

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/1a30146d-01ad-4986-85b9-8f6bdb5197cc/etsi-ts-102-657-v1.2.1-2009-06>



Reference

RTS/LI-00059

Keywords

handover, retention

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2009.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	7
Foreword.....	7
1 Scope	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	9
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	10
4 Overview of handover interface	11
4.1 Reference model.....	11
4.2 Structure of document and applicable communication domains	13
4.3 Categories of retained data	14
4.4 Handover Interface port 1 (HI-A) and Handover Interface port 2 (HI-B).....	14
4.5 Model used for the RDHI.....	15
5 Handover interface message flows.....	15
5.1 Introduction	15
5.1.1 Summary of this clause.....	15
5.1.2 Message flow modes.....	15
5.1.3 Delivery cases.....	16
5.1.4 "Active" requests and "closed" requests	16
5.1.5 Errors and failure situations	16
5.1.5.1 Error and failure types.....	16
5.1.5.2 Request process failure feedback	16
5.1.5.3 Other errors	17
5.1.6 Cancelling a request.....	17
5.1.7 Delivery of results.....	17
5.1.8 State diagram	17
5.2 Message flows for general situation.....	19
5.2.1 Delivery of a response	19
5.2.2 Cancellation of request	20
5.2.3 Multi-part delivery	21
5.3 Message flows for Authorized-Organization-initiated scenario	21
5.3.1 Delivery of results or a failure response	21
5.3.2 Cancellation of request	23
5.3.3 Multi-part delivery	23
5.4 HI-A and HI-B addressing.....	24
6 Definition of the elements for retained data messages	25
6.1 Header information.....	25
6.1.1 Use of header information	25
6.1.2 RequestID field specification.....	25
6.1.3 CSP Identifiers.....	25
6.1.3.1 Use of CSP identifiers.....	25
6.1.3.2 Third Party CSP Identifier	25
6.1.4 Timestamp	26
6.2 Retained Data response	26
6.2.1 General.....	26
6.2.2 Additional information in response messages.....	26
6.2.2.1 Record number	26
6.2.2.2 Response status	26
6.2.3 Volatile information.....	26
6.2.4 Unavailable parameters.....	26
6.3 Retained Data requests	27

6.3.1	Information contained within a request	27
6.3.2	Format of a request	27
6.3.3	Additional information in requests	28
6.3.3.1	Priority of a request	28
6.3.3.2	Maximum hits	28
6.4	Error messages	28
7	Data exchange techniques	28
7.1	General	28
7.2	HTTP data exchange	29
7.2.1	Basic configuration	29
7.2.2	Single client/server	29
7.2.3	Mutual client/server	29
7.2.4	Details common to both single and mutual cases	29
7.3	Direct TCP data exchange	30
7.3.1	Transport layer	30
7.3.1.1	Introduction	30
7.3.1.2	TCP settings	30
7.3.2	Network layer	30
7.3.3	Delivery networks	30
8	Security Measures	30
8.1	General	30
8.2	Connection Level Security	30
8.3	Application Level Security	31
8.4	Technical Security Measures	31
8.4.1	General	31
8.4.2	Connection Level	32
8.4.3	Application Level	32
8.4.3.1	Hashes	32
8.4.3.2	Digital Signatures	32
8.4.3.3	HI-B Non-Repudiation	32
8.4.3.4	Digital Signatures and Message Structure	32
Annex A (normative):	Data fields	33
A.1	Summary	33
A.1.1	Introduction to data fields	33
A.1.2	Choice of data modelling language	33
A.1.3	Overview	33
A.2	Parameter definition for common fields	34
A.2.1	RetainedDataHeader	34
A.2.1.1	Parameters	34
A.2.1.2	RequestID parameters	34
A.2.2	RetainedDataPayload	34
A.2.2.1	RequestMessage parameters	34
A.2.2.2	RequestAcknowledgement parameters	34
A.2.2.3	ResponseMessage parameters	35
A.2.2.4	GetStatusMessage parameters	35
A.2.2.5	StatusMessage parameters	35
A.2.2.6	ErrorMessage parameters	36
A.2.3	GenericSubscriberInfo	36
A.2.3.1	Parameters	36
A.2.3.2	OrganizationInfo parameters	36
A.2.3.3	IndividualInfo parameters	36
A.3	ASN.1 definitions	37
A.3.1	General	37
A.3.1.1	ASN.1 syntax tree	37
A.3.1.2	General remarks on ASN.1	37
A.3.2	ASN.1 Definitions for message headers	38
A.3.2.1	Message wrappers	38
A.3.2.2	Message headers	38

A.3.3	ASN.1 definitions for common fields.....	42
A.3.4	Schematic representation of top level ASN.1.....	44
Annex B (normative): Service-specific details for telephony services.....		45
B.1	Scope.....	45
B.2	Telephony fields.....	45
B.2.1	General.....	45
B.2.2	Telephony Subscriber.....	45
B.2.2.1	Subscriber ID.....	45
B.2.2.2	GenericSubscriberInfo.....	45
B.2.2.3	TelephonySubscriberInfo.....	45
B.2.2.4	SubscribedTelephonyServices.....	46
B.2.2.4.1	Description.....	46
B.2.2.4.2	BillingDetails.....	46
B.2.2.4.3	BillingRecords.....	46
B.2.3	Telephony ServiceUsage.....	47
B.2.3.1	Parameters.....	47
B.2.3.2	PartyInformation.....	47
B.2.4	TelephonyDevice.....	48
B.2.4.1	General.....	48
B.2.5	TelephonyNetworkElement.....	48
B.2.5.1	General.....	48
B.2.5.2	Location parameters.....	48
B.2.5.2.1	General.....	48
B.2.5.2.2	GSM Location Information.....	49
B.2.5.2.3	UMTS Location Information.....	49
B.3	ASN.1 definitions for telephony.....	49
Annex C (normative): Service-specific details for asynchronous message services.....		59
C.1	Scope.....	59
C.2	Descriptions.....	59
C.2.1	General.....	59
C.2.2	MsgSubscriber.....	59
C.2.3	MsgSubscriberID.....	60
C.2.4	MsgStore.....	60
C.2.5	MsgStoreID.....	60
C.2.6	MsgAddress.....	60
C.2.7	MsgProviderID.....	60
C.2.8	MsgServiceUsage.....	60
C.2.9	MsgTransmission.....	61
C.2.10	MsgStoreOperation.....	61
C.3	ASN.1 definitions for asynchronous message services.....	62
Annex D (normative): Service-specific details for synchronous multi-media services.....		64
D.1	Scope.....	64
Annex E (normative): Service-specific details for network access services.....		65
E.1	Scope.....	65
E.2	Descriptions.....	65
E.2.1	General.....	65
E.2.2	NASubscriber.....	65
E.2.3	NAServiceSubscription.....	66
E.2.4	NAServiceUsage.....	66
E.2.5	NADevice.....	67
E.2.6	NANwElement.....	67
E.2.7	NABillingDetails.....	68

E.3	ASN.1 definitions for network access services	68
Annex F (informative): Basic set of search routines for Retained Data.....		72
F.1	Example set of search routines	72
F.1.1	Introduction	72
F.1.2	Summary of search case	72
F.1.3	Subscriber records	72
F.2	Telephony data	73
F.2.1	Telephony subscriber	73
F.2.2	Telephony billing details	73
F.2.3	Telephony service usage	73
F.2.4	Telephony network element	73
F.3	Messaging data	74
F.3.1	Message subscriber	74
F.3.2	Message service usage	74
F.4	Network Access data	74
F.4.1	NA subscriber	74
F.4.2	NA service usage	75
Annex G (informative): Examples of search routines		76
G.1	Introduction	76
G.2	Example for telephony subscriber query in clause F.2.1	76
G.3	Example for telephony service usage query in clause F.2.3	76
Annex H (informative): Further information on data categories.....		78
H.1	General	78
H.2	Further information on subscriber data	78
H.2.1	Subscriber data requests	78
H.2.2	Generic subscriber data records	78
H.2.3	Service Specific Subscriber Reply Data	79
H.3	Further information on usage data	80
H.3.1	Usage requests	80
H.3.2	Usage data categories	80
H.3.3	Usage: Traffic Data (Reply)	80
H.3.4	Usage: Traffic Data related information (Reply)	80
H.3.5	Usage: communication independent user activities (Reply)	81
H.3.6	Usage: network Activity Data (Reply)	81
H.4	Further information on network element data	81
H.4.1	Network element requests	81
H.4.2	Network Configuration Data Reply Data	81
Annex I (informative): Manual techniques.....		82
Annex J (informative): Informative mapping of data fields to the EU Data Retention Directive.....		83
Annex K (informative): Change Request History.....		84
History		85

Intellectual Property Rights

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

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

Foreword

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/1a30146d-01ad-4986-85b9-8f6bdb5197cc/etsi-ts-102-657-v1.2.1-2009-06>

1 Scope

The present document contains handover requirements and a handover specification for the data that is identified in EU Directive 2006/24/EC on Data Retention [1]. The handover requirements from TS 102 656 [2] are derived from the requirements contained in and implied by the EU Directive [1] and by other national legislations. The present document considers both the requesting of retained data and the delivery of the results.

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

2 References

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

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

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

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

2.1 Normative references

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

- [1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- [2] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".
- [3] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".
- [4] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".
- [5] ISO 4217: "Codes for the representation of currencies and funds".
- [6] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

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

- [7] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".
- [8] ETSI TS 100 974: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Application Part (MAP) specification (GSM 09.02)".
- [9] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".
- [10] ETSI TS 125 431: "Universal Mobile Telecommunications System (UMTS); UTRAN Iub Interface Layer 1 (3GPP TS 25.431)".
- [11] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".
- [12] ETSI TS 101 109: "Digital cellular telecommunications system (Phase 2+); Universal Geographical Area Description (GAD) (3GPP TS 03.32)".
- [13] FIPS PUB 186-2: "Digital Signature Standard (DSS)".
- [14] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".
- [15] IETF RFC 2818: "HTTP Over TLS".
- [16] ETSI 123 040: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical Realization of Short Message Service (SMS) (3GPP TS 23.040)".
- [17] IETF RFC 0793: "Transmission Control Protocol".
- [18] IETF RFC 2581: "TCP Congestion Control".
- [19] IETF RFC 2988: "Computing TCP's Retransmission timer".
- [20] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".
- [21] IETF RFC 0791: "Internet Protocol".
- [22] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".
- [23] IETF RFC 0822: "Standard for the format of ARPA internet text messages".

2.2 Informative references

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

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

NOTE: Typically, this refers to a warrant or order issued by a lawfully authorized body.

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject

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

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

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

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

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

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

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

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

3.2 Abbreviations

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

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

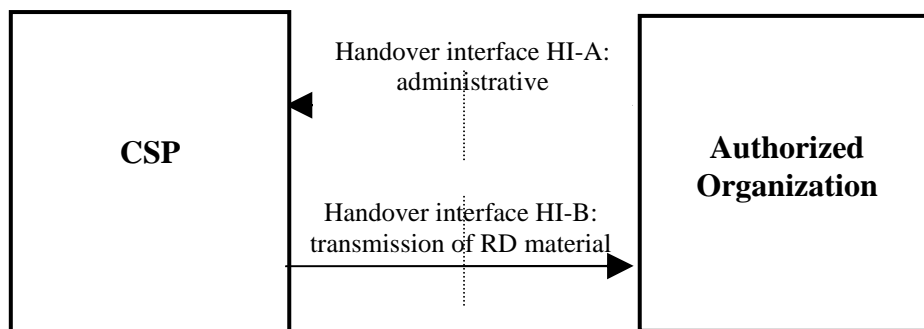
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LAN	Local Area Network
LI	Lawful Interception
MAC	Media Access Control
MSISDN	Mobile Subscriber ISDN number
MSN	Multiple Subscriber Numbers
NA	Network Access
NAS	Network Access Server
PDP	Packet Data Protocol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

4 Overview of handover interface

4.1 Reference model

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

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



NOTE 1: The term Authorized Organization covers any agency legally authorized to make RDHI requests (see clause 3.1).

NOTE 2: HI-B delivers data from CSP to the Authorized Organization. There may be related supporting lower level messages from the Authorized Organization to CSP on HI-B.

Figure 1: Functional diagram showing handover interface HI

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

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

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

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

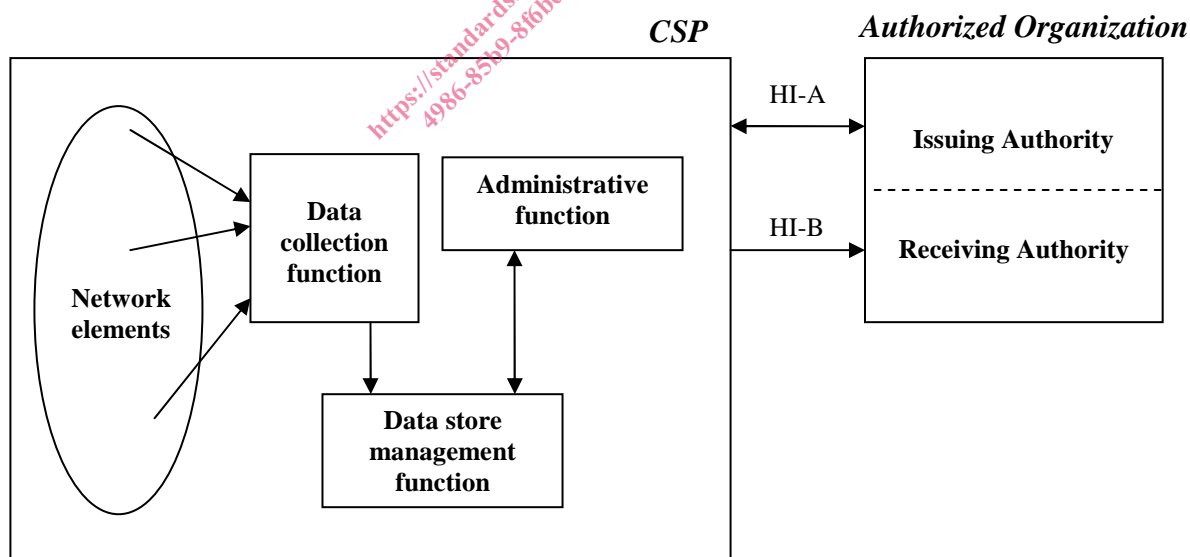


Figure 2: Functional model (informative)

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

4.2 Structure of document and applicable communication domains

The present document defines a framework that applies to all Retained Data. The present document defines a range of services (as shown in figure 3). The present document contains one annex for each service (annex B onwards).

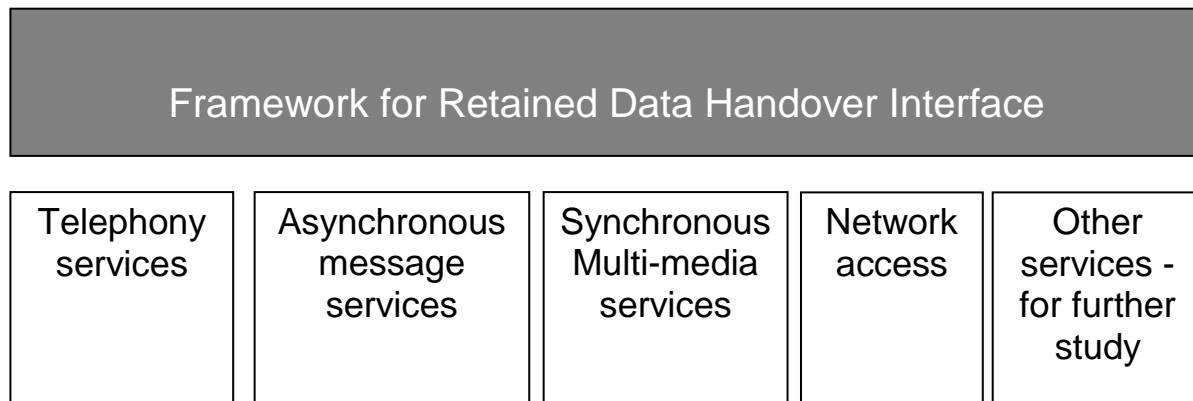


Figure 3: Framework structure

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

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

The scope of each service is as follows:

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

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

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