ETSI TS 102 657 V2.5.1 (2025-05)

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

Reference
RTS/LI-00277

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

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

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

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

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

Modal verbs terminology

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

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

1 Scope

The present document is based on requirements from ETSI TS 102 656 [i.2].

The present document contains handover requirements and a handover specification for the data that is identified in national legislations on Retained Data.

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

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

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

[1] Void.

[2] Void.

[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 code".

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

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

NOTE: ETSI TS 101 671 is in status "historical" and is not maintained.

[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+); Mobile Application Part (MAP) specification (3GPP TS 09.02)".

[9] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".

[10] Void.

[11] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[12] ETSI TS 101 109 (V7.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Geographical Area Description (GAD) (3GPP TS 03.32 version 7.2.0 Release 1998)".

[13] FIPS PUB 186-5: "Digital Signature Standard (DSS)".

[14] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

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

[16] ETSI TS 123 040: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Technical realization of the Short Message Service (SMS) (3GPP TS 23.040)".

[17] IETF RFC 793: "Transmission Control Protocol".

[18] IETF RFC 5681: "TCP Congestion Control".

NOTE: IETF RFC 5681 obsoletes IETF RFC 2581: "TCP Congestion Control".

[19] IETF RFC 6298: "Computing TCP's Retransmission Timer".

NOTE: IETF RFC 6298 obsoletes IETF RFC 2988: "Computing TCP's Retransmission Timer".

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

[21] IETF RFC 791: "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] Void.

[24] IETF RFC 5322: "Internet Message Format".

NOTE: IETF RFC 5322 obsoletes IETF RFC 2822: "Internet Message Format".

[25] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[26] IETF RFC 3261: "SIP: Session Initiation Protocol".

[27] IETF RFC 4506: "XDR: External Data Representation Standard".

[28] ISO 13616-1:2020: "Financial services — International Bank Account Number (IBAN) — Part 1: Structure of the IBAN".

NOTE: Used in the attached ASN.1 or XSD documents available in ts_102657v020501p0.zip.

[29] ISO 9362:2022: "Banking — Banking Telecommunication Messages — Business identifier code (BIC)".

NOTE: Used in the attached ASN.1 or XSD documents available in ts_102657v020501p0.zip.

[30] Void.

[31] ETSI TS 125 413: "Universal Mobile Telecommunications System (UMTS); UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling (3GPP TS 25.413)".

[32] ETSI TS 129 274: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (3GPP TS 29.274)".

[33] ETSI TS 129 061: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (3GPP TS 29.061)".

[34] ETSI TS 129 118: "Universal Mobile Telecommunications System (UMTS); LTE; Mobility Management Entity (MME) - Visitor Location Register (VLR) SGs interface specification (3GPP TS 29.118)".

[35] ETSI TS 123 272: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2 (3GPP TS 23.272)".

[36] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)".

NOTE: Used in the attached ASN.1 or XSD documents available in ts_102657v020501p0.zip.

[37] W3C® Recommendation 21 March 2017: "XML Path Language (XPath) 3.1".

[38] ETSI TS 123 008: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Organization of subscriber data (3GPP TS 23.008)".

[39] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[40] Void.

[41] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification (3GPP TS 23.003)".

[42] ETSI TS 138 413: "5G; NG-RAN; NG Application Protocol (NGAP) (3GPP TS 38.413)".

NOTE: Used in the attached ASN.1 or XSD documents available in ts_102657v020501p0.zip.

[43] ETSI TS 129 571: "5G; 5G System; Common Data Types for Service Based Interfaces; Stage 3 (3GPP TS 29.571)".

[44] ETSI TS 136 413: "LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) (3GPP TS 36.413)".

[45] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".

[46] ETSI TS 132 291:"5G; Telecommunication management; Charging management; 5G system, charging service; Stage 3 (3GPP TS 32.291)".

[47] ETSI TS 132 255: "5G; Telecommunication management; Charging management; 5G data connectivity domain charging; Stage 2 (3GPP TS 32.255)".

[48] ETSI TS 129 520: "5G; 5G System; Network Data Analytics Services; Stage 3 (3GPP TS 29.520)".

[49] ETSI TS 132 251: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Charging management; Packet Switched (PS) domain charging (3GPP TS 32.251)".

[50] ETSI TS 137 340: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; NR; Multi-connectivity; Overall description; Stage-2 (3GPP TS 37.340)".

[51] Recommendation ITU-T Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part".

[52] Recommendation ITU-T E.164: "The international public telecommunication numbering plan".

[53] GSMA™ SGP.02: "Remote Provisioning Architecture for Embedded UICC Technical Specification".

NOTE: Used in the attached ASN.1 or XSD documents available in ts_102657v020501p0.zip.

[54] Recommendation ITU-T G.984.1: "Gigabit-capable passive optical networks (GPON): General characteristics".

NOTE: Used in the attached ASN.1 or XSD documents available in ts_102657v020501p0.zip.

[55] IETF RFC 7315: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP".

[56] ETSI TS 123 558: "5G; Architecture for enabling Edge Applications (3GPP TS 23.558)".

[57] ISO 24165-2: "Digital token identifier (DTI) — Registration, assignment and structure — Part 2: Data elements for registration".

[58] ISO/IEC 10646: "Information technology — Universal coded character set (UCS)".

[59] ETSI TS 123 316: "5G; Wireless and wireline convergence access support for the 5G System (5GS)".

[60] IEEE™ EUI: "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)".

2.2 Informative references

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

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

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Recommendation ITU-T X.400: "Message handling system and service overview".

[i.2] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Authorized Organization (AO): 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

issuing 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

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

receiving authority: any entity possessing the necessary authority pursuant to law and the technical means to receive retained subscriber information or traffic data delivered by a service provider

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

response to request of information: response from the CSP to the authorized organization 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)

SG: Interface between Mme and an MSC/VLR

transmission of information: transmission of retained data from the CSP to the receiving authority

3.2 Symbols

Void.

3.3 Abbreviations

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

NOTE: Some abbreviations are only used in the ASN.1 or XSD documents available in ts_102657v020501p0.zip.

3GPP	3rd Generation Partnership Project
5G	5th Generation
5GS	5G System
ACID	Application Client ID
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
AMF	Access and Mobility management Function
AMFID	AMF IDentifier
AO	Authorized Organization
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
ASP	Application Service Provider
BER	Basic Encoding Rules
BIC	Business Identifier Code
CAN	Connectivity Access Network
CellID	Cell Identification
CGI	Cell Global Identity
CHF	CHarging Function
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CR	Change Request
CS	Circuit Switched

CSP	Communications Service Provider
CSPID	CSP IDentifier
DLT	Digital Ledger Technology
DNN	Data Network Name
DR	Data Retention
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSS	Digital Signature Standard
DTI	Digital Token Identifier
DVD	Digital Versatile Disc or Digital Video Disc
EAS	Edge Application Server
eCGI	e-UTRAN Cell Global ID
ECSP	Edge Computing Service Provider
EECID	Edge Enabler Client ID
EID	Embedded (UICC) IDentifier
EMS	Enhanced Messaging Service
EN-DC	E-UTRA-NR Dual Connectivity
EPC	Enhanced Packet Core
EPS	Evolved Packet System
ESMA	European Securities Markets Authority
eUICC	embedded UICC
eUTRAN	evolved UMTS Terrestrial Radio Access Network
FIPS	Federal Information Processing Standard
GCI	Global Cable Identifier
GGSN	Gateway GPRS Support Node
GLI	Global Line Identifier
GPRS	General Packet Radio Service
GPSI	Generic Public Subscription Identifier
GSM	Global System for Mobile communications
GW	GateWay
HI	Handover Interface
HI-A	Handover Interface A
HI-B	Handover Interface B
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
IANA	Internet Assigned Numbers Authority
IBAN	International Banking Account Number
ICCID	Integrated Circuit Card ID
ID	IDentifier
IE	Information Element
IEI	Information Element Identifier
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMEISV	IMEI Software Version
IMPI	IP Multimedia Private Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifiers
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol (version 4)
IPv6	Internet Protocol (version 6)
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
LAN	Local Area Network
LTE	3GPP Long Term Evolution (4G)
MAC	Media Access Control
MCC	Mobile Country Code
ME	Mobile Equipment
MF-B	Mediation Function B

MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MoIP	Multimedia over IP
MS	Mobile Station
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN number
MSN	Multiple Subscriber Number
N3IWF	Non 3GPP InterWorking Function
NA	Network Access
NAI	Network Access Identifier
NAS	Network Access Server
NAT	Network Address Translation
NCGI	NR Cell Global Identity
NCI	NR Cell Identity
NF	Network Function
NGAP	Next Generation Application Protocol
NR	New Radio
PAT	Port Address Translation
PDN	Public Data Network
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
P-GW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PS	Packet Switched
PSTN	Public Switched Telephone Network
PUK	Personal Unblocking Key
QoS	Quality of Service
RAI	Routing Area Identifier
RAN	Radio Access Network
RAT	Radio Access Technology
RCI	Radio Configuration Identifier
RD	Retained Data
RDHI	Retained Data Handover Interface
SAI	Service Area Identifier
SC	SMS Centre
SD	Slice Differentiator
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMF	Session Management Function
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNSSAI	Single Network Slice Selection Assistance Information
SSID	Service Set IDentifier
SST	Slice/Service Type
SUPI	SUbscriber Permanent Identifier
TAI	Tracking Area Identity
TC	Technical Committee
TCP	Transmission Control Protocol
TL	Latency Time
TLS	Transport Layer Security
TP-PID	Transfer Layer Protocol - Protocol IDentifier
TR	Time of the Request
TV	TeleVision
UDM	Unified Data Management
UDP	User Datagram Protocol

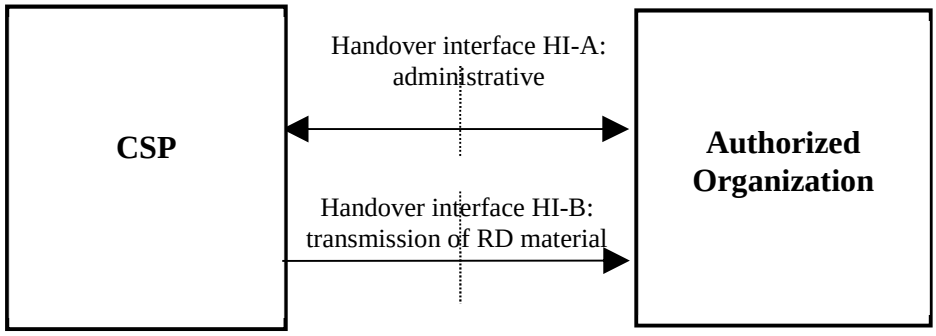
UE	User Equipment
UMS	Unified Messaging System
UMTS	Universal Mobile Telecommunication System
UPF	User Plane Function
URI	Uniform Resource Identifier
UTC	Universal Time Coordinated
UTF	Unicode Transformation Format
UTM	Universal Transverse Mercator
UTRAN	UMTS Terrestrial Radio Access Network
UUID	Universally Unique IDentifier
VAT	Value Added Tax
VMS	Voice Mail System
VoIP	Voice over IP
WGS	World Geodetic System
WLAN	Wireless Local Access Network
XML	eXtensible Markup Language
XPATH	XML PATH Language
XSD	eXtensible markup language Schema Definition 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

Edge Computing Service Provider (ECSP) and Application Service Provider (ASP) have to be considered as CSP in any of the sentences or diagrams of the present document where the term CSP is mentioned.

The end user is the consumer of the applications provided by the ASP and can have ASP service agreement with a single or multiple ASPs. The end user/UE has a subscription arrangement with a PLMN operator. The UE used by the end user is allowed to be registered on the PLMN operator network.

The ASP consumes the edge services (e.g. infrastructure, platform) provided by the ECSP and can have ECSP service agreement with a single or multiple ECSPs.

The ECSP can have PLMN operator service agreement with single or multiple PLMN operators which offer edge computing support.

The edge computing service provider and the PLMN operator can be part of the same organization, in which case the business relationship between the two is internal to a single organization.

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 should 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.

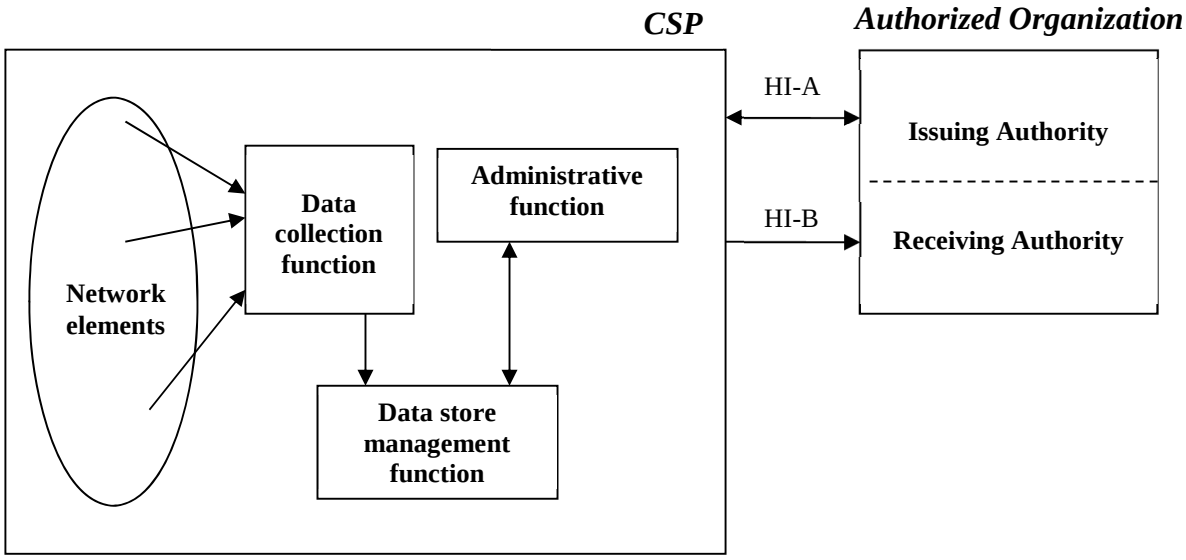


Figure 2: Functional model (informative)

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).

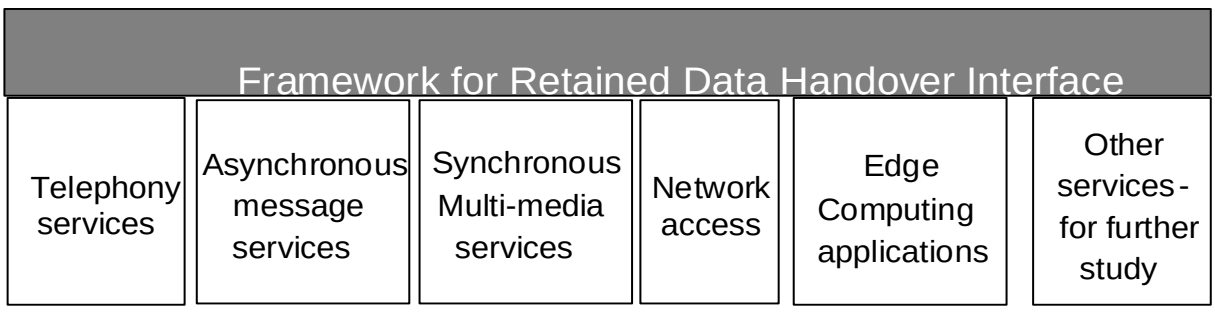


Figure 3: Framework structure

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.

The present document does not mandate or require CSPs to create data by inspecting or analysing communication content.

The scope of each service is as follows:

- Telephony services cover 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 ETSI ES 282 002 [22]) over IP) including GSM/UMTS-CS, SMS and MMS.

NOTE 1: EMS (3GPP TS 23.040 [16]) is handled as SMS.

- Asynchronous messaging services cover 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 and MMS.

- Synchronous multimedia services are covered by the present document. Specifically, the present document contains details for interactive or synchronous communication sessions beyond the telephony services.

- Edge Computing applications covers applications offered via edge computing capabilities (as defined in 3GPP TS 23.558 [56]).

- Network access services cover the services offering a capability to access public data networks (typically the internet), including GPRS/UMTS-PS, as defined in clause E.1.

NOTE 2: 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.

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).

- Billing data: information relating to a subscriber's billing details and history.

A more detailed breakdown for some 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 request, cancel and error information from/to the Authorized Organization and the organization at the CSP, which is responsible for Retained Data matters.

The Handover Interface port 2 (HI-B) shall be used for all communication (retained data information, response, status and error messages) between the CSP to the Authorized Organization.

For a complete assignment of communication types to the handover Interface ports see clause 5.4.

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

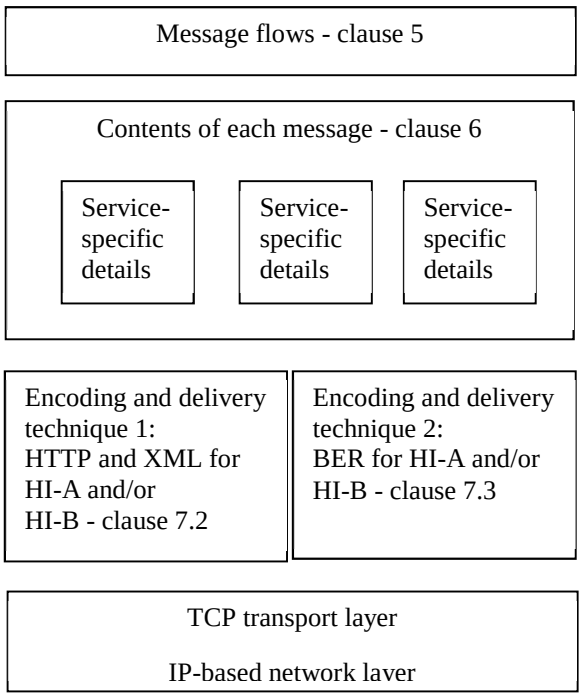


Figure 4: RDHI model

5 Handover interface message flows

5.1 Overview

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 defines the HI-A and HI-B message types.

Clause 5.5 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 5.1.5).
- The Authorized Organization cancels a request, signalling that no further results shall be delivered for that request (see clause 5.1.6).
- The delivery of some of the results before all results are ready (see clause 5.1.7).

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 or invalid authorization), 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" via the HI-B interface. 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.

Error messages shall always be sent via the interface where the original message causing the error initiated. So for example an error message responding to a broken request shall be sent via HI-A whereas an error message responding to a bad getResult message shall be sent via the HI-B interface.

5.1.5.4 Missing messages

Both the CSP and the Authorized Organization may at times be waiting for a message from the other party. It is an error for that message never to arrive, and the CSP and Authorized Organization shall take appropriate action to resolve the error situation.

This error differs from transmission errors at the transport level. Transport layer protocols (see clause 7) take care of transmission errors, and present a reliable end to end channel to their parties. However, even assuming a perfect transmission channel, messages may be lost due to issues in higher protocol levels. The CSP and Authorized Organization shall gracefully handle these situations.

There are two strategies that can be used to resolve missing messages: wait or raise a timeout indication to local operators. The timeout periods for waiting are a national issue. These periods may depend on the priority of the request (see clause 6.3.3.1) or the suggested completion time (see clause A.2.2.2).

The CSP could use the following strategies:

- Waiting for a Request message:
  - the CSP should wait indefinitely.
- Waiting for a GetResults message (Authorized-Organization-initiated scenario only):
  - the CSP should wait for at most *tpMedium* for a message to arrive, then raise a timeout indication.
- Waiting for a GetStatus or Cancel message (Authorized-Organization-initiated scenario only):
  - the CSP should wait for at most *tpLong* for either message to arrive, then raise a timeout indication.

- Waiting for a Response Acknowledgment message:
  - the CSP should wait for *tpMedium*, then raise a timeout indication.

The Authorized Organization could use the following strategies:

- Waiting for a Request Acknowledgement message:
  - the AO should wait for at most *tpMedium*, then raise a timeout indication.
- Waiting for a Response message (general scenario only):
  - the AO should wait for at most *tpLong*, then raise a timeout indication.
- Waiting for a Response message (Authorized-Organization-initiated scenario only):
  - the AO should wait for at most *tpMedium*, then raise a timeout indication.
- Waiting for Status or Cancel Acknowledgement message:
  - the AO should wait for at most *tpShort*, then raise a timeout indication.

NOTE 1: When no manual interventions are required after the initial request (when handling of DR requests is fully automated), the following approximate timeout periods are suggested. *tpShort*: a few minutes to an hour; *tpMedium*: tens of minutes to a few hours; *tpLong*: a few days.

NOTE 2: When manual interventions are necessary during the handling of a request, the timeout behaviour should be agreed upon by the Authorized Organization and the CSP on a national basis. One option may be to always wait indefinitely, and raise fatal timeout indications manually when necessary.

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.

Failure to comply with an otherwise syntactically correct cancellation (e.g. cancelling somebody else's request) shall also be indicated by an error message.

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

5.1.7 Delivery of results

Unless agreed in advance by the AO and CSP, 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 defines the criteria which cause a batch of records to be sent "once a certain number of records have been gathered" as indicated by the presence of the "maxRecordsPerBatch" parameter. The agreement outside of the message flows in the present document to allow use of that parameter does not preclude omitting it and using single shot delivery.

The present document does not define other criteria which cause a batch of records to be sent such as "after a certain time has elapsed", "once a certain volume of records have been gathered", or 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 in figure 5.

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

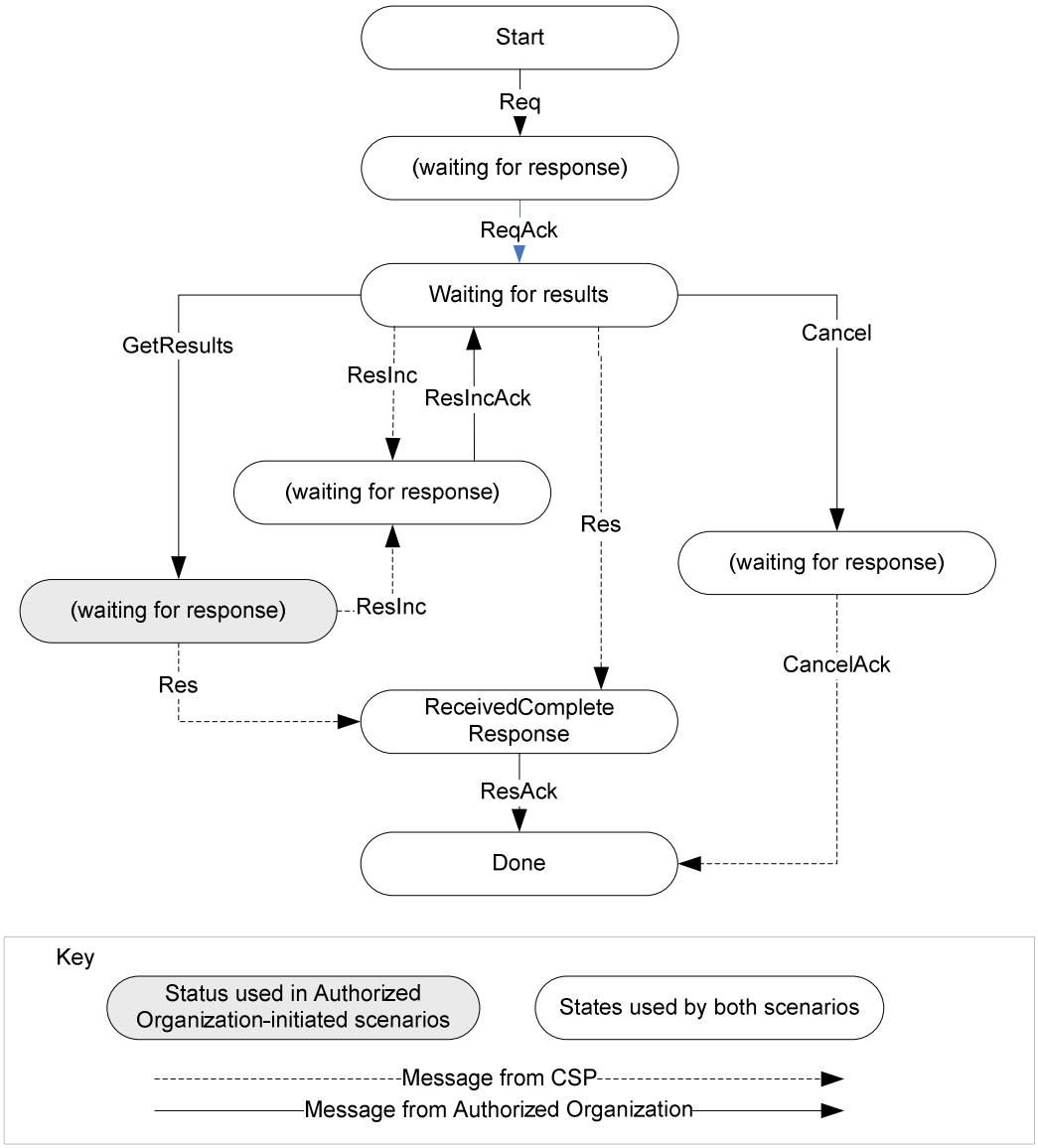


Figure 5: State diagram

The GetStatus message in clause 5.3 follows this state diagram in figure 6, independent of the state of each request.

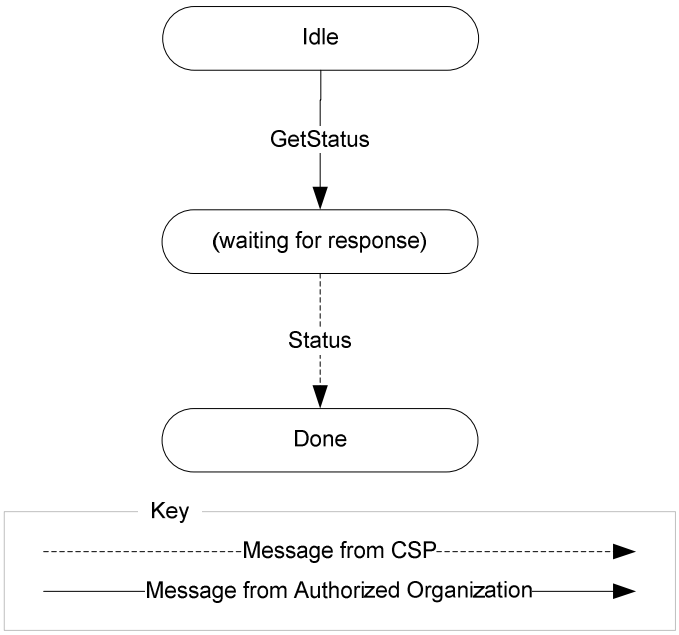


Figure 6: State diagram for GetStatus

5.1.9 Supplementary Messages

Two extra messages are provided to allow national jurisdictions to re-use the RDHI transport and session mechanisms for auxiliary RDHI-related functions. The two messages are:

- SupplementaryRequest.
- SupplementaryResponse.

These two messages define a simple request-response pair. The present document does not define any specific auxiliary functions or behaviours that may be mediated by these messages. Such definitions are left to national jurisdictions.

The SupplementaryRequest message is issued by an RDHI Client wishing to exercise a nationally defined auxiliary RDHI function.

If the RDHI Server receiving the SupplementaryRequest message can understand and accept the request, it responds with a SupplementaryResponse message. If the Server does not understand the message, it shall respond with an RDHI Error message.

The exchange of Supplementary Messages does not affect the existing RDHI state machine in any way. Existing RDHI behaviours and semantics are unaffected.

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).

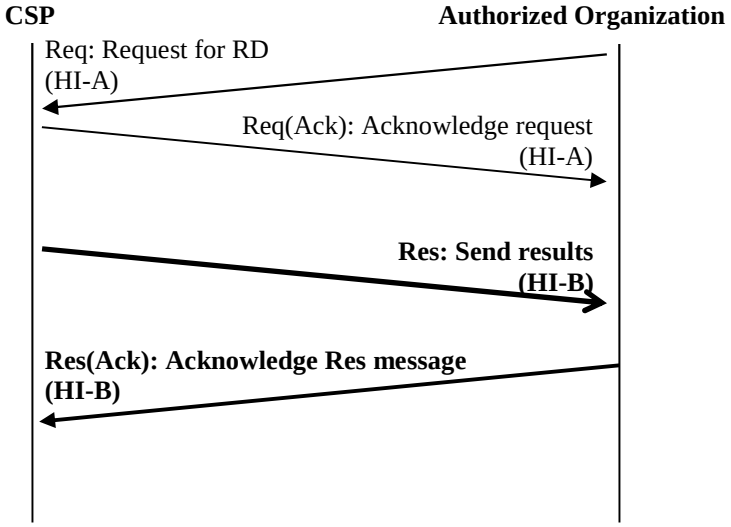


Figure 7: Message flow Successful delivery

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). Similarly, authorization failures (when one Authorized Organization attempts to cancel a request that was submitted by a different Authorized Organization) shall cause an error message. 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.

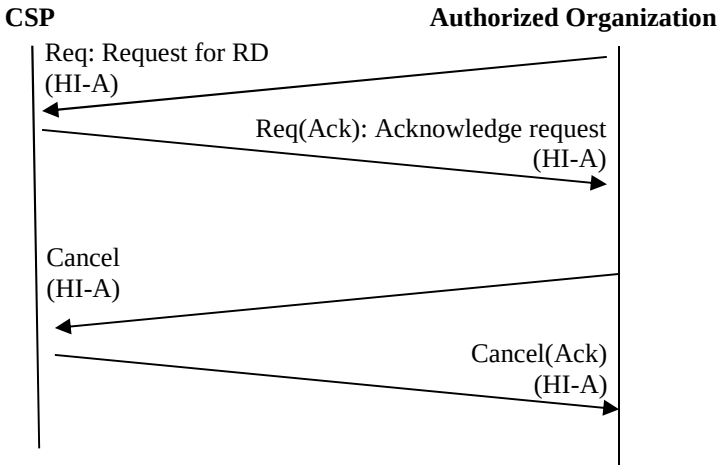


Figure 8: Message flow Cancellation by Authorized Organization

5.2.3 Multi-part delivery

As stated in clause 5.1.7, multi-part deliveries (including the sequential/parallel delivery option) 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 over HI-A.
- Incomplete sets of results are sent over HI-B according to agreed criteria (see clause 5.1.7). 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.

- The last set of results is flagged as "responseComplete" to indicate there will not be any further results to come. "Complete" means all data that was available for transmitting has been transmitted.

  For multi-part delivery of the result over HI-B there are two possible options:

  - Sequential delivery requires that there shall be no next partial delivery until the ACK has been received.
  - Parallel delivery allows the CSP to transmit multiple results messages where each results message is separately acknowledged without needing to wait for an ACK for other related results message(s). For parallel delivery, each results message shall have a response number starting at 1 and being incremented for each response message. The ACK message for a given results message has to include the response number of the message which it acknowledges.

- The Authorized Organization acknowledges the final results message with a Res(Ack) message.

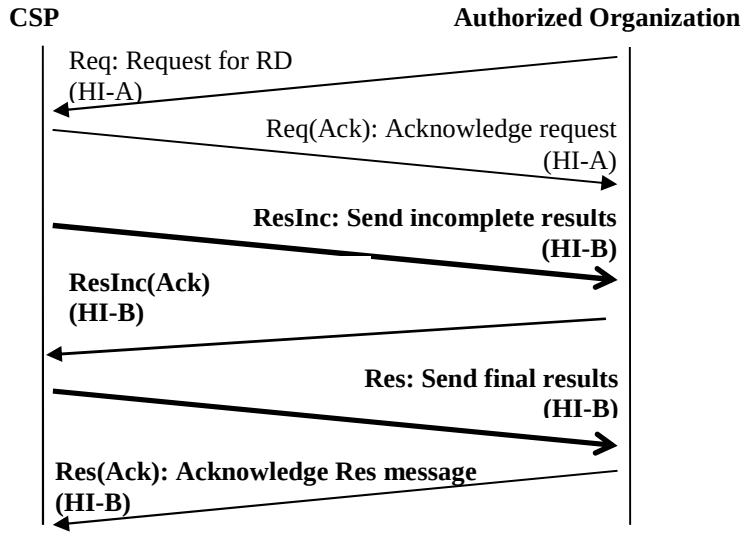


Figure 9: Message flow multi-part delivery

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 5.1.5.2) then the response will have the responseFailed flag set, and further details are included. If the results are not yet available, then the response will have the responseUnavailable flag 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 Res(Ack) without undue delay, and the request will no longer be active.

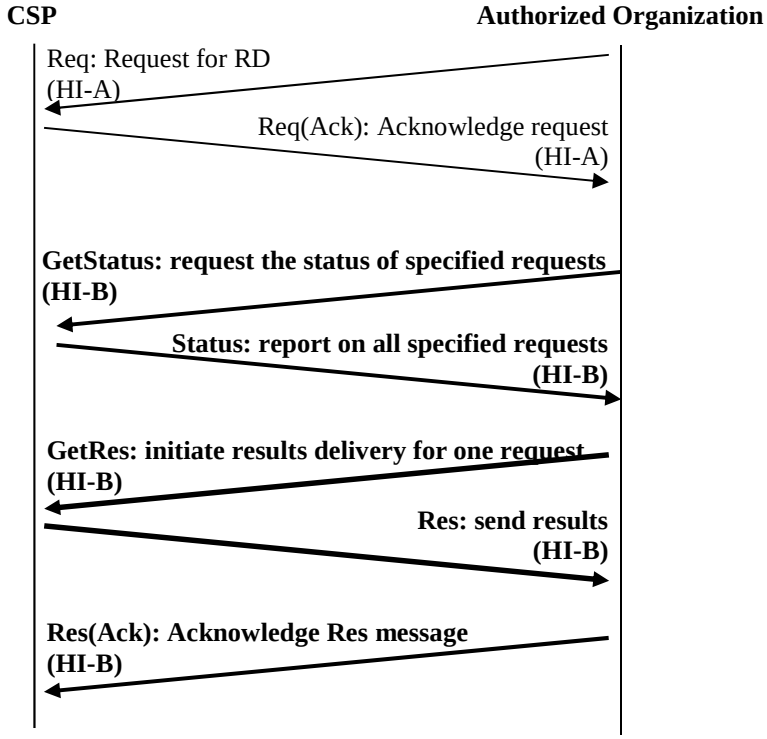


Figure 10: Delivery of results as initiated by the Authorized Organization

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 with a Res(Ack) message.

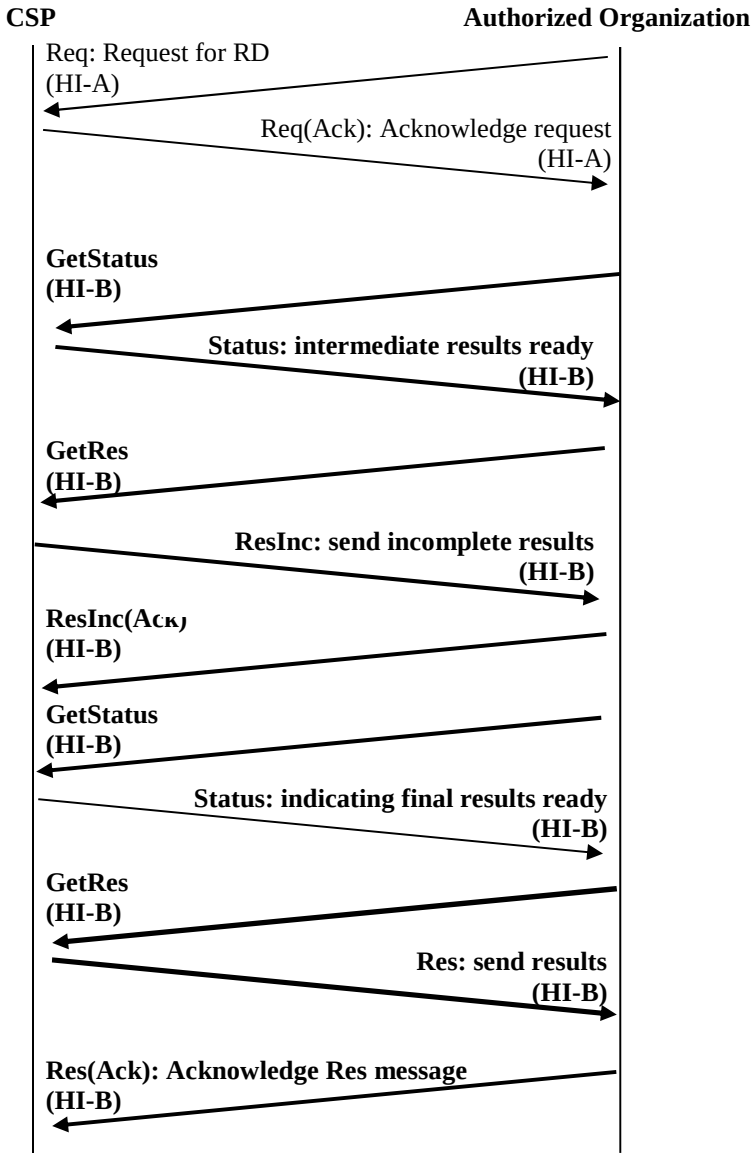


Figure 11: Delivery of results as initiated by the authorized organization in case of multi-part delivery

5.4 Message types for HI-A and HI-B

In the functional model (figure 2) the CSP communicates with the Issuing Authority using handover interface port A only, and the MF-B communicates with the Receiving Authority using handover interface port B only. The Issuing Authority and the Receiving Authority are functional entities. National regulations may choose to combine Issuing and Receiving Authorities.

Table 1 shows whether each message shall be sent as HI-A or HI-B.

Table 1: Message types that can be sent via HI-A and HI-B

Message	HI-A	HI-B	Remarks
requestMessage	x		
requestAcknowledgement	x		
getResultsMessage		x	
responseMessage (Complete)		x	
responseMessage (Incomplete)		x	
responseMessage (Unavailable)		x	
responseMessage (Failed)		x	
responseAcknowledgement		x	
cancelMessage	x		
cancelAcknowledgement	x		
getstatusMessage		x	
statusMessage		x	
errorMessage	x	x	Always sent via the same port as the request being responded to.

5.5 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 shall be prearranged between the Authorized Organization and the CSP. The messages in clause 6 can contain delivery points. These are used to avoid mentioning specific addresses.

When the Authorized Organization initiates any kind of request, the CSP shall 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 shall be sent. If no explicit delivery point is specified, the HI-B responses shall 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 RequestID distinguishes that request from any other on an international level. To do this, the RequestID 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).

Optionally, an external identifier (assignable by the Authorized Organization). The Authorized Organization may use this external identifier to correlate one or more requests.

6.1.3 CSP Identifiers

6.1.3.1 Use of CSP Identifiers (CSPID)

A CSP ID shall be agreed on a national basis. CSP IDs shall not be repeated within the same country (i.e. shall not be repeated within the same country code, as given in the request ID). The Authorized Organization and CSP shall agree a CSPID 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 CSPID, 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 (thirdPartyCSPID)

Where a CSP is holding data on behalf of another CSP, the thirdPartyCSPID shall be used to indicate that an Authorized Organization is making a Retained Data Request over the HI-A 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 thirdPartyCSPID field to indicate that the data being disclosed does not relate to a subscriber owned by the CSP specified in the CSPID field.

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

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

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

6.1.4 Timestamp (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.

6.1.5 RequestType (requestType)

An Authorized Organization may indicate a request type. The allowed types shall be defined by national agreement. It is by national agreement if the CSP should include the request type in the response.

6.1.6 RequestFlag (requestFlag)

An Authorized Organization may indicate a request flag. This request flag contains additional information associated with the request, e.g. the purpose of the request. The allowed values shall be defined by national agreement.

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 (recordNumber)

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 (ResponseStatus)

Every response shall have a ResponseStatus. The response status will define whether it is complete or incomplete (see clause 5.1.7). In addition, for Authorized-Organization-initiated situations, it is possible to indicate a status of Unavailable (see clause 5.3.1).

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. This is always indicated via the HI-B interface.

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, the parameter shall be left out.

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. Furthermore there is an option to request specific ASN.1 parameters or XML elements instead of requesting all available query data. For this an AO may use the parameter requestedData (see clause A.2.2.1) in order to transport the path of the selected parameter in XPATH notation [37]. In this case the CSP shall send a response message which includes only the selectively requested parameter. If the selected element has child nodes the whole subtree spanned from the selected element counts as selected. If this option is not used by the AO (requestedData is absent in the query) the CSP shall answer to the request in the usual way, i.e. response of all available data. The usage of the requestedData field shall be subject to national agreement.

NOTE 1: When discussing whether to use the requestedData field, implementers should be aware that using XPATH queries on ASN.1 may be difficult.

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

- EqualTo: A specified value for a given field.
- NotEqualTo: A specified value which for a given field shall not be equal to.

NOTE 2: The NotEqualTo criterion is likely to be used as an additional criterion.

- 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 to T2.

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.
- NotEqualTo: The value of the specified field of returned records shall not equal the value given.

NOTE 1: The NotEqualTo criterion is likely to be used as an additional criterion.

- 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.
- LessThanOrEqualTo: The value of the specified field of returned records shall be less than or equal to 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.

- GreaterThanOrEqualTo: The value of the specified field of returned records shall be greater than or equal to 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 shall 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 shall 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 2: 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.

The parameter MaxHits shall not be used simultaneously in a request with the numberOfRecordsLimit parameter specified in clause 6.3.3.4.

6.3.3.3 Maximum records per batch

A request may indicate that *multi-part* delivery is requested and specify an upper bound on the number of records to be returned in each batch of the result, by populating the MaxRecordsPerBatch parameter in the request.

It is a national issue to discuss whether MaxRecordsPerBatch is used and how it is used.

If the MaxRecordsPerBatch parameter is present, and if the CSP identifies more records meeting the request than the MaxRecordsPerBatch value, then *multi-part* delivery shall be used. When Status is requested, the CSP then shall provide a Status message with RequestStatus set to "incompleteResultsReady". When a Response is requested, the ResponseMessage then shall set ResponseStatus to "responseIncomplete" in each response until the final response, which shall then indicate "responseComplete".

6.3.3.4 Number of records limit

The parameter numberOfRecordsLimit shall not be used simultaneously in a request with the MaxHits parameter specified in clause 6.3.3.2. A request may specify an upper limit on the number of records to be provided by the CSP by populating the parameter numberOfRecordsLimit.

When the numberOfRecordsLimit value is reached, the CSP is required to continue searching for all matching records and indicate to the requestor the total number of records found in the database(s) with the parameter numberOfRecordsFound in the ResponseMessage. The responseStatus shall be set as responseComplete.

When the number of records found by the CSP is lower than the numberOfRecordsLimit value, the parameter numberOfRecordsFound may be omitted in the ResponseMessage.

The use of the numberOfRecordsLimit and numberOfRecordsFound feature is up to national agreement.

The parameters numberOfRecordsLimit and numberOfRecordsFound may typically be used in an automated request and response cycle. In automated cycles, the request has to be precisely formed in order to avoid multiple search passages, which could lead an overload of the queried database(s).

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).

Subject to mutual agreement at a national level, error details may also be categorized according to a list of common errors. Common error types are assigned an integer value or code and have a standard description (in the same manner as HTTP Status Codes such as "404 Not Found"). If this option is used, an error "value" and "description" shall be populated in the "CategorisedErrorDescription" structure. The values and descriptions shall be taken from a list which has been agreed nationally.

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 shall 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

7.3.0 General

The direct TCP mechanism uses XML, or 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 may be used for both the General message flows (clause 5.2) and the Authorized-Organization initiated message flows (clause 5.3).

7.3.1 Application layer

When using ASN.1 the messages are BER encoded.

When using XML over TCP the XML messages are transported in a simple packet format, defined as follows:

```
struct {
            unsigned int type;
            unsigned hyper length;
            opaque XML<>;
} XML_Message;
```

The definitions of the above mentioned fields are defined in table 1A.

Table 1A: Definition of fields in XML message

Field name	Field size (see IETF RFC 4506 [27])	Description
Type	32 bits	Type field as defined in table 2
Length	64 bits	Length of the XML data
XML	Variable	"Length" bytes of opaque XML data

Possible options for the "Type" field are defined in table 2.

Table 2: Definition of Type values

Type value	Meaning
0	Invalid / Empty Message
1	Plain XML; XML field contains uncompressed XML
2	Compressed XML; XML field contains ZLIB® compressed XML
3 - (2^32 - 1)	Reserved for future use

7.3.2 Transport layer

7.3.2.1 Introduction

Clause 6.4 of ETSI TS 102 232-1 [3] describes a transport layer that is based on the Transport Control Protocol. TCP is implemented according to IETF RFC 793 [17], IETF RFC 5681 [18], IETF RFC 6298 [19] and clause 4.2 of IETF RFC 1122 [20]. According to the interface described in clause 4.1 the CSP is the TCP sender and the Authorized Organization is the TCP receiver or contrariwise.

7.3.2.2 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" (IETF RFC 1122 [20]) should not be used.

7.3.3 Network layer

The Network layer implements the Internet Protocol according to IETF RFC 791 [21].

7.3.4 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 (IETF RFC 2818 [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 ETSI 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 messages 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 186-5 [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 shall be consistent, extensible and maintainable.

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

The present document does not supersede national legislation.

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

- Those elements that are required to meet technical delivery requirements are marked ***MANDATORY (M)***.
- 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.

Tables B.1 to B.15 and tables C.1 to C.6, assign each element M or O according to these definitions. Some of the lowest-level parameters are not listed in tables B.1 to B.15 and tables C.1 to C.6. They are defined only in the ASN.1 in clauses B.3, C.3, etc. Such elements have the same status (M 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.

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 and is attached to 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.1.4 Backwards Compatibility

From version V2.1.1 of the present document, extension markers have been added in the ASN.1 choice and sequence types that lacked extension markers. This is not backwards compatible to past versions for those modified types.

NOTE: Implementations decoding from version V2.1.1 of the specification can still decode messages encoded with older versions of the specification, but implementations older than V2.1.1 may not be able to decode messages encoded to V2.1.1 or newer.

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/O (see clause A.1.1)
requestID	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
requestType	See clause 6.1.5	O
requestFlag	See clause 6.1.6	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/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
externalIdentifier	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/O (see clause A.1.1)
requestPriority	See clause 6.3.3.1	O
requestParameters	See clause 6.3.2	O
deliveryPointHIB	See clause 5.5	O
maxHits	See clause 6.3.3.2	O
nationalRequestParameters	Defined on a national basis	O
maxRecordsPerBatch	See clause 6.3.3.3	O
requestedData	See clause 6.3.1	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/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/O (see clause A.1.1)
responseStatus	See clause 6.2.2.2.	M
responsePayload	Required if responseStatus is responseComplete or responseIncomplete (see table A.6).	O
nationalResponsePayload	Defined on a national basis.	O
responseNumber	Number to identify partial results within parallel multi-part delivery.	O

Table A.6: ResponseRecord parameters

Field name	Value	M/O (see clause A.1.1)
recordNumber	See clause 6.2.2.1	M
recordPayload	See clause 6.2	M
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/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/O (see clause A.1.1)
`statusResponse`	See clause 5.3.1	O

Table A.9: StatusResponse parameters

Field name	Value	M/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/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. Optionally generic contract information can be stored within this structure.

A.2.3.2 OrganizationInfo parameters

The OrganizationInfo field contains the following parameters.

Table A.11: OrganizationInfo parameters

Field name	Value	M/O (see clause A.1.1)
name	Name of the organization.	O
contactDetails	Address and contact details for point of contact.	O
nationalRegistrationID	Provides a unique reference for this organization (e.g. a tax registration number). The format of this field is for national agreement.	O
registeredAddress	The address to which the organization or business is registered, if known/applicable.	O
tradingAddress	The operating address of the organization or business, if known/applicable.	O
otherAddresses	Used if there are addresses for the organization which do not fit into the other categories.	O
groupID	Identity of group in organization for that generic subscriber.	O
groupAdministrator	Administrator of the group.	O
companyType	Type of company.	O
vatEnabled	Value Added Tax enabled.	O
vatNumber	VAT number of organization for that generic subscriber.	O
createIP	External IP/Port used to create account if available.	O
createTime	Creation time for the subscriber.	O
modifiedDate	Modification time for the subscriber.	O

A.2.3.3 IndividualInfo parameters

The IndividualInfo field contains the following parameters.

Table A.12: IndividualInfo parameters

Field name	Value	M/O (see clause A.1.1)
name	Name of the individual.	O
contactAddress	Address and contact details for individual.	O
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. See table A.12A.	O
profession	Profession of the individual.	O
otherAddresses	Used if there are addresses for the individual which do not fit into the other categories.	O
createTime	Creation time for the subscriber.	O

Table A.12A: AuthenticationInfo parameters

Field name	Value	M/O (see clause A.1.1)
authenticationType	The type of document used to authenticate, e.g. passport, driver's license.	O
authenticationNumber	The number of the document used to authenticate.	O
issuingCountry	The country that issued the document used to authenticate, as specified in ISO 3166-1 [4].	O
issuingOrganization	The organization that issued the document used to authenticate, e.g. United Nations.	O
nationality	The nationality of the subscriber, if indicated on the document used to authenticate.	O
authenticationDocument	The electronic copy of the document used to authenticate.	O

A.2.3.4 ContractInformation parameters

The ContractInformation structure may be used where the standardized parameters in the present document are insufficient to disclose the entire information due to a request for all available data belonging to subscription contract.

Table A.12B: ContractInformation parameters

Field name	Value	M/O (see clause A.1.1)
contractDesignation	The designation of the contract, e.g. "Mobil Flat 5000".	O
contractNumber	The number of the contract.	O
timeSpan	Time over which the contract was effective. If the contract is still effective, the endTime shall not be populated. The attribute "durationTime" shall not be used for this purpose.	O
otherInformation	For explanatory notes. The otherInformation field in this structure shall not be used for any information which is covered by standardized parameters.	O
contractDocuments	A full copy of applicable documents belonging to the contract.	O

A.2.4 PaymentDetails

The PaymentDetails structure encapsulates common payment information in multiple service-specific annexes for subscriber data. The parameters are as follows.

Table A.13: PaymentDetails parameters

Field name	Value	M/O (see clause A.1.1)
billingMethod	Method of billing (e.g. debit, transfer, prepaid, etc.).	O
bankAccount	Sequence of specific data identifying the subscriber account within his bank.	O
billingAddress	Contact details of the billing address.	O
billingIdentifier	An identifier for billing purposes. The format of this field is for CSPs to determine.	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.

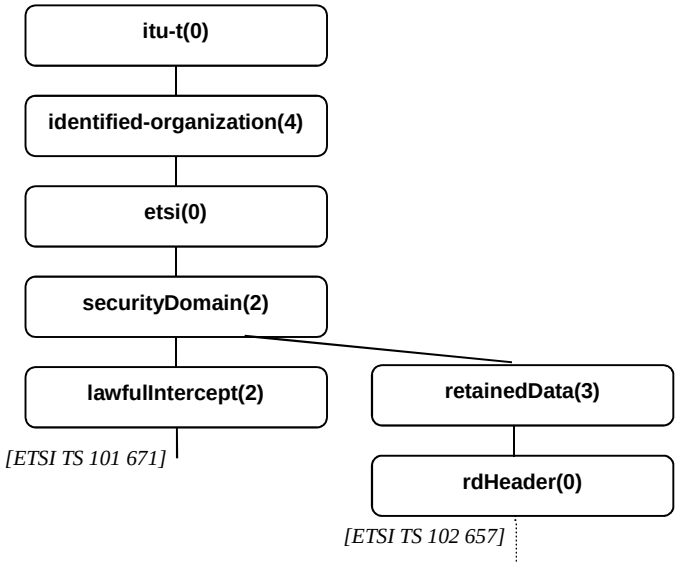


Figure A.1: Object identifier tree

A.3.1.2 General remarks on ASN.1

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 *RDMessagever32.asn* contained in archive ts_102657v020501p0.zip which accompanies the present document.

The XSD definitions are contained in *RDMessagever32.xsd* contained in archive ts_102657v020501p0.zip which accompanies the present document.

A.3.2 ASN.1 Definitions for message headers

A.3.2.1 Message wrappers

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

A.3.2.2 Message headers

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

A.3.3 ASN.1 definitions for common fields

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

A.3.4 Void

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

B.1 Scope

Telephony services cover 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, SMS and MMS.

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 is to be read in conjunction with the notes in the ASN.1 definitions given in the archive which accompanies the present document (see clause A.3.1.2).

B.2.2 Telephony Subscriber

B.2.2.0 General

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

Table B.1: TelephonySubscriber parameters

Field name	Value	M/O (see clause A.1.1)
`subscriberID`	A unique identifier for a particular subscriber within a CSP.	O
`genericSubscriberInfo`	A unique identifier for this particular subscriber within the CSP.	O
`telephonySubscriberInfo`	Service specific information about the subscriber.	O
`subscribedTelephonyServices`	List of services details that a subscriber (or account) may have.	O

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.

B.2.2.2 genericSubscriberInfo

Common information such as name and address is stored in the GenericSubscriberInfo structure. This is defined in 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/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
registeredICCID	Integrated Circuit Card ID in cases of single SIM card contracts.	O
serviceType	The type of service subscribed to.	O
installationAddress	The installation address for the subscriber's equipment, if applicable.	O
connectionDate	Date when the subscriber was actually connected that may differ from the start of subscription.	O
iMSI	IMSI of the subscriber.	O
carrierPreselect	Indication of the carrier preselection.	O
lineStatus	CSP specific description of the current line status.	O
allocatedDeviceIDs	List of all known devices allocated to this user for this subscription. The user may use other devices in addition (or instead of) these devices.	O
pUKCode	PUK code for the SIM card associated with this subscription, if applicable.	O
pUK2Code	PUK2 code for the SIM card associated with this subscription, if applicable.	O
iMEI	IMEI of the subscriber.	O
nationalTelephonySubscriptionInfo	Defined on a national basis.	O
paymentDetails	Details for payment (e.g. associated bank account, billing method or billing address).	O
deliveryAddress	The delivery address for equipment, if applicable.	O
resellerAddress	The address of the reseller or dealer, if applicable.	O
otherAddresses	Used if there are addresses for the subscription which do not fit into the other categories.	O
registeredNumbersInfo	Information about timespan of the active number and disable reasons.	O
registeredICCIDs	Integrated Circuit Card IDs in cases of MultiSIM card contracts.	O
loginInfos	Information on login details, e.g. in case of a VMS/UMS account.	O

Field name	Value	M/O (see clause A.1.1)
paymentTransactions	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause B.2.3.1.	O
iMEIs	IMEIs associated with the user's subscription (see note).	O
NOTE: There is a mismatch between the ASN.1 and XML Schema Definitions of iMEI. New implementations should use iMEIs instead.		

B.2.3 Telephony Billing Details

B.2.3.0 General

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

Table B.3: TelephonyBillingDetails parameters

Field name	Value	M/O (see clause A.1.1)
subscriberID	A unique identifier for a particular subscriber within a CSP.	O
serviceID	A unique identifier within the operator for the service or tariff subscribed to.	O
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.2.3.1.	O

B.2.3.1 BillingRecords

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

Table B.4: BillingRecords parameters

Field name	Value	M/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 or cryptocurrency specified.	O
currency	Currency of payment, in ISO 4217 [5] format.	O
cryptocurrency	Cryptocurrency of payment, defined in ISO 24165-2 [57], formatted as DigitalTokenIdentifier (see table K.4A).	O
method	Type of payment (e.g. credit card, top-up voucher). The format of this field is for agreement with the CSP.	O
nationalTelephonyBillingRecords	Defined on a national basis.	O
transactionID	Unique reference.	O
transactionStatus	Status of the transaction (i.e. "declined", "succeeded", etc.).	O
copyOfBill	The electronic copy of the bill.	O

B.2.4 TelephonyServiceUsage

B.2.4.1 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/O (see clause A.1.1)
partyInformation	A list of partyInformation structures (see clause B.2.4.2).	O
communicationTime	Total time for this service usage. Not that the time of involvement of individual parties may be shorter (see clause B.2.4.2).	O
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 [51] cause code for the termination of the call.	O
communicationType	The type of call.	O
bearerService	The bearer service for the call.	O
smsInformation	SMS information for the service usage, if applicable.	O
ringDuration	Ring duration, given in seconds.	O
mmsInformation	MMS information for service usage, if applicable.	O
nationalTelephonyServiceUsage	Defined on a national basis.	O
operatorSpecificCallDetails	Identifier or a combination of identifiers as used by the CSP to classify the call for billing procedures.	O
trunkGroupIDs	The incoming and outgoing trunk group IDs for the session/call. Format of values as defined by the CSP.	O
interOperatorIDs	The originating, terminating and transit interoperator identifiers (orig-ioi, term-ioi and transit-ioi-list) in IETF RFC 7315 [55] format, as recorded in the P-Charging-Vector.	O

B.2.4.2 PartyInformation

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

Table B.6: PartyInformation parameters

Field name	Value	M/O (see clause A.1.1)
partyRole	Role for this party (e.g. called, calling).	O
partyNumber	Number for this party in E.164 format.	O
subscriberID	Subscriber identifier, unique identifier for subscriber (see clause B.2.2.1).	O
deviceID	Device identifier.	O
locations	Location(s) encountered during a call.	O
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.2.4.1).	O
iMSI	IMSI of the party.	O
natureOfAddress	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
emailAddress	e mail address of the party for MMS.	O
iMEI	IMEI of the party.	O

Field name	Value	M/O (see clause A.1.1)
detailedLocation	Detailed location information per call and party, e.g. geoCoordinates for this partyNumber.	O
nationalTelephonyPartyInformation	Defined on a national basis.	O
partyType	Type of party (e.g. operator provided voicemail, etc.).	O
dialledDigits	Digits dialled by the party (e.g. subscriber controlled input).	O

B.2.4.3 SMSInformation

A SMsInformation structure if filled in when a SMS is involved in the communication. The parameters are as follows.

Table B.7: SmsInformation parameters

Field name	Value	M/O (see clause A.1.1)
smsEvent	Type of message event - may be single short message, a part of a composite message, a composite message, a notification message.	O
smsType	Type of sms transferred on SC - MS interface.	O
smsStatus	Status reached by the sms, i.e. submitted, delivered (listed in the ASN.1 in clause B.3).	O
smsCmRefNr	Concatenated short message reference number, in 3GPP TS 23.040 [16].	O
smsNumOfSM	Number of short messages transferred in case of composite messages.	O
smsNotifyInd	Delivery notification message generated by messaging centre.	O
smsProtocolId	Transfer Layer Protocol - Protocol Identifier (TP-PID), in 3GPP TS 23.040 [16].	O

B.2.4.4 MmsInformation

A MmsInformation structure is filled in when a MMS is involved in the communication. The parameters are as follows.

Table B.8: MmsInformation parameters

Field name	Value	M/O (see clause A.1.1)
mmsEvent	Type of message event - may be a multimedia message, a multimedia notification message, a multimedia delivery report message, a multimedia read reply message.	O
mmsStatus	Status reached by the mms, i.e. submitted, delivered (listed in the ASN.1 in clause B.3). The status "delivered-application" indicates that the MMS was retrieved by something other than a mobile handset; for example, a web browser.	O
mmsNotifInd	Delivery notification message generated.	O
mmsMsgMod	Modifications performed on the message - may be none, modified, stripped (if some parts of the message have been removed).	O

B.2.5 TelephonyDevice

B.2.5.1 General

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

Table B.9: TelephonyDevice parameters

Field name	Value	M/O (see clause A.1.1)
deviceIDType	Indicates the type of identifier used in TelephonyDeviceID, e.g. IMEI. (See ASN.1 for permissible types.)	O
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.	O
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.2.6 TelephonyNetworkElement

B.2.6.1 General

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

Table B.10: TelephonyNetworkElement parameters

Field name	Value	M/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.2.6.2).	O
validity	Time period during which the information given in this structure is or was valid.	O
nationalTelephonyNetwork Element	Defined on a national basis.	O
transmitterDetails	Characteristics of the transmitter, e.g. beam-width, radiated power, antenna height, frequency, technology.	O

B.2.6.2 Location parameters

B.2.6.2.1 General

The Location structure contains location information for the network element.

Table B.11: Location parameters

Field name	Value	M/O (see clause A.1.1)
e164-Number	E.164 number in ISUP format (see ETSI EN 300 356 [7]).	O
globalCellID	Global cell ID in 3GPP TS 09.02 [8] format.	O
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.	O
umtsLocation	UMTS location, details as defined in clause B.3.	O
sAI	Service Area Identifier, in 3GPP TS 25.413 [31] format.	O

Field name	Value	M/O (see clause A.1.1)
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
extendedLocation	Extended location information (see clause B.2.6.2.4).	O
userLocationInformation	This field contains the User Location Information of the MS as defined in 3GPP TS 29.274 [32] for EPC case, if available. (Non-EPC case user location information is covered by the above parameters in this table i.e. globalCellID, rAI, sAI).	O
tAI	The Tracking Area Identity (TAI) is coded in accordance with 3GPP TS 29.118 [34] without the TAI IEI. The tAI parameter is applicable only to the CS traffic cases (e.g. SMS over SGs) where the available location information is the one received from the Mobility Management Entity (MME) according to 3GPP TS 23.272 [35].	O
trackingAreaIdentifier	The Tracking Area Identity (TAI) is coded in accordance with 3GPP TS 29.274 [32], clause 8.21.4 without the TAI IEI and the 5G TAI see 3GPP TS 23.003 [41], clause 28.6.	O
eCGI	The E-UTRAN Cell Global Identity (eCGI) is coded in accordance with 3GPP TS 29.118 [34] without the eCGI IEI. The eCGI parameter is applicable only to the CS traffic cases (e.g. SMS over SGs) where the available location information is the one received from the Mobility Management Entity (MME) according to 3GPP TS 23.272 [35].	O
maritimeTransport	Provides information about the mobile cells embarked on ships using satellite transponder backhaul.	O
nCGI	The NR Cell Global Identity (NCGI), composed of the concatenation of the PLMN Identifier (PLMN-Id) and the NR Cell Identity (NCI) as shown in 3GPP TS 23.003 [41] given in ASN.1 BER encoding a 5 octet string with the 4 most significant bits set to zero as padding. (See note 2.)	O
n3gaLocation	The use of this parameter is not recommended, as its ASN.1 definition is not aligned with the format specified in 3GPP TS 29.571 [43]. The parameter n3gppaLocation should be used instead.	O
airTransport	Provides information about the mobile cells embarked on aircraft using satellite transponder backhaul.	O
bSSID	The Basic Service Set Identification of the WLAN Access Point. Equivalent to the MAC address of the Access Point.	O
locationInformationSource	Source of the location information. The format and content is to be determined on a national basis. The locationInformationSource will typically contain a network node name according to clause 4.1 of 3GPP TS 32.251 [49] or a NF service consumer name according to clause 4.1 of 3GPP TS 32.291 [46].	O
n3gppaLocation	Non-3GPP access user location, see 3GPP TS 29.571 [43], clause 5.4.4.10. (See note 2.) It is: 1. Unique non 3GPP TAI used in the PLMN. This IE shall contain the N3IWF identifier received over NGAP and shall be encoded as a string of hexadecimal characters. Pattern: '^[A-Fa-f0-9]+$'. 2. UE local IPv4 address (used to reach the N3IWF). 3. UE local IPv6 address (used to reach the N3IWF). UDP or TCP source port number. It shall be present if NAT is detected.	O
transmitterDetails	Characteristics of the transmitter, e.g. beam-width, radiated power, antenna height, frequency, technology.	O
NOTE 1: The population of the maritimeTransport and airTransport fields is a national issue and out of scope for the present document. NOTE 2: At least one of nCGI, and n3gppaLocation shall be present. Several of them may be present.		

B.2.6.2.2 GSM Location Information

Table B.12: GSMLocation parameters

Field name	Value	M/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
geoCoordinatesDec	Geographical decimal latitude-longitude location. Formats as described in ASN.1.	O

B.2.6.2.3 UMTS Location Information

Table B.13: UMTSLocation parameters

Field name	Value	M/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.2.6.2.4 Extended Location

Table B.14: Extended location parameters

Field name	Value	M/O (see clause A.1.1)
spot	Geographical coordinate or postal address of the location, details as defined in clause B.3.	O
circle	Geographical coordinate or postal address of the location, each with radius, details as defined in clause B.3.	O
region	Corner marks of an area, consisting of geographical coordinates or postal addresses of locations, details as defined in clause B.3.	O
route	Stretch of way, consisting of geographical coordinates or postal addresses of locations, details as defined in clause B.3.	O

B.2.6.3 TransmitterDetails parameters

B.2.6.3.1 General

The TransmitterDetails structure contains transmitter information for the network element.

Table B.15: TransmitterDetails parameters

Field name	Value	M/O (see clause A.1.1)
`alternativeID`	Alternative naming scheme for cells.	O
`beamWidth`	Beam width in degrees.	O
`radiatedPower`	Radiated power in watts.	O
`antennaHeight`	Height of antenna from ground in metres.	O
`range`	Indication of range or radius of cell or sector coverage in meters.	O
`frequency`	Transmitter frequency in kHz.	O
`technology`	Transmitter technology, e.g. gen2G, gen3G, eUTRAN, wLAN.	O
`nationalTransmitterDetails`	Defined on a national basis.	O

B.3 ASN.1 definitions for telephony

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

B.4 Void

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).

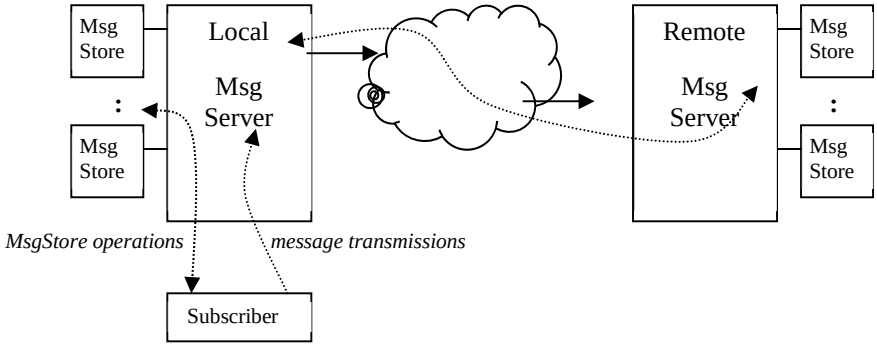


Figure C.1: Schematic overview of message handling

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 given in the archive which accompanies the present document (see clause A.3.1.2).

C.2.2 MsgSubscriber

C.2.2.0 General

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/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 in the service-independent annex A.	O
paymentDetails	Details for payment (e.g. associated bank account, billing method or billing address).	O

C.2.2.1 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.2.2.2 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/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.	O
providerID	A unique identifier of the provider hosting this message store.	O
msgForwardingAddresses	The list of all messaging addresses of the subscriber to which a message delivered to this message store is forwarded.	O
msgStoreSubscriberRelatedIDs	The list of service specific identifiers associated with the message store.	O

C.2.2.3 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.2.2.4 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 IETF RFC 5322 [24]-style address [24]. Other messaging systems (e.g. X.400 [i.1]) use their own messaging addresses.

C.2.2.5 MsgProviderID

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

C.2.2.6 MsgForwardingAddresses

The list of all messaging addresses of the subscriber to which a message delivered to this message store is forwarded.

C.2.2.7 MsgStoreSubscriberRelatedIDs

The list of all related identifiers of the subscriber associated with the message store, e.g. a secondary email account or a phone number. These identifiers are typically used to reset the password of the message store.

C.2.3 MsgServiceUsage

C.2.3.0 General

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.2.3.1 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/O (see clause A.1.1)
dateTime	Date and time when the subscriber submitted the message to the CSP's message server.	O
subscriberID	Unique identifier of the subscriber sending the message.	O
senderAddress	The available address of the sender (see note).	O
recipients	The list of all available recipients of the message (see note).	O
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.	O
serverID	IP address of the destination of the message transmission.	O
messageID	Unique identifier for the message - for example IETF RFC 5322 [24] 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
clientPort	Port number of the source of the message transmission.	O
serverPort	Port number of the destination of the message transmission.	O
NOTE: Depending on implementation and national discussion, some addresses may not be available, or may not be checked or reliable.		

C.2.3.2 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/O (see clause A.1.1)
dateTime	Date and time when the subscriber performed the indicated operation.	O
subscriberID	Unique identifier of the subscriber performing the operation.	O
msgStore	Unique identifier of the message store being manipulated.	O
operation	Type of manipulation performed by the subscriber.	O
senderAddress	The available address of the sender (see note).	O
recipients	List of all the available recipients of the message (see note).	O
protocol	Message store manipulation protocol.	O
clientID	IP address of the subscriber who performed the indicated operation.	O
serverID	IP address of the message server hosting the message store being manipulated.	O
messageID	Unique identifier for the message - for example IETF RFC 5322 [24] message-id header.	O
clientPort	Port number of the subscriber who performed the indicated operation.	O
serverPort	Port number of the message server hosting the message store being manipulated.	O
NOTE: Depending on implementation and national discussion, some addresses may not be available, or may not be checked or reliable.		

C.2.4 MsgBillingDetails parameters

C.2.4.0 General

The MsgBillingDetails structure contains billing information for the message service.

Table C.5: MsgBillingDetails parameters

Field name	Value	M/O (see clause A.1.1)
subscriberID	A unique identifier for a particular subscriber within a CSP.	O
serviceID	A unique identifier within the operator for the service or tariff subscribed to.	O
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 C.2.4.1.	O
nationalMsgBillingDetails	Defined on a national basis.	O

C.2.4.1 MsgBillingRecords

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

Table C.6: MsgBillingRecords parameters

Field name	Value	M/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 or cryptocurrency specified.	O
`currency`	Currency of payment, in ISO 4217 [5] format.	O
`cryptocurrency`	Cryptocurrency of payment, defined in ISO 24165-2 [57], formatted as DigitalTokenIdentifier (see table K.4A).	O
`method`	Type of payment (e.g. credit card, top-up voucher). The format of this field is for agreement with the CSP.	O
`nationalMsgBillingRecords`	Defined on a national basis.	O
`msgTransactionID`	Unique reference for this transaction/billing record.	O
`msgTransactionStatus`	Status of the transaction (i.e. "declined", "succeeded", etc.).	O
`copyOfBill`	The electronic copy of the bill.	O

C.3 ASN.1 definitions for asynchronous message services

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

C.4 Void

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

D.1 Scope

Synchronous multimedia services covers those services offering the facilities listed below. It covers services that provides VoIP and MoIP functionality. Carrier class VoIP could also be covered by annex B if no IP layer information is needed.

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

- Initiate communication set up.
- Accept communication set up.
- Conduct communication with one or more other parties.
- Cancel communication.
- Use a basic set of value-added services.

NOTE: Multimedia services cover services provided via IMS 3GPP TS 23.228 [25].

D.2 Multimedia fields

D.2.1 General

This clause describes the fields and parameters of the Multimedia ASN.1 definitions given in clause D.3. This clause should be read in conjunction with the notes in the ASN.1 definitions given in the archive which accompanies the present document (see clause A.3.1.2).

D.2.2 Multimedia Subscriber

D.2.2.0 General

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

Table D.1: MultimediaSubscriber parameters

Field name	Value	M/O (see clause A.1.1)
`subscriberID`	A unique identifier for this particular subscriber within the CSP.	O
`genericSubscriberInfo`	General personal information defined in annex A.	O
`multimediaSubscriberInfo`	Service specific information about the subscriber.	O
`subscribedMultimediaServices`	List of services details that a subscriber (or account) may have.	O
`multimediaServiceRegistrationInfo`	Information on registration activity.	O

D.2.2.1 subscriberID

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.

D.2.2.2 genericSubscriberInfo

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

D.2.2.3 multimediaSubscriberInfo

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

D.2.2.4 subscribedMultimediaServices

D.2.2.4.1 Description

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

Table D.2: SubscribedMultimediaServices parameters

Field name	Value	M/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
registeredIdentifiers	The multimedia identifiers(s) assigned to the subscriber as part of this subscription, if applicable.	O
registeredICCID	Integrated Circuit Card ID (ICCID) number of the subscriber, in ASCII format. When a subscription has several ICCID and IMSI the parameter registeredICCIDs shall be used.	O
serviceType	The type of service subscribed to.	O
installationAddress	The installation address for the subscriber's equipment, if applicable.	O
connectionDate	Date that the subscription was actually connected (may be different to the start of the subscription).	O
iMSI	IMSI associated with the subscriber.	O
sUPI	If the CSP assigns an SUPI to the subscriber, this may be populated here. When a subscription has several SUPIs, the parameter registeredICCIDs shall be used.	O
gPSI	If the CSP assigns a GPSI to the subscriber as specified in 3GPP TS 29.571 [43], table 5.3.2-1, this may be populated here. When a subscription has several GPSIs, the parameter registeredICCIDs shall be used.	O
carrierPreselect	Flag to indicate that the subscriber has carrier preselect active.	O
lineStatus	CSP-specific description of current line or subscription status e.g. "Active", "Suspended", etc.	O
nationalMultimediaServices	Defined on a national basis.	O
paymentDetails	Details for payment (e.g. associated bank account, billing method or billing address).	O
deliveryAddress	The delivery address for equipment, if applicable.	O
resellerAddress	The address of the reseller or dealer, if applicable.	O
otherAddresses	Used if there are addresses for the subscription which do not fit into the other categories.	O
orderTime	Time when the subscribed service was ordered by user.	O

Field name	Value	M/O (see clause A.1.1)
iMEIs	IMEIs associated with the user's subscription.	O
registeredICCIDs	Integrated Circuit Card IDs numbers in case of Multi-SIM subscription.	O
privateUserIdentities	One or several Private User Identities (IMPI) of the IP Multimedia Subsystem subscription.	O
allocatedDeviceIDs	List of all known devices allocated to this user for this subscription. The user may use other devices in addition (or instead of) these devices.	O
paymentTransactions	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause D.2.3.3.	O

D.2.2.5 multimediaServiceRegistrationInfo

multimediaServiceRegistrationInfo contains data concerning context of the registration. The format and content of the subordinate fields is for CSPs to determine. This structure contains the registration information.

Table D.2A: MultimediaServiceRegistrationInfo parameters

Field name	Value	M/O (see clause A.1.1)
emailAddress	Email address associated with account.	O
languageAtRegistration	Language selected for account.	O
accountCreationTime	Time of creation.	O
accountCreationIP	IP associated with account.	O
accountCreationCountry	Country associated with account.	O
clientPlatformType	Platform associated with account.	O
clientVersion	Version of platform.	O

D.2.3 MultimediaBillingDetails

D.2.3.1 MultimediaBillingDetails

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

Table D.3: MultimediaBillingDetails parameters

Field name	Value	M/O (see clause A.1.1)
subscriberID	A unique identifier for a particular subscriber within a CSP.	O
serviceID	A unique identifier within the operator for the service or tariff subscribed to.	O
billingAddress	The billing address for this subscription.	O
multimediaBillingAddress	The billing address for a multimedia subscription. See clause D.2.3.2.	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 D.2.3.3.	O
nationalMultimediaBillingDetails	Defined on a national basis.	O

D.2.3.2 MultimediaBillingAddress

The billing address contains postal information for a particular payment. The parameters are as follows.

Table D.3A: MultimediaBillingAddress parameters

Field name	Value	M/O (see clause A.1.1)
addressSuppliedTime	Address submission time.	O
name	Name of account holder.	O
address	Address of account holder.	O

D.2.3.3 MultimediaBillingRecords

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

Table D.4: MultimediaBillingRecords parameters

Field name	Value	M/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 or cryptocurrency specified.	O
currency	Currency of payment, in ISO 4217 [5] format.	O
cryptocurrency	Cryptocurrency of payment, defined in ISO 24165-2 [57], formatted as DigitalTokenIdentifier (see table K.4A).	O
method	Type of payment (e.g. credit card, top-up voucher). The format of this field is for agreement with the CSP.	O
nationalMultimediaBillingRecords	Defined on a national basis.	O
multimediaTransactionID	Unique identifier for the billing transaction.	O
multimediaTransactionStatus	Status of the billing transaction.	O
copyOfBill	The electronic copy of the bill.	O

D.2.4 Multimedia ServiceUsage

D.2.4.1 Parameters

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

Table D.5: MultimediaServiceUsage parameters

Field name	Value	M/O (see clause A.1.1)
partyInformation	A list of partyInformation structures (see clause D.2.4.2).	O
communicationTime	Total time for this service usage. Not that the time of involvement of individual parties may be shorter (see clause D.2.4.2).	O
reasonCause	Cause code for end of call, e.g. encoded SIP Reason Cause codes.	O
communicationType	Type of bearer service used in the session.	O
bearerService	The bearer service for the communication.	O
qualityOfService	The quality of service parameter for the communication.	O
ringDuration	Ring duration, given in seconds for VoIP.	O
callID	Identifier of the retained call data, e.g. SIP callID, for correlating data from different DR sources in CSP.	O

Field name	Value	M/O (see clause A.1.1)
originalCallID	Identifier of the retained call data before any modification made by the node and usable to correlate data by different DR sources in CSP.	O
callState	State reached by the session with reference to the called subscriber connection, e.g. b not reached, b alerted, b answered.	O
answerTime	Date and time when the communication has been answered by the called party in case of sessions.	O
contentType	List of the media type of the message body, e.g. application/sdp, text/html.	O
mediaComponents	List of media component changes during the session.	O
imsInformation	IMS-specific information.	O
nationalMultimediaServiceUsage	Defined on a national basis.	O
serviceID	A unique identifier within the operator for the service or tariff.	O
providerID	A unique identifier for the service provider. The format of this field is to be determined by national agreement.	O
cdrNumber	Identifier for record - Format of value defined by CSP.	O
clientIP	IP of client at time of service usage.	O
relayIP	IP of relay - Multimedia service provider infrastructure seen as originating or terminating the call.	O
vmLength	Voice mail length given as an integer in seconds.	O
reason	Reason description: text description to explain reasonCause (see above).	O
smsInformation	SMS information for the service usage, if applicable.	O
mmsInformation	MMS information for service usage, if applicable.	O
trunkGroupIDs	The incoming and outgoing trunk group IDs for the session/call. Format of values as defined by the CSP.	O
interOperatorIDs	The originating, terminating and transit interoperator identifiers (orig-ioi, term-ioi and transit-ioi-list) in IETF RFC 7315 [55] format, as recorded in the P-Charging-Vector.	O

D.2.4.2 PartyInformation

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

Table D.6: PartyInformation parameters

Field name	Value	M/O (see clause A.1.1)
partyRole	Role for this party (e.g. called, calling).	O
partyIdentity	Identifier for this party. URI is used in case of IMS service.	O
subscriberID	Subscriber identifier, unique identifier for subscriber (see clause D.2.2.1).	O
communicationTime	Time that this party was involved in the communication, if this was a multiparty communication. Shall be omitted if it is the same as the time of the whole service usage (see clause D.2.4.1).	O
iMSI	IMSI associated with the party, if available.	O
natureOfAddress	Nature of the address - may be "international number", "national number" or "subscriber number".	O
uRI	URI of the party.	O
partyNumber	E.164 number associated to party.	O
naAssignedAddress	Address used by the subscriber's client for the connection.	O
forwardedTransferredIdentifier	Forwarded Identifier if communication was transferred.	O
terminatingTransferredIdentifier	Terminating identifier if communication was transferred.	O
nationalMultimediaPartyInformation	Defined on a national basis.	O
userAgent	User agent field, e.g. SIP user agent, see IETF RFC 3261 [26].	O

Field name	Value	M/O (see clause A.1.1)
octetsUploaded	Number of uploaded octets.	O
octetsDownloaded	Number of downloaded octets.	O
accessNetworkInformation	The network-provided and User Equipment (UE) provided access-type, access-class and cell information of the party from the content of the P-Access-Network-Info field as specified in 3GPP TS 24.229 [39], these fields shall only be populated when they can be extracted. In addition the location and time of the access may also be provided. In any case the complete content of the P-Access-Network-Info header field shall be provided in the paniHeaderContent parameter.	O
cellularNetworkInfo	This field contains the content of one SIP "Cellular-Network-Info" header, when the UE supporting one or more cellular radio access technologies but using a non-cellular IP-CAN, such as untrusted WLAN access, provides this header field to relay information to its service provider about the radio cell identity of the cellular radio access network on which the UE most recently camped.	O
privateUserIdentity	Private User Identity (IMPI) associated with the party, if available.	O
iMEI	IMEI associated with the party, if available.	O

D.2.4.3 IMSInformation

This ImsInformation structure is used for service usage information in case of IMS service; the parameters are as follows.

Table D.7: IMSInformation parameters

Field name	Value	M/O (see clause A.1.1)
service	Type of IMS service used by subscriber, e.g. session, message, refer.	O
roleOfNode	Specification on the role of the Data Retention Source in the reported communication, e.g. originating, terminating, proxy, b2bus.	O
serviceInfo	List of service-specific data.	O

D.2.4.4 MediaComponents

This structure contains the information on media components.

Table D.8: MediaComponent parameters

Field name	Value	M/O (see clause A.1.1)
time	Time when this media component has been processed.	O
mediaName	Media component name (from "m=" line in SDP data).	O
mediaDescription	Media component description (from "attribute-line" content in SDP data).	O
mediaInitiator	Media component initiator, i.e. called Party, calling Party.	O
accessCorrelationID	Correlation identifier for the access used for SIP usage.	O
nationalMultimediaMediaComponent	Defined on a national basis.	O

D.2.5 MultimediaDevice

D.2.5.1 General

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

Table D.9: MultimediaDevice parameters

Field name	Value	M/O (see clause A.1.1)
`deviceIDType`	Indicates the type of identifier used in MultimediaDeviceID, e.g. IMEI. (See ASN.1 for permissible types).	O
`multimediaDeviceID`	Unique identifier for the multimedia device. If this identifier happens to have a particular format (e.g. IMEI), then this may be indicated using deviceIDType.	O
`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

D.3 ASN.1 definitions for Multimedia

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

D.4 Void

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

E.1 Scope

Network access services cover the services offering a capability to access public data networks (typically the internet), including GPRS/UMTS-PS/EPS/5GS.

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 given in the archive which accompanies the present document (see clause A.3.1.2).

E.2.2 NASubscriber

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

Table E.1: NASubscriber parameters

Field name	Value	M/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
`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 in the service-independent annex A.	O

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/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.	O
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
sUPI	If the CSP assigns an SUPI to the subscriber, this may be populated here.	O
gPSI	If the CSP assigns a GPSI to the subscriber as specified in 3GPP TS 29.571 [43], table 5.3.2-1, this may be populated here.	O
allocatedDeviceIDs	List of all known devices allocated to this user for this subscription. The user may use other devices in addition (or instead of) these devices.	O
naServiceStatus	CSP-specific description of current service status, e.g. "Active", "Ceased", etc.	O
registeredICCID	Integrated Circuit Card ID of subscriber. When a subscription has several ICCID and IMSI the parameter registeredICCIDs shall be used.	O
nationalNASubscription	Description of the subscription to a Network Access service.	O
paymentDetails	Details for payment (e.g. associated bank account, billing method or billing address).	O
additionalIPAddresses	Additional IP addresses when CSP provides several IP addresses to one subscriber.	O
timedIPAddresses	IP addresses with validity period when CSP provides several IP addresses for different time periods.	O
deliveryAddress	The delivery address for equipment, if applicable.	O
resellerAddress	The address of the reseller or dealer, if applicable.	O
otherAddresses	Used if there are addresses for the subscription which do not fit into the other categories.	O
mSISDNs	Mobile Station International ISDN Numbers (MSISDNs) allocated to this subscription. In case the multinumbering option is used, there may be several MSISDNs provided as permanent subscriber data for the PS Network Access Mode GPRS (see 3GPP TS 23.008 [38]).	O
registeredICCIDs	Several Integrated Circuit Card IDs numbers in case of Multi-SIM subscription.	O
paymentTransactions	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause B.2.3.1.	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/O (see clause A.1.1)
naAccessTime	Date and time of the (attempted) network access.	O
naAuthID	Logon name (username) used to obtain network access.	O
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.	O
naDeviceId	Information on the device used to access the service.	O
naNwElementID	Network element (NAS) onto which the subscriber's device is connected to the service.	O
sNSSAI	Single Network Slice Selection Assistance Information (S-SNSSAI), specific to 5G System (see 3GPP TS 29.571 [43], 3GPP TS 29.520 [48], 3GPP TS 32.255 [47] and 3GPP TS 23.003 [41]).	O
notifyUri	Identifies the recipient of Notifications sent by the Charging Function (CHF). See 3GPP TS 32.291 [46], clause 6.1.5.2.2.	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.	O (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
octetsDownloaded	Number of octets downloaded by the subscriber during the network access session.	O
octetsUploaded	Number of octets uploaded by the subscriber during the network access session.	O
endReason	Indication of why the network access session ended.	O
subscriberID	Identifier for a known user of this network access.	O
ePSInformation	Information specific to Evolved Packet System (see table E.5A).	O
fiveGSInformation	Information specific to 5G System (see table E.5C).	O
wiFiInformation	Information specific to Wi-Fi® (see table E.5B).	O
addressTranslationInformation	Details of the NAT and PAT operations carried out on the connection by the provider, if applicable.	O
additionalLocations	List of additional locations during the network access service usage, if applicable.	O
NOTE: This is required if the naStatus indicates a successful network access attempt.		

Table E.4: DialUpInformation parameters

Field name	Value	M/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.	O
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/O (see clause A.1.1)
iMSI	IMSI associated with the network access.	O
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 ETSI TS 101 671 [6].	O
gPRSEvent	GPRS event, as per 3GPP TS 33.108 [11].	O

Table E.5A: EPSInformation parameters

Field name	Value	M/O (see clause A.1.1)
iMSI	IMSI associated with the network access.	C
iMSIUnauthenticatedFlag	This field indicates the provided served IMSI is not authenticated (emergency bearer service situation).	O
mSISDN	Primary MSISDN associated with the network access.	O
iMEISV	IMEISV of the ME, if available. It is used for identifying the user in case Served IMSI is not present during emergency bearer service.	O
s-GWAddress	The control plane IP address of the S-GW used.	O
p-GWAddress	The control plane IP address of the P-GW used.	O
p-GWPLMN-ID	PLMN identifier (MCC and MNC) of the P-GW.	O
aPNNetworkID	The logical name of the connected access point to the external packet data network (network identifier part of APN).	O
pDP-PDNType	PDP/PDN type, i.e. IPv4, IPv6, IPv4v6, coded as in 3GPP TS 29.274 [32], clause 8.34 (octet 5).	O
pDP-PDNAddress	IP address allocated for the PDP context/PDN connection, i.e. IPv4 address when PDP/PDN Type is IPv4 or IPv6 prefix when PDP/PDN Type is IPv6 or IPv4v6. This parameter shall be present except when both the PDP type is PPP and dynamic IP CAN bearer address assignment is used.	O
pDP-PDNAddressExtension	This field holds IPv4 address of the served IMSI, if available, when PDP/PDN type is IPv4v6.	O
dynamicAddressFlag	Indicates whether served PDP/PDN address is dynamic, which is allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity. This field is missing if IPv4 address is static when PDN Type is IPv4, or if IPv6 address is static when PDN Type is IPv6 or IPv4v6.	O
dynamicAddressFlagExt	Indicates whether served IPv4 PDP/PDN address is dynamic, which is allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity with PDP/PDN type IPv4v6. This field is missing if IPv4 address is static.	O
rATType	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in 3GPP TS 29.061 [33], when available.	O
ePSEvent	EPS event, as per 3GPP TS 33.108 [11].	O
uERadioCapID	The UE radio capability ID is an identifier used to represent a set of UE radio capabilities, defined in 3GPP TS 23.003 [41]. It is encoded as a string of hexadecimal digits from most significant (Type Field) to least significant (RCI).	O
NOTE: In case of 3GPP E-UTRAN New Radio - Dual Connectivity (EN-DC of 3GPP TS 37.340 [50]) to allow dual connectivity to combine LTE and 5G NR radio access, clause 5.2.1.11 of 3GPP TS 32.251 [49] recommend to have an data volumes for the Secondary RAT (5G NR), reported on a per EPS bearer basis. The value of field rATType will indicate such secondary access based for release 15 and above on 3GPP TS 29.061 [33].		

Table E.5B: WiFiInformation parameters

Field name	Value	M/O (see clause A.1.1)
bSSID	The Basic Service Set Identification for the connection. This is also the MAC address of the access point (the present document assumes that records are for infrastructure mode, not ad-hoc mode). The MAC address of the user is given in the naDeviceID in the structure.	O
sSID	The human-readable Service Set Identifier.	O
username	Username as seen by the CSP. For Wi-Fi® it is not necessarily the case that this will have been verified in any way.	O
locationOfAccessPoint	Location of the Access Point. It should be populated as lat/long, grid reference or postal address.	O
authenticationType	How the user authenticated themselves.	O
additionalAuthenticationInformation	Additional information known about the user on the basis of the authentication process.	O
accessPointIPAddress	IP address of the Access Point.	O
accessPointAdditionalDescriptions	Informal description of location, category or type of access point, or a name of the network to which the access point belongs.	O
accessPointAdditionalProviders	For Wi-Fi®, there may be other parties involved in hosting or owning the Access Points, e.g. access point provider or partner providers.	O
cSPDefinedName	CSP-defined label or name assigned to the access point, see note. The access points of a CSP within a venue or geographical location typically share this name.	O
NOTE: The format of cSPDefinedName is outside of the scope of the present document.		

Table E.5C: FIVEGSInformation parameters

Field name	Value	M/O (see clause A.1.1)
sUPI	Served SUPI associated with the network access, based on IMSI or NAI as defined in 3GPP TS 23.003 [41]. When the GCI and GLI are reported (as defined in 3GPP TS 23.003 [41], clauses 28.15.2 and 28.16.2 respectively), they are included in the NAI parameter.	O
dNN	String representing a Data Network Name as defined in clause 9A of 3GPP TS 23.003 [41] and 3GPP TS 32.255 [47], table 6.2.1.2.1.	O
pEI	Permanent Equipment Identifier of the ME that may contain: • an IMEI or IMEISV, as specified in clause 6.2 of 3GPP TS 23.003 [41]; • a MAC address for a 5G-RG or FN-RG via wireline access, as specified in clause 4.7.7 of 3GPP TS 23.316 [59]. Written as six groups of two hexadecimal digits separated by a colon; • an IEEE Extended Unique Identifier (EUI-64) for UEs as defined in [60] not supporting any 3GPP access technologies. Written as eight groups of two hexadecimal digits separated by a colon.	O
gPSI	Generic Public Subscription Identifier (GPSI) associated with the session.	O
pDUSessionID	See 3GPP TS 29.571 [43].	O

Field name	Value	M/O (see clause A.1.1)
sNSSAI	Single Network Slice Selection Assistance Information (S-SNSSAI), specific to 5G System onto which the subscriber's device is connected to the service. It is made of the Slice/Service Type (SST) and of the Slice Differentiator (SD). This last parameter is optional (see 3GPP TS 32.291 [46], 3GPP TS 29.571 [43] and 3GPP TS 23.003 [41]).	O
pDUIPv4Address	The IPv4 address of the served SUPI allocated for the PDP context / PDN connection. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.11.	O
pDUIPv6Address	The IPv6 address of the served SUPI allocated for the PDP context / PDN connection. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.11.	O
pDUAddressPrefixLength	PDU Address prefix length of an IPv6 typed Served PDP Address. Not required for prefix length of 64 bits. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.11.	O
rFSPIndex	Unsigned integer represents the "Subscriber Profile ID for RAT/Frequency Priority" as specified in 3GPP TS 36.413 [44]. Minimum = 1. Maximum = 256.	O
applicationId	String providing an application identifier and formatted For Further Study. (See 3GPP TS 29.571 [43]).	O
applicationServiceProviderIdentity	String providing an identifier of the application service provider. See 3GPP TS 32.291 [46], table 6.1.6.2.2.9-1.	O
serviceId	Identity of the used service. See 3GPP TS 32.291 [46], table 6.1.6.3.2-1.	O
chargingId	Correlates different records of a single PDU session. See 3GPP TS 32.291 [46], table 6.1.6.3.2-1.	O
pDUType	PDU type is defined in 3GPP TS 29.571 [43], it may be dual IPv4V6, IPv4, IPv6, Unstructured; Ethernet. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.8.	O
sSCMode	SscMode (enumeration) 3GPP TS 32.291 [46] indicates the different mode: 1. SSC_MODE_1 2. SSC_MODE_2 3. SSC_MODE_3_MULTIPDUSESSION 4. SSC_MODE_3_MULTIHOME See 3GPP TS 32.291 [46], clause 6.1.6.2.2.8.	O
vPLMNId	PLMN identifier of the visited network, based on SMF PLMN ID. Refer 3GPP TS 29.571 [43]. See 3GPP TS 32.291 [46].	O
hPLMNId	PLMN identifier of the home network, based on SUPI PLMN ID. Refer 3GPP TS 29.571 [43]. See 3GPP TS 32.291 [46].	O
chargingCharacteristics	Charging Characteristics. See 3GPP TS 32.291 [46].	O
chargingCharacteristicsSelectionMode	Charging Characteristics Selection Mode. See 3GPP TS 32.291 [46].	O
pDUSessionStartTime	The time in UTC format which represents the start of a PDU session at the SMF. dateTime, see 3GPP TS 32.255 [47], clause 6.2.1.2.	O
pDUSessionStopTime	The time in UTC format which represents the stop of a PDU session at the SMF. dateTime, see 3GPP TS 32.255 [47], clause 6.2.1.2.	O

Field name	Value	M/O (see clause A.1.1)
lowPriorityIndicator	Boolean, indicates if the PDU session has a low priority. See 3GPP TS 32.291 [46].	O
dataOffStatus	Boolean, indicated the change in 3GPP PS Data off status of UE. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.8.	O
diagnostics	It provides a more detailed cause value from SMF. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.8.	O
uETimeZone	The UE Time Zone the UE is currently located. Refer 3GPP TS 29.571 [43].	O
uPFAddress	The user plane IP address of the UPF used (mentioned in 3GPP TS 32.255 [47]).	O
aMFAddress	The control plane IP address of the aMF used (mentioned in 3GPP TS 32.255 [47]).	O
uDMAddress	The IP address of the UDM used, mentioned in 3GPP TS 32.255 [47].	O
sMFAddress	The IP address of the SMF and in 3GPP TS 32.255 [47]. IPv4Address. Refer 3GPP TS 29.571 [43].	O
uPFId	The UPF identifier, function defined in 3GPP TS 23.501 [45], mentioned in 3GPP TS 32.255 [47], and associated to some 5GS events. See 3GPP TS 32.291 [46]. Given as an NFInstanceID (UUID).	O
aMFIdentifier	The AMF identifier, function defined in 3GPP TS 23.501 [45], mentioned in 3GPP TS 32.255 [47] and associated to some 5GS events.	O
uDMIdentifier	The UDM identifier, function defined in 3GPP TS 23.501 [45], mentioned in 3GPP TS 32.255 [47], and associated to some 5GS events. As it is not defined in 3GPP TS 23.003 [41], CSPs have to defined them and transmit their choice to AOs.	O
sMFIdentifier	The SMF identifier, function defined in 3GPP TS 23.501 [45] and in 3GPP TS 32.255 [47] associated to some 5GS events. Given as an NFInstanceID (UUID).	O
uPFPDNAddress	IP address allocated for the UPF context/UPF connection, i.e. IPv4 address when PDN Type is IPv4 or IPv6 prefix when PDN Type is IPv6 or IPv4v6. This parameter shall be present. (mentioned in 3GPP TS 32.255 [47]).	O
uPFPDNAddressExtension	This field holds IPv4 address of the served SUPI, if available, when PDN type is IPv4v6. (mentioned in 3GPP TS 32.255 [47]).	O
dynamicAddressFlag	Indicates whether served PDN address is dynamic, which is allocated during slice/bearer activation, initial attach (mentioned in 3GPP TS 32.255 [47]).	O
dynamicAddressFlagExt	Indicates whether served IP/PDN address is dynamic, which is allocated during slice/bearer activation, initial attach This field is missing if IP address is static (mentioned in 3GPP TS 32.255 [47], clause 6.2.1.2).	O

Field name	Value	M/O (see clause A.1.1)
rAT5Type	This field indicates the Radio Access Technology (RAT) type of PDU session currently, used by the Mobile Station as defined in 3GPP TS 29.571 [43], such as New Radio, Evolved Universal Terrestrial Radio Access, Wireless LAN, Virtual (Virtual shall be used if the N3IWF does not know the access technology used for an untrusted non-3GPP access), when available. Formatted as per 3GPP TS 32.291 [46], clause 6.1.6.2.2.8.	O
flowQosInfo	Authorized QoS applicable for service data flow. See 3GPP TS 29.571 [43] and 3GPP TS 32.291 [46].	O
serviceID	Identity of the used service, given as an integer. See 3GPP TS 32.291 [46], clause 6.1.6.3.2-1.	O
uERadioCapID	The UE radio capability ID is an identifier used to represent a set of UE radio capabilities, defined in 3GPP TS 23.003 [41]. It is encoded as a string of hexadecimal digits from most significant (Type Field) to least significant (RCI).	O
rANSecondaryRATType	Secondary RAT usage is reported from RAN in the 5G charging service. See 3GPP TS 32.291 [46], clause 6.1.6.2.2.17.	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/O (see clause A.1.1)
naDeviceId	Identifier of this device, e.g. the MAC address, PEI.	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
subscriberID	Identifier for a known user of this device or equipment.	O
uERadioCapID	Identifier used to represent a set of UE radio capabilities, defined in 3GPP TS 23.003 [41].	O

E.2.6 NANwElement

This structure contains information on a Network Access Server (NAS).

Table E.7: NANwElement parameters

Field name	Value	M/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/O (see clause A.1.1)
subscriberID	Unique identifier for this subscriber.	O
serviceID	Identifier for the service e.g. account plan name.	O
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.2.3.1.	O
naTransactionID	Unique reference for this transaction/billing record, to be defined on a national basis.	O
naTransactionStatus	Status of the transaction (i.e. "declined", "succeeded", etc.), to be defined on a national basis.	O

E.3 ASN.1 definitions for network access services

For ASN.1 definitions, refer to the ASN.1 module in the archive which accompanies the present document (see clause A.3.1.2).

E.4 Void

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

F.1 Example set of search routines

F.1.1 Overview

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 table F.1.

F.1.2 Summary of search case

Table F.1

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

Table F.2

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 records with matching national registration id are returned.

F.2.2 Telephony billing details

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

Table F.3

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**.

Table F.4

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:

Table F.5

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 analysed 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

Table F.6

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**.

Table F.7

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

Table F.8

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.

Table F.9

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**.

Table F.10

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

Table G.1

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. In cases where endTimes are provided as part of a constraint, a non-populated value in a record can be considered to be greater than the specified endTime in the constraint.

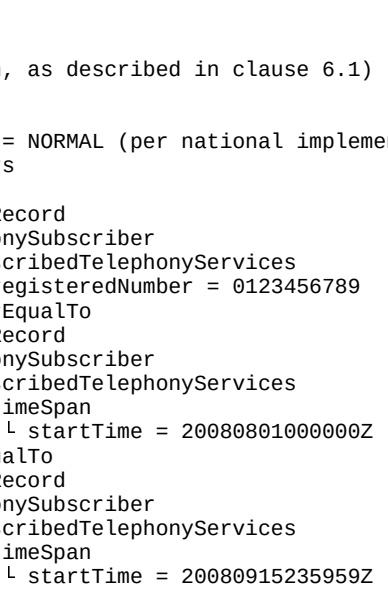


Figure G.1: Example for telephony subscriber query

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: provide service usage records for phone number 0123456789 for calls, which were initiated from that number between 5 September 2008 and 15 September 2008.

Table G.2

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)
       └ requestParameters
          ├ equals
          │  └ telephonyRecord
          │     └ telephonyServiceUsage
          │        └ partyInformation
          │           ├ partyNumber = 0123456789
          │           └ partyRole = 0 (=originating-Party)
          ├ greaterThanOrEqualTo
          │  └ telephonyRecord
          │     └ telephonyServiceUsage
          │        └ communicationTime
          │           └ timeSpan
          │              └ startTime = 20080905000000Z
          └ lessThanOrEqualTo
             └ telephonyRecord
                └ telephonyServiceUsage
                   └ communicationTime
                      └ timeSpan
                         └ startTime = 20080915235959Z
```

Figure G.2: Example for telephony usage query

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): Single versus multi-part deliveries

J.1 General

Subject to national agreement, the multi-part delivery of results may be used replacing the default single shot delivery (clause 5.1.7). In clause 5.2.3 the option of delivering results of an RD query in multiple parts is described. When multi-part is set as possible national delivery option, a CSP may promptly send data that are at hand and follow up with data that takes longer to collect, if and when available. There is however no rule for when to apply multi-part deliveries. In absence of such guidance it is likely that all deliveries will be made in multiple parts, since additional data might always be available. It is also undefined when to send the final message, so the transfer will tend to be open-ended.

In this annex there is an elaboration of criteria for when to apply multi-part deliveries.

J.2 Criteria for multi-part delivery

The maximum time allowed for transfer of retained data from a network element to a storage from which it can be retrieved is called Latency Time (TL). This time may vary, depending on type of network element and operating conditions. An upper limit for TL under different conditions may be set in national requirements. When a request for retained data is made, the related time span is specified as T1-T2. This means that retained data for all events that have occurred during the time span between T1 and T2 and meet the search criteria are to be sent to the receiving authority. T2 will be less than or equal to the time of the request, TR (see however clause J.3). If TL is larger than the difference between TR and T2, some retained data from before T2 can be expected to be collected later than TR, such that multi-part delivery will be necessary, if available data are sent promptly. At a time T2+TL, it can be assumed that all events have been collected.

Figures J.1 and J.2 illustrate the conditions for single- vs multi-part deliveries.

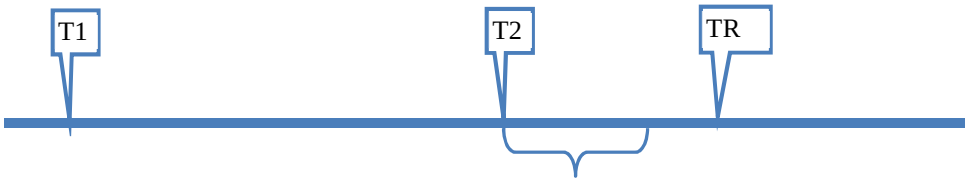


Figure J.1: TR occurs later than T2+TL and thus a single part delivery can be applied

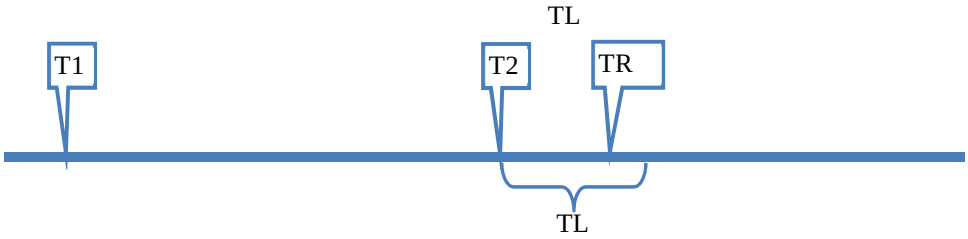


Figure J.2: TR occurs earlier than T2+TL, so a multi-part delivery should be applied

In figure J.2, the last delivery should be sent at time T2+TL, indicating that transmission is complete.

NOTE 1: A CSP may choose to make multi-part deliveries in a sequence in order to break up large transmission volumes into more manageable parts.

NOTE 2: It may be agreed to have a single delivery when all data are available, rather than applying multiple deliveries.

J.3 Subscriptions into the future

It is conceivable to make T2 larger than TR, i.e. subscribe to delivery of retained data into the future. This is a subject for national preferences. An AO may also choose to repeat the request at certain intervals until an investigation has been closed.

Annex K (normative): Service-specific details for Edge Computing applications

K.1 Overview

Edge Computing applications covers those applications offered via edge computing capabilities.

A user may expect an application that is offered via edge computing capabilities, e.g. to:

- Discover the most appropriate Edge Application Servers (EAS) available in the edge data network which support the Edge Computing application.
- Initiate, cancel and terminate an application session with an EAS.
- Support service continuity to minimizing the application layer service interruption by replacing the Source EAS connected to the application client in the UE, with a Target EAS.

K.2 Edge Computing fields

K.2.1 General

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

K.2.2 Edge Computing Subscriber

K.2.2.1 General

This structure contains the information on the Edge Computing subscriber, and the subscribed edge applications, independent of actual usage.

Table K.1: EdgeComputingSubscriber parameters

Field name	Value	M/O (see clause A.1.1)
`subscriberID`	EECID (Edge Enabler Client ID) which represents a unique identifier for this particular subscriber within the ECSP. See 3GPP TS 23.558 [56], clause 7.2.2.	O
`genericSubscriberInfo`	General personal information defined in annex A.	O
`edgeComputingSubscriberInfo`	Edge Computing specific information about the subscriber.	O
`subscribedEdgeComputingApplications`	List of edge applications details that a subscriber (or account) may have.	O

K.2.2.2 subscriberID

The subscriberID is a unique identifier for a particular subscriber within an ECSP, called Edge Enabler Client ID (EECID). The format and content of this field is a string.

K.2.2.3 genericSubscriberInfo

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

K.2.2.4 edgeComputingSubscriberInfo

Information about the subscriber which is specific to edge applications is contained in the SubscriberInfo structure.

K.2.2.5 subscribedEdgeComputingApplications

K.2.2.5.1 Description

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

Table K.2: SubscribedEdgeComputingApplications parameters

Field name	Value	M/O (see clause A.1.1)
edgeComputingApplicationID	A unique identifier within the edge computing ASP for the edge computing application or tariff subscribed to. It is referred as Application Client ID (ACID) in 3GPP TS 23.558 [56], table 8.2.2-1.	O
providerID	A unique identifier for edge computing ASP. 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
registeredIdentifiers	The edge computing application identifiers(s) assigned to the subscriber as part of this subscription, if applicable.	O
edgeComputingApplicationType	The type of edge computing application subscribed to. It is referred as ACType in 3GPP TS 23.558 [56], table 8.2.2-1.	O
installationAddress	The installation address for the subscriber's equipment, if applicable.	O
connectionDate	Date that the subscription was actually connected (may be different to the start of the subscription).	O
iMSI	IMSI associated with the subscriber if available.	O
sUPI	SUPI of the subscriber if available.	O
gPSI	GPSI of the subscriber if available.	O
lineStatus	Edge computing ASP-specific description of current line or subscription status e.g. "Active", "Suspended", etc.	O
paymentDetails	Details for payment (e.g. associated bank account, billing method or billing address).	O
subscriptionType	Describes the nature of the subscription (e.g. prepay, postpay).	O
deliveryAddress	The delivery address for equipment, if applicable.	O
resellerAddress	The address of the reseller or dealer, if applicable.	O
otherAddresses	Used if there are addresses for the subscription which do not fit into the other categories.	O
orderTime	Time when the subscribed application was ordered by user.	O
allocatedDeviceIDs	List of all known devices allocated to this user for this subscription. The user may use other devices in addition (or instead of) these devices. The allocatedDeviceID may be an IMEI, MAC address, etc.	O
paymentTransactions	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause K.2.3.	O

K.2.3 EdgeComputingApplicationBillingDetails

K.2.3.1 EdgeComputingApplicationBillingDetails

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

Table K.3: EdgeComputingApplicationBillingDetails parameters

Field name	Value	M/O (see clause A.1.1)
subscriberID	A unique identifier for a particular subscriber within an edge computing ASP.	O
edgeComputingApplicationID	A unique identifier within the edge computing ASP for the edge computing application or tariff subscribed to.	O
billingAddress	The billing address for this subscription.	O
billingIdentifier	A unique identifier for billing purposes. The format of this field is for edge computing ASPs to determine.	O
billingRecords	A sequence of billing records, one for each payment by the subscriber on this subscription - see clause K.2.3.2.	O
edgeComputingBillingAddress	The billing address for an edge computing application subscription.	O
copyOfBill	The electronic copy of the bill.	O

K.2.3.2 EdgeComputingApplicationBillingRecords

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

Table K.4: EdgeComputingApplicationBillingRecords parameters

Field name	Value	M/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
cryptocurrency	Cryptocurrency of payment, as defined in ISO 24165-2 [57] as unique fixed-length Digital Token Identifier by a registry, issuing one identifier for a specific token, i.e. a specific digital asset, a cryptocurrency.	O
method	Type of payment (e.g. credit card, top-up voucher). The format of this field is for agreement with the edge computing ASP.	O
edgeComputingApplicationTransactionID	Unique identifier for the billing transaction.	O
edgeComputingApplicationTransactionStatus	Status of the billing transaction.	O

Table K.4A: Data elements of records associated to a Digital Token Identifier

Field name	Value	M/O (see clause A.1.1)
digitalTokenIdentifier	Digital Token Identifier (DTI) is based on base record or fork record, with some informative data elements as defined in ISO 24165-2 [57]. A registrar authority, such Digital Token Identifier Foundation will assign such unique value for a specific token. The European Securities and Markets Authority (ESMA's) Digital Ledger Technology (DLT) Pilot regime is based on DTI registered by Digital Token Identifier Foundation. This foundation has based its register on ISO 24165-2 [57].	O
baseRecord	UTF8String, defined by the registrar authority (see ISO 24165-2 [57]).	O
forkRecord	UTF8String, if the DTI is based from a fork record of the original base record.	O
informativeDataElements	It is made of: • Digital Token Name (UTF8String) • Token Identifier Type (UTF8String) • DTI Registration Authority Identifier (UTF8String) • Other Data Elements that a Registration Authority may add as UTF8String	O
digitalTokenName	Two kinds of name, a long name -(UTF8String) and a short name (UTF8String). Their value is defined by the Registration Authority, according to ISO 24165-2 [57]. The original Language Digital Token Name is needed for each of them. Such language name (an UTF8String) is based on ISO/IEC 10646 [58].	O
tokenIdentifierType	Two different types based on their technology: • Digital Token (their elements are defined in clause a of 5.3 of ISO 24165-2 [57]) • Digital Ledger (their elements are defined in clause b of 5.3 of ISO 24165-2 [57])	O
digitalTokenIdentifierType	ISO 24165-2 [57] defines 4 types: • Auxiliary Digital Token • Native Digital Token • Distributed Ledger without a Native Digital Token • Functionally fungible group of Digital Tokens	O
digitalLedgerTechnologyType	Two types are defined by ISO 24165-2 [57]: • Blockchain • Other	O
dTIRegistrationAuthorityIdentifier	Defined in ISO 24165-2 [57]. Its value is an UTF8String.	O

Field name	Value	M/O (see clause A.1.1)
otherDataElements	Based on ISO 24165-2 [57], other data elements are made of: • Underlying Asset External Identifiers Type (an UTF8String) • Underlying Asset External Identifiers Value (an UTF8String) • Digital Token External Identifiers Type (an UTF8String) • Digital Token External Identifiers Value (an UTF8String) • Digital Token Reference Implementation URL (an UTF8String) • Digital Token Unit Multiplier (an UTF8String) • Auxiliary Digital Token (an UTF8String) • Public Distributed Ledger Indicator	O
publicDistributedLedgerIndicator	Public Distributed Ledger Indicator has two values: private or public based on ISO 24165-2 [57].	O

K.2.4 EdgeComputingApplicationUsage

K.2.4.1 Parameters

The EdgeComputingApplicationUsage structure is used for edge computing application usage information, such as call data records. The parameters are as follows.

Table K.5: EdgeComputingApplicationUsage parameters

Field name	Value	M/O (see clause A.1.1)
subscriberID	A unique identifier for a particular subscriber within an edge computing ASP.	O
communicationTime	Total time for this edge computing application session.	O
octetsSent	Number of octets sent by the client to the EAS during the application session.	O
octetsReceived	Number of octets sent by the EAS to the client during the application session.	O
reasonCause	Cause code for end of application session, i.e. normal end, client abort, EAS abort.	O
qualityOfService	The quality of service parameters for the application session.	O
edgeComputingApplicationID	A unique identifier within the edge computing ASP for the edge computing application or tariff.	O
providerID	A unique identifier for the edge computing ASP. The format of this field is to be determined by national agreement.	O
cdrNumber	Identifier for record - Format of value defined by edge computing ASP.	O
clientIP	IP of client at time of application usage.	O

Field name	Value	M/O (see clause A.1.1)
edgeApplicationServersInfo	For each EAS among the set of EASs serving the application session, information related to the EAS, i.e. EAS ID, EAS IP address, EAS location, service continuity requirement indication, virtual resource usage for serving the application session (mean virtual CPU, mean virtual memory, mean virtual disk, and the start and stop time of virtual resource allocation, See 3GPP TS 32.291 [46], table 6.1.6.2.12.3-2).	O

K.2.5 EdgeComputingDevice

K.2.5.1 General

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

Table K.6: EdgeComputingDevice parameters

Field name	Value	M/O (see clause A.1.1)
deviceIDType	Indicates the type of identifier used in edgeComputingDeviceID, e.g. IMEI. (See ASN.1 for permissible types).	O
edgeComputingDeviceID	Unique identifier for the edge computing device. If this identifier happens to have a particular format (e.g. IMEI), then this may be indicated using deviceIDType.	O
subscriberID	Identity of a known user of this equipment.	O

Annex L (informative): Bibliography

- ISO 639:2023: "Code for individual languages and language groups".

Annex M (informative): Change history

Status of the present document: ETSI TS 102 657 Handover interface for the request and delivery of retained data		
TC LI approval 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) Version 1.1.1 prepared by Rapporteur
December 2008	V1.1.2	Re-publication of First publication of the ETSI 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
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 Rapporteur
July 2009	V1.3.1	Included Change Requests: TS102657CR009r1 (Cat B) Error Data Retention for MMS TS102657CR013 (Cat B) Addition of per-subscription device allocation TS102657CR014 (Cat B) Addition of traffic volumes to NAServiceUsage TS102657CR015r1 (Cat B) Addition PUK code to TelephonySubscription TS102657CR016r1 (Cat B) Addition of extra TelephonyEventTypes TS102657CR017r1 (Cat F) Cleanup of RDHI TS TS102657CR018r1 (Cat B) Addition of new ASN.1 parameters TS102657CR020r1 (Cat B) Enabling the transmission of warrants independently of a certain request TS102657CR021 (Cat B) Data Retention for EMS TS102657CR022 (Cat B) National parameters These CRs were approved by TC LI#21 (29 June - 1 July 2009; Sophia Antipolis) Version 1.3.1 prepared by Rapporteur
September 2009	V1.4.1	Included Change Requests: TS102657CR023 (Cat D) Description of the SMS and MMS TS102657CR024r1 (Cat D) Addition of per-subscription device Cleanup of RDHI TS TS102657CR025 (Cat B) Additional MMS delivery flag These CRs were approved by TC LI#22 (22-24 September 2009; Trouville) Version 1.4.1 prepared by Rapporteur
February 2010	V1.5.1	Included Change Requests: TS102657CR004r2 (Cat B) Additional fields for the RDHI on Multimedia Services TS102657CR028r1 (Cat B) Additional cell information TS102657CR030 (Cat B) Extra explanatory MMS status text These CRs were approved by TC LI#23 (9-11 February 2010, Rome) Version 1.5.1 prepared by Rapporteur

Status of the present document: ETSI TS 102 657 Handover interface for the request and delivery of retained data		
TC LI approval date	**Version**	**Remarks**
July 2010	V1.6.1	Included Change Requests: TS102657CR031 (Cat D) Corrections on cross-references and on responseStatus "responseUnavailable" TS102657CR032 (Cat C) Acknowledgements via handover interface ports A and B TS102657CR035 (Cat B) Extra email addresses TS102657CR034 (Cat B) Billing details for email services TS102657CR038 (Cat D) Corrections to Multimedia services section TS102657CR039r1 (Cat B) Additions to Multimedia services section TS102657CR032r1 (Cat B) Addition of a status field to network access subscription TS102657CR033 (Cat B) Addition of ICCID field in network access structure TS102657CR036r1 (Cat B) Single versus Multi-part deliveries These CRs were approved by TC LI#24 (15-17 June 2010, Aachen) Version 1.6.1 prepared by Rapporteur
September 2010	V1.7.1	Included Change Requests: TS102657CR040 (Cat B) National parameters in NASubscription TS102657CR041r1 (Cat B) Extra information in billing records TS102657CR042 (Cat B) Extended location information TS102657CR043 (Cat B) Optional parameters "profession" in the IndividualInfo sequence TS102657CR044 (Cat B) Swiss Map Datum CH1903 in Location information These CRs were approved by TC LI#25 (21-23 September 2010, St. Petersburg) Version 1.7.1 prepared by Rapporteur
February 2011	V1.8.1	Included Change Requests: TS102657CR046 (Cat D) Clarification of example G.2 TS102657CR047 (Cat B) Addition of endReason field to NAServiceUsage TS102657CR048 (Cat F) Correction to Single versus Multi-part deliveries TS102657CR049 (Cat B,C) Addition of direct TCP delivery of XML messages These CRs were approved by TC LI#26 (15-17 February 2011, Sophia Antipolis) Version 1.8.1 prepared by Rapporteur
September 2011	V1.9.1	Included Change Requests: TS102657CRO45r2 (Cat B) Transport level timeouts TS102657CR051 (Cat F) Correction of error in ASN.1 part TS102657CR053r2 (Cat F) Modification of requirement for handling unavailable parameters TS102657CR054r2 (Cat F) Clarification/extension of definitions TS102657CR055 (Cat F) Inconsistency concerning IP Multimedia Subsystem handling TS102657CR057 (Cat D) Supplementary note to IMEI TS102657CR058r1 (Cat F) Editorial corrections TS102657CR059r1 (Cat B) Subscription payment details TS102657CR060r1 (Cat F) Addition to geographical parameters TS102657CR061 (Cat B) Adding TransactionID and TransactionStatus parameters for NABilling records TS102657CR063 (Cat B) Adding the parameter "subscriberID" to the "NAServiceUsage" and "NADevice" sequences TS102657CR064 (Cat F) Corrections of definitions in ETSI TS 102 657 clause D.2.4.1 These CRs were approved by TC LI#27 (28-30 June 2011, Mariehamn TS102657CR052r6 (Cat F) Ambiguous message flow presentation TS102657CR062r1 (Cat C) Providing multiple fixed IP addresses (e.g. range) TS102657CR065 (Cat D) Correction of wrong reference to 3GPP TS 25.413 TS102657CR068r2 (Cat D) Clarification: using responseIncomplete and responseComplete on multi-part-delivery TS102657CR069 (Cat B) Addition of partyType and dialled digits to telephony party information TS102657CR071 (Cat F) Party information definition for DR TS102657CR072r1 (Cat B) ResponseNumber for parallel usage of the method multi-part delivery These CRs were approved by TC LI#28 (13-15 September 2011, Mariehamn Version 1.9.1 prepared by Rapporteur

Status of the present document: ETSI TS 102 657 Handover interface for the request and delivery of retained data		
TC LI approval date	**Version**	**Remarks**
March 2012	V1.10.1	Included Change Requests: TS102657 CR066r1 (Cat F) Integrated Circuit Card ID (ICCID) in "Service Usage" data TS102657 CR073r1 (Cat F,D) Alignment of parameter definitions with ASN.1 definitions TS102657 CR074r1 (Cat F) Correction of various errors in the document TS102657 CR075r1 (Cat F) Text improvements and clarifications TS102657 CR076r1 (Cat B) Addition of supplementary messages TS102657 CR077 (Cat D) Referencing SAI (Service Area Identifier) These CRs were approved by TC LI#29 (24-26 January 2012, Dublin) Version 1.10.1 prepared by Rapporteur
October 2012	V1.11.1	Included Change Requests: TS102657 CR079r1 (Cat B) Retained Data EPS Information This CR was approved by TC LI#31 (25-27 September 2012, Split) Version 1.11.1 prepared by Rapporteur
June 2013	V1.12.1	Included Change Requests: TS102657 CR081r1 (Cat B) Updates for RDHI This CR was approved by TC LI#33 (11-13 June 2013 Joensuu) Version 1.12.1 prepared by Rapporteur
September 2013	V1.13.1	Included Change Requests: TS102657 CR082r1 (Cat B) Addition of pre-pay flag beyond Telephony This CR was approved by TC LI#34 (24-26 September 2013 Edinburgh) Version 1.13.1 prepared by Rapporteur
January 2014	V1.14.1	Included Change Requests: TD009 - CR083 (Cat C) Additional address types TD010r1 - CR084 (Cat B) Update for Network Address Translation TD012 - CR086 (Cat C) Changes for Wi-Fi® TD014 CR087 (Cat F) Missing reference for telephony location TD017r2 CR088 (Cat C) Transmitter Details Technology TD018r1 CR089 (Cat C) EPS location TD029r2 CR090 (Cat B) Max Records Per Batch TD030r1 CR091 (Cat C) Updates to multimedia TD031r1 CR092 (Cat C) Updates to Network Access CR approved by TC LI#35 (Milan) Version 1.14.1 prepared by Rapporteur
June 2014	V1.15.1	TD027 CR093 (Cat F) Update to references TD028r1 CR094r1 (Cat C) Device details TD032r1 CR095r1 (Cat F) XSD correction (change to XSD file only)
September 2014	V1.16.1	TD029r2 CR097r2 (Cat C) Minor issues (Para 5.2.2 and 6.4)
September 2015	V1.17.1	TD028r1 CR098r1 (Cat B) Selective requests by using XPATH notation TD029r2 CR099r2 (Cat B) Additional ASN.1 parameters TD009r1 CR100r1 (Cat B) Additional locations information for mobile Network Access
February 2017	V1.18.1	LI(16)P43020r2 CR101r2 (Cat B) Location for maritime and air mobile comm. LI(17)P44008 CR102 (Cat F) Error in RDMessagever17.xsd, NAServiceUsage Tree LI(17)P44017r3_CR103r3 (Cat B) Adding parameter RequestType LI(17)P44018r4 CR104r4 (Cat B) Adding parameters numberOfRecordsLimit and numberOfRecordsFound LI(17)P44019r1 CR105r1 (Cat B) MSISDN in NAServiceSubscription LI(17)P44020r4 CR106r4 (Cat B) Access Network Information in MultimediaPartyInformation
June 2017	V1.19.1	LI(17)45034r2 CR107r2 (Cat B) PaniHeaderContent parameter
October 2017	V1.20.1	LI(17)46015r1 CR108r1 (Cat F) Upgrade of reference FIPS 186
February 2018	V1.21.1	LI(18)47038r1 CR 109r1: MultimediaServiceRegistrationInfo references country subdivision instead of country

Status of the present document: ETSI TS 102 657 Handover interface for the request and delivery of retained data		
TC LI approval date	**Version**	**Remarks**
June 2018	V1.22.1	LI(18)P48021r2 CR110r2 (Cat B) Addition of an External Identifier and of a Request Flag to the Retained Data Header LI(18)P48022r2 CR111r2 (Cat B) Addition of parameters to common fields LI(18)P48023r2 CR112r2 (Cat B) Addition of parameter bSSID to location LI(18)P48024r2 CR113r2 (Cat B) Addition of Telephony and Multi-SIM Support to Multimedia Subscription and Usage LI(18)P48025r2 CR114r2 (Cat B) Addition of multi-ICCID in Network Access LI(18)P48026r3 CR115r3 (Cat B) Addition of parameter MsgForwardingAddresses and MsgStoreSubscriberRelatedIDs to MsgStore
July 2019	V1.23.1	LI(19)P51036r1 CR117r1 (Cat B) New MapDatum for Switzerland LI(19)P51037r1 CR118r1 (Cat B) Linking subscriptions with payment transactions LI(19)P51038r2 CR119r2 (Cat B) Providing passport or ID copy LI(19)P51039r3 CR120r3 (Cat B) Providing copy of bill LI(19)P51040r2 CR121r2 (Cat F) Change ratType of epsInformation to OPTIONAL in ASN.1 definition LI(19)P51047r5 CR122r5 (Cat B) New parameters for retained data
October 2019	V1.24.1	LI(19)P52014r1 CR123r1 (Cat B) Add location information source LI(19)P52016r1 CR125r1 (Cat B) Add SUPI and GPSI 5G parameters LI(19)P52017 CR126 (Cat F)_Correction of AMFID sequence LI(19)P52018r2 CR127r1 extend n3gaLocation ASN.1 and XSD LI(19)P52043r2 CR128r1 Providing copies of contract documents
February 2020	V1.25.1	LI(20)P53024_CR129 (Cat B) Add_Transmitter_Details_to_Location LI(20)P53025r1_CR130 (Cat B) Add Timed IP-Addresses to NAServiceSubscription
July 2020	V1.26.1	LI(20)P54017r2_CR132r2 (Cat B) Addition of EID Parameter in the Subscrip LI(20)P54019r2_CR133r2 (Cat F) Correction of Coding of NCGI in the ASN.1 LI(20)P54031r4_CR134r4 Addition of 3GPP UE Radio Capability ID LI(20)P54032r3_CR135r3 Update of 5GS different parameters
February 2021	V1.27.1	LI(21)P56016r1_CR136r1 (Cat F) Gender enumeration extension
October 2021	V1.28.1	LI(21)P58014r1_CR137 (Cat B) Add "sendMsg" and "forwardMsg" in the "MsgStoreOperation" LI(21)P58015r3_CR138 (Cat B) Add Client and Server Ports to MsgServiceUsage LI(21)P58016r2_CR139 (Cat B) Add a cSPDefinedName in the WiFiInformation structure LI(21)P58017r3_CR140 (Cat B) Add Trunk Group IDs and IOIs to the Telephony and Multimedia Usage Records
November 2022	V1.29.1	LI(22)P61006r1_CR141 (Cat B) Enhancement related to Edge Computing LI(22)P61016r1_CR142 (Cat F) Moving ASN.1 to attachment
June 2023	V2.1.1	LI(23)P63044r3_CR143 (Cat C) Cryptocurrencies used as payment accepted by Cloud Providers
December 2023	V2.2.1	LI(23)P64006r1_CR144 (Cat B) RAT5Type alignment with TS 129 571
March 2024	V2.3.1	LI(24)P65013r2_CR 145r2 Cat B: Extension of the Definition of PEI LI(24)P65014r2_CR 146r2 Cat F: Change the XML-Schema-definition of iMEI in SubscribedTelephonyServices
July 2024	V2.4.1	LI(24)P66011: CR 147r1 Cat B: Addition of Cellular-Network-Info Header to MultimediaServiceUsage
February 2025	V2.5.1	LI(25)P68009r2: CR 148 Cat B: Addition of crypto-currencies to the billing records LI(25)P68010r1: CR 149 Cat F: Correction of the ASN.1 and XML definitions of DigitalTokenIdentifier

History

Document history		
V1.1.1	November 2008	Publication (Withdrawn)
V1.1.2	December 2008	Publication
V1.2.1	June 2009	Publication
V1.3.1	September 2009	Publication
V1.4.1	December 2009	Publication
V1.5.1	June 2010	Publication
V1.6.1	September 2010	Publication
V1.7.1	October 2010	Publication
V1.8.1	June 2011	Publication
V1.9.1	December 2011	Publication
V1.10.1	September 2012	Publication
V1.11.1	November 2012	Publication
V1.12.1	August 2013	Publication
V1.13.1	November 2013	Publication
V1.14.1	March 2014	Publication
V1.15.1	August 2014	Publication
V1.16.1	October 2014	Publication
V1.17.1	December 2015	Publication
V1.18.1	April 2017	Publication
V1.19.1	August 2017	Publication
V1.20.1	November 2017	Publication
V1.21.1	April 2018	Publication
V1.22.1	September 2018	Publication
V1.23.1	August 2019	Publication
V1.24.1	January 2020	Publication
V1.25.1	March 2020	Publication
V1.26.1	August 2020	Publication
V1.27.1	April 2021	Publication
V1.28.1	December 2021	Publication
V1.29.1	December 2022	Publication
V2.1.1	August 2023	Publication
V2.2.1	January 2024	Publication

Document history		
V2.3.1	March 2024	Publication
V2.4.1	July 2024	Publication
V2.5.1	May 2025	Publication