determine.	O
billingRecords	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause B.2.2.4.3.	O

B.2.2.4.3 BillingRecords

Each billing record contains information for a particular payment. The parameters are as follows.

Table B.4: BillingRecords parameters

Field name	Value	M/C/O (see clause A.1.1)
time	Time of the payment.	O
place	Location of the payment.	O
amount	The amount of the payment, in currency specified.	O
currency	Currency of payment, in ISO 4217 [5] format.	O
method	Type of payment (e.g. credit card, top-up voucher). The format of this field is for agreement with the CSP.	O

B.2.3 Telephony ServiceUsage

B.2.3.1 Parameters

The TelephonyServiceUsage structure is used for service usage information, such as call data records. The parameters are as follows.

Table B.5: TelephonyServiceUsage parameters

Field name	Value	M/C/O (see clause A.1.1)
partyInformation	A list of partyInformation structures (see clause B.2.3.2).	C
communicationTime	Total time for this service usage. Not that the time of involvement of individual parties may be shorter (see clause B.2.3.2).	C
eventInformation	A list of telephony events that occurred during this call. Telephony events may relate to Call Forwarding, Conference Calls, Messaging, etc. (listed in the ASN.1 in clause B.3).	O
endReason	The Q.850 cause code for the termination of the call.	O
communicationType	The type of call.	C
bearerService	The bearer service for the call.	C
smsInformation	SMS information for the service usage, if applicable.	O
ringDuration	Ring duration, given in seconds.	O

B.2.3.2 PartyInformation

A PartyInformation structure is filled in for each party involved in the communication. The parameters are as follows.

Table B.6: PartyInformation parameters

Field name	Value	M/C/O (see clause A.1.1)
partyRole	Role for this party (e.g. called, calling).	C
partyNumber	Number for this party in E.164 format.	C
subscriberID	Subscriber identifier, unique identifier for subscriber (see clause B.2.2.1).	O
deviceID	Device identifier.	C (see note 1)
locations	Location(s) encountered during a call.	O (see note 2)
communicationTime	Time that this party was involved in the call, if this was a multiparty call. Shall be omitted if it is the same as the time of the whole service usage (see clause B.2.3.1).	O
iCCID	Integrated Circuit Card ID (ICCID) number of the party, in ASCII format.	O
iMSI	IMSI of the party.	C
natureOfTheAddress	Nature of the address - may be "International number", "national number" or "subscriber number".	O
forwardedTransferredNumber	Forwarded number if call was transferred.	O
terminatingTransferredNumber	Terminating number if call was transferred.	O
NOTE 1: Further information is given in EU DRD [1], clause 5.e.2. NOTE 2: For mobile calls, only the start location is explicitly mentioned in the EU DRD [1].		

B.2.4 TelephonyDevice

B.2.4.1 General

The TelephonyDevice structure is used to describe devices such as mobile handsets.

Table B.7: TelephonyDevice parameters

Field name	Value	M/C/O (see clause A.1.1)
deviceIDType	Indicates the type of identifier used in TelephonyDeviceID, e.g. IMEI. (See ASN.1 for permissible types).	C
telephonyDeviceID	Unique identifier for the telephony device. If this identifier happens to have a particular format (e.g. IMEI), then this may be indicated using deviceIDType.	C
subscriberID	Identity of a known user of this equipment. This identity may be registered in cases where the provider has supplied the user with a device. It may also be recorded ad-hoc based on service usage data, depending on national legislation.	O

B.2.5 TelephonyNetworkElement

B.2.5.1 General

The TelephonyNetworkElement structure is used to describe network elements such as mobile cells.

Table B.8: TelephonyNetworkElement parameters

Field name	Value	M/C/O (see clause A.1.1)
telephonyNetworkID	Unique identifier for the network element (e.g. MSC ID).	O
cellInformation	Location information for this network element. See location parameters below (clause B.2.5.2).	C
validity	Time period during which the information given in this structure is or was valid.	O

B.2.5.2 Location parameters

B.2.5.2.1 General

The Location structure contains location information for the network element. This information is contained in a Location structure, which has been taken from TS 101 671 [6].

Table B.9: Location parameters

Field name	Value	M/C/O (see clause A.1.1)
e164-Number	E.164 number in ISUP format (see EN 300 356 [7]).	O
globalCellID	Global cell ID in TS 100 974 [8] format.	C
rAI	Routing Area Identifier in current SGSN, in 3GPP TS 24.008 [9] format, without Routing Area Identification IEI (only last 6 octets are used).	O
gsmLocation	GSM location, details as defined in clause B.3.	C
umtsLocation	UMTS location, details as defined in clause B.3.	C
sAI	Service Area Identifier, in 3GPP TS 25.431 [10] format.	O
oldRAI	Routing Area Identifier in old SGSN, in 3GPP TS 24.008 [9] format, without Routing Area Identification IEI (only last 6 octets are used).	O
postalLocation	Postal address of the location.	O

B.2.5.2.2 GSM Location Information

Table B.10: GSMLocation parameters

Field name	Value	M/C/O (see clause A.1.1)
geoCoordinates	Geographical latitude-longitude location. Formats as described in ASN.1.	O
utmCoordinates	Universal Transverse Mercator location. Formats of individual fields described in ASN.1 comments.	O
utmRefCoordinates	Universal Transverse Mercator reference co-ordinates.	O
wGS84Coordinates	WGS84 co-ordinates, format as defined in 3GPP TS 03.32 [12].	O

B.2.5.2.3 UMTS Location Information

Table B.11: UMTSLocation parameters

Field name	Value	M/C/O (see clause A.1.1)
point	Geographical latitude-longitude location. Latitudes and longitudes specified as integers, with additional latitude sign.	O
pointWithUncertainty	Geographical latitude-longitude location with additional uncertainty code to indicate radius of uncertainty.	O
polygon	Sequence of latitude-longitude locations that define a polygon.	O

B.3 ASN.1 definitions for telephony

```
TelephonyRecord ::= CHOICE
{
    telephonySubscriber          [1] TelephonySubscriber,
    telephonyBillingDetails      [2] TelephonyBillingDetails,
    telephonyServiceUsage        [3] TelephonyServiceUsage,
    telephonyDevice              [4] TelephonyDevice,
    telephonyNetworkElement      [5] TelephonyNetworkElement,
    ...
}
```

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

```
TelephonySubscriber ::= SEQUENCE
{
    subscriberID                    [1] TelephonySubscriberId OPTIONAL,
        -- unique identifier for this subscriber, e.g. account number
    genericSubscriberInfo           [2] GenericSubscriberInfo OPTIONAL,
        -- generic personal information about this subscriber
    telephonySubscriberInfo         [3] TelephonySubscriberInfo OPTIONAL,
        -- service-specific information about this subscriber
    subscribedTelephonyServices     [4] SEQUENCE OF SubscribedTelephonyServices OPTIONAL,
        -- a subscriber (or account) may have more than one service listed against them
    ...
}
```

```
TelephonySubscriberId ::= UTF8String
    -- unique identifier for this subscriber, e.g. account number
```

```
TelephonySubscriberInfo ::= NULL
    -- Reserved
```

```
SubscribedTelephonyServices ::= SEQUENCE
{
    serviceID               [1] UTF8String OPTIONAL,
        -- Unique identifier for this service within the operator
    providerID              [2] UTF8String OPTIONAL,
        -- Unique identifier for the service provider
    timeSpan                [3] TimeSpan OPTIONAL,
        -- Start and end data, if applicable, of the subscription
    registeredNumbers       [4] SEQUENCE OF PartyNumber OPTIONAL,
        -- The set of telephone numbers registered for this service
    registeredICCID         [5] UTF8String OPTIONAL,
    serviceType             [6] TelephonyServiceType OPTIONAL,
    installationAddress     [7] AddressInformation OPTIONAL,
        -- installation address, if different from the registered address
    connectionDate          [8] GeneralizedTime OPTIONAL,
        -- Date the subscriber was actually connected
        -- (May differ from the start of subscription)
    iMSI                    [9] IMSI OPTIONAL,
    carrierPreselect        [10] BOOLEAN OPTIONAL,
    lineStatus              [11] UTF8String OPTIONAL,
        -- CSP-specific description of current line status, e.g. "Active", "Ceased", etc.
    ...
}
```

```
TelephonyBillingDetails ::= SEQUENCE
{
    subscriberID        [1] TelephonySubscriberId OPTIONAL,
    serviceID           [2] UTF8String OPTIONAL,
    billingAddress      [3] ContactDetails OPTIONAL,
    billingIdentifier   [4] BillingIdentifier OPTIONAL,
    billingRecords      [5] SEQUENCE OF BillingRecords OPTIONAL,
    ...
}
```

```
BillingIdentifier ::= OCTET STRING
    -- Used to correlate billing information
    -- useful if the bill-payer is not the subscriber, e.g. company mobiles
```

```
BillingRecords ::= SEQUENCE
{
    time                [1] GeneralizedTime OPTIONAL,
    place               [2] UTF8String OPTIONAL,
    amount              [3] REAL OPTIONAL,
    currency            [4] UTF8String (SIZE(3)) OPTIONAL,
        -- as per ISO 4217 [5]
    method              [5] UTF8String OPTIONAL,
        -- i.e. credit card etc.
    ...
}
```

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

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

```
TelephonyServiceUsage ::= SEQUENCE
{
    partyInformation        [1] SEQUENCE OF TelephonyPartyInformation OPTIONAL,
        -- 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 OPTIONAL,
        -- Time and duration of the communication
    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,
    ringDuration            [8] INTEGER OPTIONAL,
    ...
}
```

```
TelephonyPartyInformation ::= SEQUENCE
{
    partyRole                       [1] TelephonyPartyRole OPTIONAL,
    partyNumber                     [2] PartyNumber OPTIONAL,
    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
    communicationTime               [6] TimeSpan OPTIONAL,
        -- Time and duration of the communication
    iCCID                           [7] UTF8String OPTIONAL,
        -- Integrated Circuit Card ID (ICCID) number of the party, in ASCII format
    iMSI                            [8] IMSI OPTIONAL,
    natureOfAddress                 [9] UTF8String OPTIONAL,
        -- Nature of address indicator, e.g. "National", "International"
    forwardedTransferredNumber      [10] PartyNumber OPTIONAL,
    terminatingTransferredNumber    [11] PartyNumber OPTIONAL,
    ...
}
```

```
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,
        -- format as per 3GPP TS 23.040 [16]
    smsNumOfSM      [5] INTEGER (0..65535) OPTIONAL,
    smsNotifyInd    [6] BOOLEAN OPTIONAL,
    smsProtocolId   [7] OCTET STRING (SIZE(1)) OPTIONAL,
        -- format as per 3GPP TS 23.040 [16]
    ...
}
```

```
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 ::= CHOICE
{
    basicEventType              [1] BasicEventType,
    callConferenceEventType     [2] CallConferenceEventType,
    callForwardingEventType     [3] CallForwardingEventType,
    messagingEventType          [4] MessagingEventType,
    prepayServiceEventType      [5] PrepayServiceEventType,
    ...
}
```

```
BasicEventType ::= 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),
    tpyInvoke(16),
    tpyPrivateComm(17),
    serviceActivation(18),
    transit(19),
    mSOriginating(20),
    callForwarding(21),
    mSTerminating(22),
    ...
}
```

```
CallForwardingEventType ::= ENUMERATED
{
    cfuActivation(1),
    cfuModification(2),
    cfuDe-activation(3),
    cfcNoReplyActivation(4),
    cfcNoReplyModification(5),
    cfcNoReplyDe-activation(6),
    cfcBusyActivation(7),
    cfcBusyModification(8),
    cfcBusyDe-activation(9),
    cfcOutOfRangeActivation(10),
    cfcOutOfRangeModification(11),
    cfcOutOfRangeDe-activation(12),
    cfcUnavailableActivation(13),
    cfcUnavailableModification(14),
    cfcUnavailableDe-activation(15),
    cfuFaxActivation(16),
    cfuFaxModification(17),
    cfuFaxDe-activation(18),
    ...
}
```

```
CallConferenceEventType ::= ENUMERATED
{
    confBeginSeizure(1),
    confAdd(2),
    confSplit(3),
    confIsolate(4),
    confReattach(5),
    confDrop(6),
    confBeginActive(7),
    ...
}
```

```
MessagingEventType ::= ENUMERATED
{
    mSOriginatingSMSinMSC(1),
    mSTerminatingSMSinMSC(2),
    shortMessageDelivery(3),
    mMMessage(4),
    mMNotification(5),
    mMDeliveryReport(6),
    mMReadReply(7),
    ...
}
```

```
PrepayServiceEventType ::= ENUMERATED
{
    serviceActivation(1),
    ...
}
```

```
TelephonyLocation ::= SEQUENCE
{
    telephonyNetworkID  [1] TelephonyNetworkID OPTIONAL,
        -- ID of the network element location (e.g. Cell ID)
    timeSpan            [2] TimeSpan OPTIONAL,
        -- 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
{
    deviceIDType        [1] ENUMERATED
        -- Type of identifier for telephony device
    {
        unknown(0),
        imei(1),
        macAddress(2),
        ...
    } OPTIONAL,
    telephonyDeviceID   [2] TelephonyDeviceID OPTIONAL,
        -- Unique identifier for this telephony device according to type of identifier
    ...,
    subscriberID        [3] TelephonySubscriberId OPTIONAL
        -- Identifier for a known user of this equipment.
        -- Usage of this parameter is subject to national legislation.
}
```

```
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 OPTIONAL,
    cellInformation     [2] Location OPTIONAL,
        -- The Location information id
    validity            [3] TimeSpan OPTIONAL,
    ...
}
```

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

```
-- ====================
-- Location information
-- ====================

Location ::= SEQUENCE
{
    e164-Number         [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
        -- Coded in the same format as the ISUP location number (parameter
        -- field) of the ISUP (see EN 300 356 [7])
    globalCellID        [2] OCTET STRING (SIZE (5..7)) OPTIONAL,
        -- See MAP format (see TS GSM 09.02 [8])

    rAI                 [3] OCTET STRING (SIZE (6)) OPTIONAL,
        -- The Routeing Area Identifier (RAI) in the current SGSN is coded in accordance with
        -- 3GPP TS 24.008 [9] without the Routing Area Identification IEI (only the
        -- last 6 octets are used)
    gsmLocation         [4] GSMLocation OPTIONAL,
    umtsLocation        [5] UMTSLocation OPTIONAL,
    sAI                 [6] OCTET STRING (SIZE (7)) OPTIONAL,
        -- format:  PLMN-ID 3 octets (no. 1-3)
        --          LAC     2 octets (no. 4-5)
        --          SAC     2 octets (no. 6-7)
        --          (according to 3GPP TS 25.431 [10])
    oldRAI              [7] OCTET STRING (SIZE (6)) OPTIONAL,
        -- the "Routeing Area Identifier" in the old SGSN is coded in accordance with
        -- 3GPP TS 24.008 [9] without the Routing Area Identification IEI
        -- (only the last 6 octets are used)
        -- This parameter is duplicated from 3GPP TS 33.108 [11]
    ...,
    postalLocation      [8] AddressInformation OPTIONAL
}
```

```
GSMLocation ::= CHOICE
{
    geoCoordinates      [1] SEQUENCE
    {
        latitude    [1] UTF8String (SIZE(7..10)) OPTIONAL,
            -- format: XDDMMSS.SS
        longitude   [2] UTF8String (SIZE(8..11)) OPTIONAL,
            -- format: XDDDMMSS.SS
        mapDatum    [3] MapDatum OPTIONAL,
        azimuth     [4] INTEGER (0..359) OPTIONAL,
            -- The azimuth is the bearing, relative to true north
        ...
    },
        -- format: XDDMMSS.SS (on latitudes) or XDDDMMSS.SS (on longitudes)
        --      X           : N(orth), S(outh), E(ast), W(est)
        --      DD or DDD   : degrees (numeric characters)
        --      MM          : minutes (numeric characters)
        --      SS.SS       : seconds, the second part (.SS) is optional
        -- Example:
        --      latitude (short form)       N502312
        --      longitude (long form)       E1122312.18
    utmCoordinates      [2] SEQUENCE
    {
        utm-Zone    [1] UTF8String (SIZE(3)) OPTIONAL,
        utm-East    [2] UTF8String (SIZE(6)) OPTIONAL,
        utm-North   [3] UTF8String (SIZE(7)) OPTIONAL,
            -- Universal Transverse Mercator
            -- example  utm-Zone    32U
            --          utm-East    439955
            --          utm-North   5540736
        mapDatum    [4] MapDatum OPTIONAL,
        azimuth     [5] INTEGER (0..359) OPTIONAL,
            -- The azimuth is the bearing, relative to true north
        ...
    },
    utmRefCoordinates   [3] SEQUENCE
    {
        utm-GridZone                [1] UTF8String (SIZE(2)) OPTIONAL,
            -- numerals from 1 to 60
        utm-GridBand                [2] UTF8String (SIZE(1)) OPTIONAL,
            -- character between C and X
        squareID                    [3] UTF8String (SIZE(2)) OPTIONAL,
            -- characters from A to Z
        numericalLocationEasting    [4] UTF8String (SIZE(5)) OPTIONAL,
        numericalLocationNorthing   [5] UTF8String (SIZE(5)) OPTIONAL,
            -- Universal Transverse Mercator Reference = Military Grid Reference System (MGRS)
            -- example  utm-GridZone               32
            --          utm-GridBand               U
            --          squareID                   PU
            --          numericalLocationEasting   9129
            --          mumericalLocationNorthing  4045
            -- In both panels, utm-GridBand and squareID the 'I' and 'O' characters are not used
            -- because of their similarity to the digits one and zero.
        mapDatum                [6] MapDatum OPTIONAL,
        azimuth                 [7] INTEGER (0..359) OPTIONAL,
            -- The azimuth is the bearing, relative to true north
        ...
    },
    wGS84Coordinates    [4] OCTET STRING,
        -- format is as defined in 3GPP TS 03.32 [12]
    ...,
    geoCoordinatesDec   [5] SEQUENCE
    {
        latitudeDec     [1] UTF8String (SIZE(3..12)) OPTIONAL,
            -- format: XDD.nnnnnnnn
        longitudeDec    [2] UTF8String (SIZE(4..13)) OPTIONAL,
            -- format: XDDD.nnnnnnnn
        mapDatum        [3] MapDatum OPTIONAL,
        azimuth         [4] INTEGER (0..359) OPTIONAL,
            -- The azimuth is the bearing, relative to true north
        ...
    }
```

```
        -- format: XDD.nnnnnnnn (on latitudes) or XDDD.nnnnnnnn (on longitudes)
        --      X           : N(orth), S(outh), E(ast), W(est)
        --      DD or DDD   : degrees (numeric characters)
        --      nnnnnnnn    : post decimal positions (numeric characters)
        -- Example:
        --      latitude        N50.38666667
        --      longitude       E112.38671670
}
```

```
MapDatum ::= ENUMERATED
{
    wGS84(1),
        -- World Geodetic System 1984
    wGS72(2),
    eD50(3),
        -- European Datum 50
    rD(4),
        -- Rijks Driehoek (Netherlands)
    potsdamDatum(5),
    datumAustria(6),
    eTRS89(7),
        -- European Terrestrial Reference System 1989
    nAD27(8),
        -- North American Datum 1927
    oSGB36(9),
        -- Ordnance Survey of Great Britain
    oSNI52(10),
        -- Ordnance Survey of Northern Ireland
    tM65(11),
    iTM(12),
        -- Irish Transverse Mercator
    ...
}
```

```
UMTSLocation ::= CHOICE
{
    point                   [1] GA-Point,
    pointWithUnCertainty    [2] GA-PointWithUnCertainty,
    polygon                 [3] GA-Polygon,
    ...
}
```

```
GeographicalCoordinates ::= SEQUENCE
{
    latitudeSign    [1] ENUMERATED
    {
        north,
        south
    } OPTIONAL,
    latitude        [2] INTEGER (0..8388607) OPTIONAL,
    longitude       [3] INTEGER (-8388608..8388607) OPTIONAL,
    ...
}
```

```
GA-Point ::= SEQUENCE
{
    geographicalCoordinates     [1] GeographicalCoordinates,
    ...
}
```

```
GA-PointWithUnCertainty ::=SEQUENCE
{
    geographicalCoordinates     [1] GeographicalCoordinates,
    uncertaintyCode             [2] INTEGER (0..127)
}
```

```
maxNrOfPoints                   INTEGER ::= 15
```

```
GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF GA-Polygon-Elements
```

```
GA-Polygon-Elements ::= SEQUENCE
{
    geographicalCoordinates     [1] GeographicalCoordinates,
    ...
}
```

```
-- ====================
-- General definitions
-- ====================
```

```
PartyNumber ::= UTF8String
    -- E164 address of the node in international format
```

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

C.1 Scope

Asynchronous messaging services cover asynchronous communications involving the intermediate storage of messages. This includes e-mail, webmail but excludes chat, which is synchronous, and excludes SMS.

The facilities a user may expect to find are e.g.:

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

SMS is handled under "telephony services", and is excluded from this annex.

Figure C.1 illustrates the relations between subscribers and message service providers. It also illustrates the operations on message stores, and message transmissions (dotted lines).

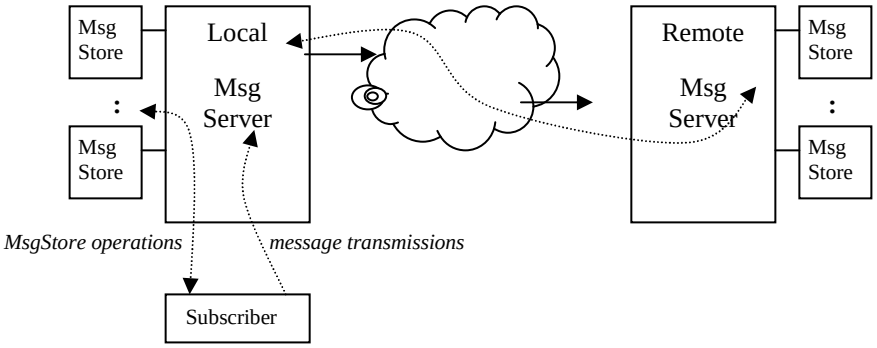


Figure C.1: Schematic overview of message handling

When messages are delivered to a message server, the server will temporarily store that message in a store. At a later time, an authorized subscriber can access the message store, and retrieve the message. Subscribers can perform other operations on message stores, such as deleting or adding messages.

C.2 Descriptions

C.2.1 General

This clause describes the fields and parameters of the Asynchronous Message ASN.1 definitions given in clause C.3. This clause should be read in conjunction with the notes in the ASN.1 definitions themselves.

C.2.2 MsgSubscriber

This structure contains the information on the subscriber, and the subscribed services, independent on actual usage.

Table C.1: MsgSubscriber parameters

Field name	Value	M/C/O (see clause A.1.1)
validity	Time period during which the information given in this structure is or was valid.	O
subscriberID	A unique identifier for this particular subscriber within the CSP.	O
msgStores	Descriptions of the private message stores associated with this subscriber. See clause C.2.4.	O
subscriber	Common information such as name and address is stored the GenericSubscriberInfo structure. This is defined the service-independent annex A.	C

C.2.3 MsgSubscriberID

A unique identifier for subscribers within a CSP. This could be an account name, subscriber number, or any other identification assigned by the CSP.

C.2.4 MsgStore

This structure contains the information on a particular message store, including the addresses associated with this message store.

Table C.2: MsgStore parameters

Field name	Value	M/C/O (see clause A.1.1)
Validity	Time period during which the information given in this structure is or was valid.	O
msgStoreID	A unique identifier for this particular message store within the CSP.	O
aliases	The complete list of all addresses that get delivered into this message store. This may (as a national option) include wildcard addresses (e.g. "@example.com"), meaning that all email to that domain is delivered into the message store.	C
providerID	A unique identifier of the provider hosting this message store.	O

C.2.5 MsgStoreID

A unique identifier for message stores. This could be a mailbox name, or any other identification used by the CSP's message server.

C.2.6 MsgAddress

A messaging address, i.e. an address to which messages can be sent. In the case of Internet e-mail this will be an RFC0822-style address [23]. Other messaging systems (e.g. X.400) use their own messaging addresses.

C.2.7 MsgProviderID

A unique identifier for messaging service providers. This could, for example, be the company name, or company registration number.

C.2.8 MsgServiceUsage

This structure contains the information on the activities performed by a subscriber. There are two types of actions: those that manipulate message stores, and the sending of a new message.

C.2.9 MsgTransmission

This structure contains all information on the sending of a message by a subscriber. For some services delivery failures result in a separate error message being returned to the sender. Bounced messages then result into two separate transmissions: the message sent by the subscriber and the error message sent by the remote message server.

Table C.3: MsgTransmission parameters

Field name	Value	M/C/O (see clause A.1.1)
dateTime	Date and time when the subscriber submitted the message to the CSP's message server.	C
subscriberID	Unique identifier of the subscriber sending the message.	C
senderAddress	The available address of the sender (see note).	C
recipients	The list of all available recipients of the message (see note).	C
msgStores	List of all local message stores that received a copy of the message. This is both relevant for incoming messages, and for outgoing messages that have a local recipient.	O
deliveryStatus	Result of the transmission from the CSP's message server towards the final destination. Final delivery may pass through a number of intermediate message servers. This field does not indicate the end-to-end delivery status. It indicates the status of the "next hop".	O
protocol	Message transmission protocol used.	O
clientID	IP address of the source of the message transmission.	C
serverID	IP address of the destination of the message transmission.	O
messageID	Unique identifier for the message - for example RFC 0822 [23] message-id header.	O
sourceServerName	Name for the server sending the message (if appropriate).	O
destinationServerName	Name for the server receiving the message (if appropriate).	O
NOTE: Depending on implementation and national discussion, some addresses may not be available, or may not be checked or reliable		

C.2.10 MsgStoreOperation

This structure contains all information on the manipulation of a message store by a subscriber.

Table C.4: MsgStoreOperation parameters

Field name	Value	M/C/O (see clause A.1.1)
dateTime	Date and time when the subscriber performed the indicated operation.	C
subscriberID	Unique identifier of the subscriber performing the operation.	C
msgStore	Unique identifier of the message store being manipulated.	O
operation	Type of manipulation performed by the subscriber.	C
senderAddress	The available address of the sender (see note).	C
recipients	List of all the available recipients of the message (see note).	C
protocol	Message store manipulation protocol.	O
clientID	IP address of the subscriber who performed the indicated operation.	C
serverID	IP address of the message server hosting the message store being manipulated.	O
messageID	Unique identifier for the message - for example RFC 0822 [23] message-id header.	O
NOTE: Depending on implementation and national discussion, some addresses may not be available, or may not be checked or reliable.		

C.3 ASN.1 definitions for asynchronous message services

```
MessageRecord ::= CHOICE
{
    msgSubscriber           [1] MsgSubscriber,
    msgServiceUsage         [2] MsgServiceUsage,
    ...
}
```

```
-- ====================================
-- Definitions of Message Subscriber Data
-- ====================================
```

```
MsgSubscriber ::= SEQUENCE
    -- Generic information on a service subscriber, supplemented with information specific to
    -- asynchronous message services
{
    validity        [1] TimeSpan OPTIONAL,
    subscriberID    [2] MsgSubscriberID OPTIONAL,
    msgStores       [3] SEQUENCE OF MsgStore OPTIONAL,
        -- message stores allocated to this subscriber
    subscriber      [4] GenericSubscriberInfo OPTIONAL,
    ...
}
```

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

```
MsgStore ::= SEQUENCE
    -- Location into which messages are temporarily stored. All asynchronous message services by
    -- definition require some message store. E.g. in the case of e-mail this will be a mailbox
{
    validity        [1] TimeSpan OPTIONAL,
    msgStoreID      [2] MsgStoreID OPTIONAL,
    aliases         [3] SEQUENCE OF MsgAddress OPTIONAL,
        -- The complete list of all addresses that get delivered into this message store.
    providerID      [4] MsgProviderID OPTIONAL,
    ...
}
```

```
MsgStoreID ::= OCTET STRING
   -- Unique identifier of the message store. Since not all IDs will necessarily be human
   -- readable, a generic byte string is used
```

```
MsgAddress ::= UTF8String
   -- Messaging address, an address to which messages can be sent. In the case of Internet e-mail
   -- this will be an RFC822-style address
   -- NOTE – as of v1.2.1, this field has changed from OCTET STRING to UTF8String
```

```
MsgProviderID ::= UTF8String
    -- Unique identifier for a service provider, e.g. company name
    -- NOTE – as of v1.2.1, this field has changed from OCTET STRING to UTF8String
```

```
-- ====================================
-- Definitions of Message Service Usage
-- ====================================
```

```
MsgServiceUsage ::= CHOICE
    -- Choice of different types of activities
    -- Manipulation of stored address books is outside the scope
{
    msgTransmission     [1] MsgTransmission,
    msgStoreOperation   [2] MsgStoreOperation,
    ...
}
```

```
MsgTransmission ::= SEQUENCE
    -- Sending of an outgoing message, or reception of an incoming message
{
    dateTime                [1] GeneralizedTime OPTIONAL,
    subscriberID            [2] MsgSubscriberID OPTIONAL,
    senderAddress           [3] MsgAddress OPTIONAL,
    recipients              [4] SEQUENCE OF MsgAddress OPTIONAL,
    msgStores               [5] SEQUENCE OF MsgStoreID OPTIONAL,
        -- List of all local msgStores that received a copy of the message
        -- For transit messages this field is not used
    deliveryStatus          [6] ENUMERATED
    {
        unknown(0),
        succeeded(1),
            -- Delivery might still fail at a subsequent mail server
        failed(2),
            -- E.g. when mailbox quota exceeded (mailbox full)
        retried(3),
            -- Deferred and retried at a later time
        ...
    } OPTIONAL,
    protocol                [7] ENUMERATED
    {
        smtp(0),
        x400(1),
        ...
    } OPTIONAL,
    clientID                [8] IPAddress OPTIONAL,
    serverID                [9] IPAddress OPTIONAL,
    ...,
    messageID               [10] MessageID OPTIONAL,
    sourceServerName        [11] UTF8String OPTIONAL,
    destinationServerName   [12] UTF8String OPTIONAL
}
```

```
MsgStoreOperation ::= SEQUENCE
    -- Manipulation of a message store.
{
    dateTime        [1] GeneralizedTime OPTIONAL,
    subscriberID    [2] MsgSubscriberID OPTIONAL,
    msgStore        [3] MsgStoreID OPTIONAL,
    operation       [4] ENUMERATED
    {
        connect(0),
            -- Successful authorization for access to msgStore
        disconnect(1),
        retrieveMsg(2),
            -- Viewing msg using a webmail client is also considered retrieval
        partialretrieveMsg(3),
            -- E.g. the TOP command in POP3
        deleteMsg(4),
        addMsg(5),
            -- E.g. the APPEND command in IMAP
        ...,
        editMsg(6)
    } OPTIONAL,
    senderAddress   [5] MsgAddress OPTIONAL,
        -- For Internet email, use the From address in the mail headers
    recipients      [6] SEQUENCE OF MsgAddress OPTIONAL,
        -- For Internet email, use the To, CC, and BCC addresses in the mail headers
    protocol        [7] ENUMERATED
    {
        pop(0),
        imap(1),
        ...,
        webmail(2)
    } OPTIONAL,
    clientID        [8] IPAddress OPTIONAL,
    serverID        [9] IPAddress OPTIONAL,
    ...,
    messageID       [10] MessageID OPTIONAL
}
```

```
MessageID ::= UTF8String
   -- Unique identifier for this message, e.g RFC 822 header
```

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

D.1 Scope

Multimedia services are not covered in the present document.

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

E.1 Scope

Network access services covers the services offering a capability to access public networks (typically the internet), including GPRS/UMTS-PS.

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.

E.2 Descriptions

E.2.1 General

This clause describes the fields and parameters of the Network Access ASN.1 definitions given in clause E.3. This clause should be read in conjunction with the notes in the ASN.1 definitions themselves.

E.2.2 NASubscriber

This structure contains the information on the subscriber, and the subscribed services, independent on actual usage.

Table E.1: NASubscriber parameters

Field name	Value	M/C/O (see clause A.1.1)
`validity`	Time period during which the information given in this structure is or was valid.	O
`subscriberID`	A unique identifier for this particular subscriber within the CSP.	C
`naSubscriptions`	List of all known services subscribed to by this user with this CSP.	O
`allocatedDeviceIDs`	List of all known devices allocated to this user. The user may use other devices in addition (or instead of) these devices.	O
`subscriber`	Common information such as name and address is stored the GenericSubscriberInfo structure. This is defined the service-independent annex A.	C

E.2.3 NAServiceSubscription

This structure contains the information on a particular subscription by a subscriber.

Table E.2: NAServiceSubscription parameters

Field name	Value	M/C/O (see clause A.1.1)
validity	Time period during which the information given in this structure is or was valid.	O
naServiceID	A unique identifier for the type of service, e.g. account plan name.	O
naProviderID	A unique identifier for the network access provider, e.g. company name or company registration number.	O
naAuthID	A unique identifier for this particular subscription, e.g. logon name.	C
options	An optional human readable text with restrictions or options to the subscription, e.g. "fixed IP address; max 50 hr/month".	O
installationAddress	The installation address of the subscriber's equipment, if applicable.	O
fixIpAddress	If the CSP assigns a fixed IP address to the subscriber (i.e. not allocated each time the service is used), then this IP address may be populated here.	O
imsi	If the CSP assigns an IMSI to the subscriber, this may be populated here.	O

E.2.4 NAServiceUsage

This structure contains the information on network access and attempted access by a subscriber.

Table E.3: NAserviceUsage parameters

Field name	Value	M/C/O (see clause A.1.1)
naAccessTime	Date and time of the (attempted) network access.	C
naAuthID	Logon name (username) used to obtain network access.	C
nwAccessType	Type of network access attempted. If not undefined(0), this should be one of the types supported by the NAS.	O
naStatus	Results of the access attempt.	O
interval	Start time and end time of network access. Used only if naStatus indicates a success. This is also the period during which the IP address is assigned to this subscriber.	C
naDeviceId	Information on the device used to access the service.	C
naNwElementID	Network element (NAS) onto which the subscriber's device is connected to the service.	O
naAssignedAddress	IP address assigned by the network access service. Depending on the service and type of subscription this may be a fixed address (unique to this subscriber) or dynamic (shared among multiple subscribers), or accompanied by a port number where Port Address Translation is used.	C (see note)
location	Location of the network access, if applicable.	O
dialUpInformation	Information specific to dial-up access (see table E.4).	O
gprsInformation	Information specific to gprs access (see table E.5).	O
NOTE: This is required if the naStatus indicates a successful network access attempt.		

Table E.4: DialUpInformation parameters

Field name	Value	M/C/O (see clause A.1.1)
diallingNumber	Telephone number used at the subscriber side for dial-up access. Used only if **nwAccessType** indicates a dial-up service.	C
dialledNumber	Telephone number used at the network element side for dial-up access.	O
callback	Call back number used for dial-up access. Call back causes the call to be charged by the dial-up network operator to the CSP, not to the subscriber.	O

Table E.5: GPRSInformation parameters

Field name	Value	M/C/O (see clause A.1.1)
iMSI	IMSI associated with the network access.	C
mSISDN	MSISDN associated with the network access.	O
sgsnAddress	IP address of the SGSN.	O
ggsnAddress	IP address of the GGSN.	O
pdp-address-allocated	PDP address allocated for the network access.	O
apn	APN of the network access.	O
pdp-type	PDP type, format as per TS 101 671 [6].	O
gPRSEvent	GPRS event, as per 3GPP TS 33.108 [11].	O

E.2.5 NADevice

This structure contains information on the device used by the subscriber to access the service. It is allowed to use the MAC address, DSL ID, or other ID as the device ID (naDeviceId). MAC addresses can often be changed. If the MAC address is used as the primary device ID, then naDeviceId cannot be guaranteed to be unique (two devices could have the same MAC address).

Table E.6: NADevice parameters

Field name	Value	M/C/O (see clause A.1.1)
naDeviceId	Identifier of this device, e.g. the MAC address.	O
description	Human readable description of the device.	O
location	Installation address of the device, if known.	O
macAddress	MAC or ethernet address as presented to the network.	O
dslID	DSL identifier of the DSL connection to the CSP.	O

E.2.6 NANwElement

This structure contains information on a network access server (NAS).

Table E.7: NANwElement parameters

Field name	Value	M/C/O (see clause A.1.1)
validity	Time period during which the information given in this structure is or was valid.	O
naNwElementID	A unique identifier of this network access server.	O
naProviderID	A unique identifier of the CSP, e.g. company name or company registration number.	O
supportedAccessTypes	The list of access types supported by this network access server.	O
location	Installation address of this network access server, if known and meaningful.	O

E.2.7 NABillingDetails

The NABillingDetails structure gives information about the network access subscriber's billing history for a particular subscription. The parameters are as follows.

Table E.8: NABillingDetails parameters

Field name	Value	M/C/O (see clause A.1.1)
billingAddress	The billing address for this subscription.	O
billingIdentifier	A unique identifier for billing purposes. The format of this field is for CSPs to determine.	O
billingRecords	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause B.2.2.4.3.	O

E.3 ASN.1 definitions for network access services

```
NetworkAccessRecord::= CHOICE
{
    naSubscriber        [1] NASubscriber,
    naServiceUsage      [2] NAServiceUsage,
    naDevice            [3] NADevice,
    naNetworkElement    [4] NANwElement,
    naBillingDetails    [5] NABillingDetails,
    ...
}
```

```
-- ==========================================
-- Definitions of Network Access Subscriber Data
-- ==========================================
```

```
NAProviderID ::= UTF8String
```

```
NAAuthID ::= UTF8String
```

```
NaSubscriberID ::= UTF8String
```

```
NASubscriber ::= SEQUENCE
    -- Generic information on a service subscriber, supplemented with information specific to
    -- network access services.
{
    validity            [1] TimeSpan OPTIONAL,
    subscriberID        [2] NaSubscriberID OPTIONAL,
        -- Unique identifier for this subscriber, e.g. account number
    naSubscriptions     [3] SEQUENCE OF NAServiceSubscription OPTIONAL,
        -- List of all known services subscribed to by this user
    allocatedDeviceIDs  [4] SEQUENCE OF NADeviceId OPTIONAL,
        -- List of all known devices allocated to this user.
    subscriber          [5] GenericSubscriberInfo OPTIONAL ,
        -- Name, address and other generic subscriber information
    ...
}
```

```
NAServiceSubscription ::= SEQUENCE
    -- Description of the subscription to a Network Access service
{
    validity            [1] TimeSpan OPTIONAL,
    naServiceID         [2] UTF8String OPTIONAL,
        -- Identifier for the service, e.g. account plan name.
    naProviderID        [3] NAProviderID OPTIONAL,
        -- Unique identifier for the provider of the service, e.g. company name
    naAuthID            [4] NAAuthID OPTIONAL,
        -- Unique identifier for this subscription, e.g. logon name
    options             [5] UTF8String OPTIONAL,
        -- Human readable text with restrictions or options to the subscription
    installationAddress [6] AddressInformation OPTIONAL,
    fixIpAddress        [7] IPAddress OPTIONAL,
        -- fix assigned IP address
    imsi                [8] IMSI OPTIONAL,
    ...
}
```

```
-- ========================================
-- Definitions of Network Access Service Usage
-- ========================================
```

```
NAServiceUsage ::= SEQUENCE
{
    naAccessTime        [1] GeneralizedTime OPTIONAL,
        -- Time of connection to the NAS
    naAuthID            [2] NAAuthID OPTIONAL,
        -- Username used to obtain network access
    nwAccessType        [3] NwAccessType OPTIONAL,
        -- Type of network access attempted. If not undefined(0), this should be one of the types
        -- supported by the NAS (identified below by naNwElementID)
    naStatus            [4] ENUMERATED
    {
        unknown(0),
        succeeded(1),
            -- Authentication OK and access granted
        failed(2),
            -- Authentication failure (wrong credentials or time out)
        rejected(3),
            -- Rejected by the CSP (e.g. usage limits exceeded)
        ...
    } OPTIONAL,
    interval            [5] TimeSpan OPTIONAL,
        -- Start time and end time (duration) of network access.
    naDeviceId          [6] NADeviceId OPTIONAL,
        -- Device used to access the service
    naNwElementID       [7] NANwElementID OPTIONAL,
        -- Network element (NAS) onto which the naDevice is connected
    naAssignedAddress   [8] SEQUENCE OF NAAssignedAddress OPTIONAL,
        -- IP address assigned by the network access service. May be fixed or dynamic
    location            [9] Location OPTIONAL,
        -- Location of the access (for e.g. GPRS handsets)
    dialUpInformation   [10] DialUpInformation OPTIONAL,
    gprsInformation     [11] GprsInformation OPTIONAL,
    ...
}
```

```
NwAccessType ::= ENUMERATED
{
    undefined(0),
    dialUp(1),
        -- DialUp access
    xDSL(2),
        -- DSL access
    cableModem(3),
        -- Cable access
    lAN(4),
        -- LAN access
    wirelessLAN(5),
        -- Wireless LAN access (e.g. hotspot)
    wimax(6),
    mobilePacketData(7),
        -- Network access over GSM/3GPP GPRS, UMTS, etc.
    ...
}
```

```
DialUpInformation ::= SEQUENCE
{
    diallingNumber      [1] PartyNumber OPTIONAL,
        -- Telephone number used for dial-up access
    dialledNumber       [2] PartyNumber OPTIONAL,
    callback            [3] PartyNumber OPTIONAL,
        -- Call back number used for dial-up access
    ...
}
```

```
GprsInformation ::= SEQUENCE
{
    iMSI                    [1] IMSI OPTIONAL,
    mSISDN                  [2] PartyNumber OPTIONAL,
    sgsnAddress             [3] SEQUENCE OF IPAddress OPTIONAL,
    ggsnAddress             [4] IPAddress OPTIONAL,
    pDP-address-allocated   [5] IPAddress OPTIONAL,
    aPN                     [6] UTF8String OPTIONAL,
    pDP-type                [7] OCTET STRING (SIZE(2)) OPTIONAL,
        -- format as per TS 101 671 [6]
    ...,
    gPRSEvent               [8] GPRSEvent OPTIONAL
        -- format as per 3GPP TS 33.108 [11]
}
```

```
GPRSEvent ::= ENUMERATED
{
    pDPContextActivation(1),
    pDPContextDeactivation(4),
    gPRSAttach(5),
    gPRSDetach(6),
    locationInfoUpdate(10),
        -- sMS ommited from 3GPP TS 33.108 [11],
    pDPContextModification(11),
    servingSystem(12),
    ...
}
```

```
-- ====================================
-- Definitions of Network Access Device
-- ====================================
```

```
NADeviceId ::= UTF8String
```

```
NADevice ::= SEQUENCE
{
    naDeviceId      [1] NADeviceId OPTIONAL,
        -- Identifier of this device.
    description     [2] UTF8String OPTIONAL,
        -- Human readable description of device
    location        [3] Location OPTIONAL,
    macAddress      [4] OCTET STRING (SIZE (6)) OPTIONAL,
        -- MAC or ethernet address
    dslID           [5] UTF8String OPTIONAL,
    imei            [6] IMEI OPTIONAL,
    ...
}
```

```
IMEI ::= OCTET STRING (SIZE(8))
    -- format as per TS GSM 09.02 [8Error! Reference source not found.]
```

```
IMSI ::= OCTET STRING (SIZE(3..8))
    -- format as per TS GSM 09.02 [8]
```

```
-- ====================================
-- Definitions of Message Network element
-- ====================================
```

```
NANwElementID ::= UTF8String
```

```
NANwElement ::= SEQUENCE
    -- In this context, the network element is more commonly referred to as NAS
{
    validity                [1] TimeSpan OPTIONAL,
        -- Period for which this interval is valid
    naNwElementID           [2] NANwElementID OPTIONAL,
        -- Unique ID of this NAS (Network Access Server)
    naProviderID            [3] NAProviderID OPTIONAL,
        -- Unique identifier of the provider managing this NAS.
    supportedAccessTypes    [4] SEQUENCE OF NwAccessType OPTIONAL,
    location                [5] Location OPTIONAL,
    ...
}
```

```
IPAddress ::= CHOICE
{
    iPv4BinaryAddress   [1] OCTET STRING (SIZE(4)),
    iPv6BinaryAddress   [2] OCTET STRING (SIZE(16)),
    iPTextAddress       [3] IA5String (SIZE(7..45)),
    ...
}
```

```
NAAssignedAddress ::= SEQUENCE
{
    addressSetOrRangeOrMask     [1] IPAddressSetOrRangeOrMask OPTIONAL,
    portNumber                  [2] INTEGER OPTIONAL,
        -- populated with the outbound port number
    addressType                 [3] ENUMERATED
    {
        unknown(0),
        internal(1),
        external(2),
        ...
    } OPTIONAL,
    assignedTime                [4] TimeSpan OPTIONAL,
    ...,
    destinationAddress          [5] IPAddress OPTIONAL,
        -- used in cases where a single external IP/port pair is translated to multiple internal
        -- IP/port pairs, with the destination IP/port used to multiplex them
    destinationPort             [6] INTEGER OPTIONAL
        -- used in cases where a single external IP/port pair is translated to multiple internal
        -- IP/port pairs, with the destination IP/port used to multiplex them
}
```

```
IPAddressSetOrRangeOrMask ::= CHOICE
{
    set     [0] SEQUENCE OF IPAddress,
    range   [1] IPRange,
    mask    [2] IPMask
}
```

```
IPRange ::= SEQUENCE
    -- Things like 172.16.10.0/26
{
    prefix          [0] IPAddress,
    subnetlength    [1] INTEGER (1..128)
}
```

```
IPMask ::= SEQUENCE
    -- Things like 172.16.10.0/255.255.255.240
{
    base    [0] IPAddress,
    mask    [1] IPAddress
}
```

```
NABillingDetails    ::= SEQUENCE
{
    subscriberID        [1] NaSubscriberID OPTIONAL,
    serviceID           [2] UTF8String OPTIONAL,
    billingAddress      [3] ContactDetails OPTIONAL,
    billingIdentifier   [4] BillingIdentifier OPTIONAL,
    billingRecords      [5] SEQUENCE OF BillingRecords OPTIONAL,
    ...
}
```

```
END -- end of RDMessage
```

Annex F (informative): Basic set of search routines for Retained Data

F.1 Example set of search routines

F.1.1 Introduction

The purpose of this informative annex is to give some guidance for implementation of specific search routines.

The following set of search routines are given as guidelines. It is a national option to which extent this set is used and possibly extended with additional search cases.

This annex specifies search cases for retrieval of top level record types according to the table F.1.

F.1.2 Summary of search case

Table F.1: Summary of search case

Record type	Clause(s)	Comments, search parameters
Any records		
timeSpan T1-T2		For any search, a time span relating to time of retention is to be provided.
Telephony Record		
telephonySubscriber	F.2.1	Subscriber ID, name, address, phone number (originating/terminating), national registration identifier.
telephonyBillingDetails	F.2.2	Subscriber ID.
telephonyServiceUsage	F.2.3	Phone number (originating/terminating), device ID (IMEI), location (originating).
telephonyDevice	-	Implicit through service usage. Since this is CPE, the identity of which will not be known except in conjunction with usage, it is not relevant to query about it independently.
telephonyNetworkElement	F.2.4	Network element ID, location.
Message Record		
msgSubscriber	F.3.1	Subscriber ID, name, address, message store ID, national registration identifier.
msgServiceUsage	F.3.2	Subscriber ID, sender address, recipient address.
Network Access Record		
naSubscriber	F.4.1	Subscriber ID, name, address, NA device id, national registration identifier, location (of access point), MAC address, DSL ID.
nsServiceUsage	F.4.2	Device ID, location (of access point), MAC address, DSL ID.
naDevice	-	Implicit through service usage or subscriber data. Since this is CPE, the identity of which will not be known except in conjunction with usage, it is not relevant to query about it independently.
naNetworkElement	-	Implicit through service usage. Since this is equipment in the network, which is not specific to any individual user, it is not relevant to query about it independently.

F.1.3 Subscriber records

The subscriber records are retrieved per service by providing the appropriate service-specific subscriber record type, filled in with applicable search parameters.

F.2 Telephony data

F.2.1 Telephony subscriber

Search parameter	Result
subscriberId	Telephony subscriber record with matching subscriber id is returned.
registeredNumber	Subscriber record for telephony service with matching phone number is returned.
name, address	Subscriber record(s) with matching subscriber name and/or address are returned.
nationalRegistration/identificationNumber (any service)	Subscriber record with matching national registration id are returned.

F.2.2 Telephony billing details

The billing details for a specific telephony subscriber will be returned.

Search parameter	Result
subscriberId (telephony)	Billing records for the supplied subscriber id will be returned.

F.2.3 Telephony service usage

Records of telephony service usage will be returned through search on one or more of the following parameters in **partyInformation**:

Search parameter	Result
partyNumber	All telephony service usage records containing the provided party number (originating/terminating) will be returned.
deviceID	All telephony service usage records containing the provided device id (originating/terminating) will be returned (see note).
location	All telephony service usage records made from the provided location (originating) will be returned.
NOTE: In practical use the type of device id will be an IMEI.	

F.2.4 Telephony network element

Searches on telephony network elements are relevant for finding where a certain cell-id is located or which cell-ids are located in a certain area at some given time. Search parameters are one of:

Search parameter	Result
telephonyNetworkID	Entry of a network element ID will return the record containing cell information for this ID (see note 1).
cellInformation (Location data)	Entry of location data will return network element IDs within the specified area (see note 2).
NOTE 1: It ought to be possible to use wildcarding for network ID, which would return a set of matching records, which subsequently may be analyzed to select those which are located within an area of interest. NOTE 2: This assumes that the input parameters can be given according to a format specifying an area and that network elements are searchable based on a delimited area.	

F.3 Messaging data

F.3.1 Message subscriber

Search parameter	Result
subscriberId	Messaging subscriber record with matching subscriber id is returned.
msgStoreId	Subscriber record for messaging service involving the supplied storage id (mailbox id) is returned.
name, address	Subscriber record(s) with matching subscriber name and/or address are returned.
nationalRegistration/identificationNumber	Subscriber record with matching national registration id is returned.

F.3.2 Message service usage

Usage records for message services may be found through the following parameters of **msgTransmission**.

Search parameter	Result
subscriberID (for messaging)	Service usage records for the given subscriber ID will be returned.
senderAddress	Usage records, which contain a sender address matching the entry, will be returned.
recipients	Usage records, which contain a recipient address matching the entry, will be returned.

F.4 Network Access data

F.4.1 NA subscriber

Search parameter	Result
subscriberId	Subscriber record with matching subscriber id is returned.
name, address	Subscriber record(s) with matching subscriber name and/or address are returned.
nationalRegistration/identificationNumber	Subscriber record with matching national registration id is returned.

In addition to this, the following parameters in **allocatedDeviceIDs** may be used to retrieve network access subscriber data:

Search parameter	Result
naDeviceId	Subscriber record containing the given device ID will be returned (see note).
location	Subscriber record containing the given location will be returned.
macAddress	Subscriber record containing the given MAC address will be returned.
dslID	Subscriber record containing the given DSL ID will be returned.
naAssignedAddress	Usage records containing the given IP address will be returned.
NOTE: It is assumed that a network access device (typically a DSL or cable modem) relates to a specific subscribed access service.	

F.4.2 NA service usage

Searches for NA service usage can be made based on the user device, as recorded in **naDevice**:

Search parameter	Result
naDeviceId	Usage records containing the given device ID will be returned.
location	Usage records containing the given location will be returned.
macAddress	Usage records containing the given MAC address will be returned.
dslID	Usage records containing the given DSL ID will be returned.

Annex G (informative): Examples of search routines

G.1 Introduction

This annex gives extra details for how to implement a number of search routines described in annex F.

Each clause takes an example request from annex F, and shows how it would be constructed using this handover standard. The example shows the inputs (listed in annex F), and a diagram representing the PDU for the request message.

G.2 Example for telephony subscriber query in clause F.2.1

This clause describes how to construct the following telephony subscriber request, described in clause F.2.1.

The specific question is: Please provide data for subscriptions with telephone number 0123456789, which were started in the time span between 1 August 2008 and 15 September 2008.

Request Parameter	Value
registeredNumber	Subscriber record for telephony service with matching phone number is returned.
timeSpan	A range of times for the start of the subscription.

```
RetainedDataMessage
 ├ retainedDataHeader
 │  └ (header information, as described in clause 6.1)
 └ retainedDataPayload
    └ requestMessage
       ├ requestPriority = = NORMAL (per national implementation)
       └ requestParameters
          ├ equals
          │  └ telephonyRecord
          │     └ telephonySubscriber
          │        └ subscribedTelephonyServices
          │           └ registeredNumber = 0123456789
          ├ greaterThan
          │  └ telephonyRecord
          │     └ telephonySubscriber
          │        └ subscribedTelephonyServices
          │           └ timeSpan
          │              └ startTime = 20080801000000Z
          └ lessThan
             └ telephonyRecord
                └ telephonySubscriber
                   └ subscribedTelephonyServices
                      └ timeSpan
                         └ startTime = 20080915235959Z
```

G.3 Example for telephony service usage query in clause F.2.3

This clause describes how to construct the following telephony subscriber request, described in clause F.2.3.

The specific question being asked is: Please provide service usage records for phone number 0123456789 for calls, which were initiated from that number between 5 September 2008 and 15 September 2008.

Request Parameter	Value
partyNumber	Telephone number of interest in the call.
partyRole	Role (originating or terminating) of the telephone number specified. To request all calls involving the given number, regardless of its role, this parameter can be omitted.
timeSpan	A range of times for the start of the call.

```
RetainedDataMessage
 ├ retainedDataHeader
 │  └ (header information, as described in clause 6.1)
 └ retainedDataPayload
    └ requestMessage
       ├ requestPriority = NORMAL (per national implementation)
       └ requestConstraints
          ├ equals
          │  └ telephonyRecord
          │     └ telephonyServiceUsage
          │        └ partyInformation
          │           ├ partyNumber = 0123456789
          │           └ partyRole = 0 (=originating-Party)
          ├ greaterThan
          │  └ telephonyRecord
          │     └ telephonyServiceUsage
          │        └ communicationTime
          │           └ timeSpan
          │              └ startTime = 20080905000000Z
          └ lessThan
             └ telephonyRecord
                └ telephonyServiceUsage
                   └ communicationTime
                      └ timeSpan
                         └ startTime = 20080915235959Z
```

NOTE: Regarding the response records returned in this example: provided a record meets the criteria in the request, then both the begin- and end-time can be included in the response (if they are part of the communication record).

Annex H (informative): Further information on data categories

H.1 General

There is a distinction between data categories that are based on user activity (such as Usage data) and those that are independent of user or network activity - information not generated or processed by network elements (such as Subscriber or Network Element information).

The distinction in type of request is made to allow national adaptation of the present document. The distinctions can be necessary for different levels of authorizations and/or providers. The distinction for different levels of authorizations and/or providers can also be met by national adaptation of the field delivered in the reply. A single request can contain a combination of types (e.g. a, b and c for a generic activity request).

EXAMPLE: A Subscriber Data Request even within one nation can have different levels of authorizations: billing information and/or a PUK-code will not be part of a "standard" request.

H.2 Further information on subscriber data

H.2.1 Subscriber data requests

The following records could be used to make a subscriber data request:

a) Name.

b) Address.

c) Postcode (with street number).

d) National ID no.

e) Birth date.

f) Service identifier
(e.g. phone/network number, email address, IP-addresses, device-ID, log on names, etc.).

g) Location.

Ad g): Discussion on prepaid identification.

In order to be selective a combination of entries can be made. The allowed single and combined entries are a national issue.

H.2.2 Generic subscriber data records

This clause contains the Subscriber Data Reply information. As this information is not derived from network information it can be structured more open and might not be addressed in the network based clauses.

The reply to a subscriber data request will depend on the structure and the fields available in the CSP's subscriber database and the national juridical framework.

In general the reply contains:

a) Names.

b) Addresses.

c) Birth dates.

d) Service identifier.

e) Authentication.

f) Applicable services.

g) Applicable supplementary services.

h) Service association.

i) Timestamp.

Ad a): Multiple names, addresses and birth dates can be available for the subscriber, billing and phonebook information.

Ad d): The service identification can be the phone numbers, email addresses, permanent IP-addresses, log on names, conference call identifier, etc.

Ad e): Depending on national regulations, no authentication information will be given, type will be given (credit card, passport etc) or details will be given (credit card number, passport number, etc).

Ad f): The applicable services can be given as type of subscriptions and as a list of applicable network services. (For example a mobile subscription can be called "Budget II" and can give access to all GSM services excluding GPRS and UMTS, also a limitative list GSM, GPRS, UMTS-PS, and UMTS-CS could be given.

Ad g): The entry can be associated with CSP activated services like call bearing, ex- number, carrier pre-select, 0800/0900 number, multiple SIM, PUK-code, etc.

Ad h): A service identifier is associated with a specific service or tele service (for example a MS-ISDN can be associated with a service like GSM and/or UMTS and within GSM it can also associate to the tele service voice, fax or data).

H.2.3 Service Specific Subscriber Reply Data

a) Service identifier.

b) Applicable services.

c) Applicable supplementary services.

d) Service association.

e) Timestamp.

H.3 Further information on usage data

H.3.1 Usage requests

Usage requests would typically be based on:

a) Network addresses (for example IMSI, email, IP-address).

b) User addresses (for example (MS-)ISDN, email, URI).

c) Hardware address (device-ID for example IMEI, MAC).

d) Location (for example CellID).

H.3.2 Usage data categories

Usage data can be broken down into the following sub-categories:

a) Usage: Traffic data.

b) Usage: Traffic data related information.

c) Usage: Communication independent user activities.

d) Usage: Network activity data.

H.3.3 Usage: Traffic Data (Reply)

In general the reply contains:

a) Network addresses.

b) User addresses.

c) Communication entity.

d) Tele-/bearer service used.

e) Supplementary service.

f) Timestamp.

Ad c): The association of the network/user address with the role in the communication (A, B, C-address, FROM/TO/CC/BCC, etc).

H.3.4 Usage: Traffic Data related information (Reply)

In general the reply contains:

a) Hardware address.

b) Location.

c) Timestamp.

H.3.5 Usage: communication independent user activities (Reply)

In general the reply contains:

a) User associated log on/off.

b) (de)activation of supplementary services.

c) Pre paid updates.

d) Timestamp.

H.3.6 Usage: network Activity Data (Reply)

In general the reply contains:

a) Equipment/Network associated log on/off.

b) Roaming information.

c) Timestamp.

H.4 Further information on network element data

H.4.1 Network element requests

Network element requests would typically be based on:

a) Location.

b) Network element.

Ad a): The association between a location in WGS84 or Postcode to the likely CellIDs can be requested.

Ad b): The association of for example between a CellID and its location and direction can be requested.

H.4.2 Network Configuration Data Reply Data

In general the reply contains:

a) Location association with network elements.

b) Network element association with location.

c) Timestamp.

Annex I (informative): Manual techniques

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 (clause 5) 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 clause 6.
- Lower layers (encoding, transport, etc) (clause 7) in general would not be followed. Where appropriate, consistent encoding schemes are recommended.

Annex J (informative): Informative mapping of data fields to the EU Data Retention Directive

Table J.1 provides an informative mapping of data fields to the EU Data Retention Directive [1].

Table J.1: Mapping of data fields to the EU Data Retention Directive

Table	Field name(s)	Clause of Article 5 that explicitly mentions these fields
A.2.10	Name, ContactDetails	1.a.1.ii / 1.a.2.iii / 1.b.1.ii / 1.b.2.ii
A.2.11	Name, ContactAddress	1.a.1.ii / 1.a.2.iii /1.b.1.ii /1.b.2.ii
B.2.5	PartyInformation,	1.a.1.i / 1.b.1.i / 1.e.1.i / 1.e.2.i
B.2.5	CommunicationTime	1.c.1
B.2.5	CommunicationType	1.d.1
B.2.5	BearerService	1.d.1
B.2.6	PartyRole, PartyNumber,	1.a.1.i / 1.b.1.i / 1.e.1.i / 1.e.2.i
B.2.6	DeviceID	1.e.2.iii / 1.e.2.v
B.2.6	Location	1.f.1
B.2.7	DeviceIDType, TelephonyDeviceID	1.e.2.iii / 1.e.2.v
B.2.8	TelephonyNetworkID, CellInformation	1.f.2
B.2.9	GlobalCellID, GsmLocation, UmtsLocation	1.f.2
C.2.1	Subscriber	1.a.2.iii / 1.b.2.ii
C.2.2	Aliases	1.a.2.i
C.2.3	DateTime	1.c.2.ii
C.2.3	SenderAddress	1.a.2.i
C.2.3	Recipients	1.b.2.i
C.2.3	ClientID	1.d.2
C.2.4	DateTime	1.c.2.ii
C.2.4	SenderAddress	1.a.2.i
C.2.4	Recipients	1.b.2.i
C.2.4	ClientID	1.d.2
E.2.1	Subscriber	1.a.2.iii
E.2.2	NaAuthID	1.c.2.i
E.2.3	AccessTime	1.c.2.i
E.2.3	NaAuthID	1.c.2.i
E.2.3	Interval, naAssignedAddress	1.c.2.i
E.2.3	naDevice	1.e.3.ii
E.2.3	DialInNumber	1.e.3.i

Annex K (informative): Change Request History

Status of the present document: TS 102 657 Handover interface for the request and delivery of retained data		
Date	**Version**	**Remarks**
October 2008	V1.1.1	First publication of the TS after approval by ETSI/TC LI#19 (30 September - 2 October 2008; Prague) (Withdrawn!!) Rapporteur is Mark Shepherd (NTAC)
December 2008	V1.1.2	Re-publication of First publication of the TS 102 657 v1.1.1 + attachments is to be withdrawn. Correction needed because of modifications made in draft v1.1.1 by editHelp during publication process without informing ETSI/TC LI. ASN.1 and XML attachments are brought in line with ASN.1 definition in the specification. PvdA
February 2009	V1.2.1	Included Change Requests: TS102657CR001r1 (Cat F) Error message information clarifications TS102657CR002r1 (Cat F) Revised error message information TS102657CR003r1 (Cat C) Inclusion of RDHI UMTS fields TS102657CR005r2 (Cat B) Inclusion of subscriberID in telephonyDevice TS102657CR006r1 (Cat C) Adding postal location information to Location TS102657CR007 (Cat C) Additional fields for NAT/PAT support TS102657CR008r1 (Cat C) Changes to email specification TS102657CR010r1 (Cat C) Adding decimal geoCoordinates to GSMLocation TS102657CR011 (Cat F) Cleanup Corrections TS102657CR012 (Cat B) Additional fields for second surname in ASN.1 “PersonName” definition These CRs were approved by TC LI#20 (3 - 5 February; Levi) Version 1.2.1 prepared by Mark Canterbury (HO UK)

History

Document history		
V1.1.1	November 2008	Publication (withdrawn)
V1.1.2	December 2008	Publication
V1.2.1	June 2009	Publication