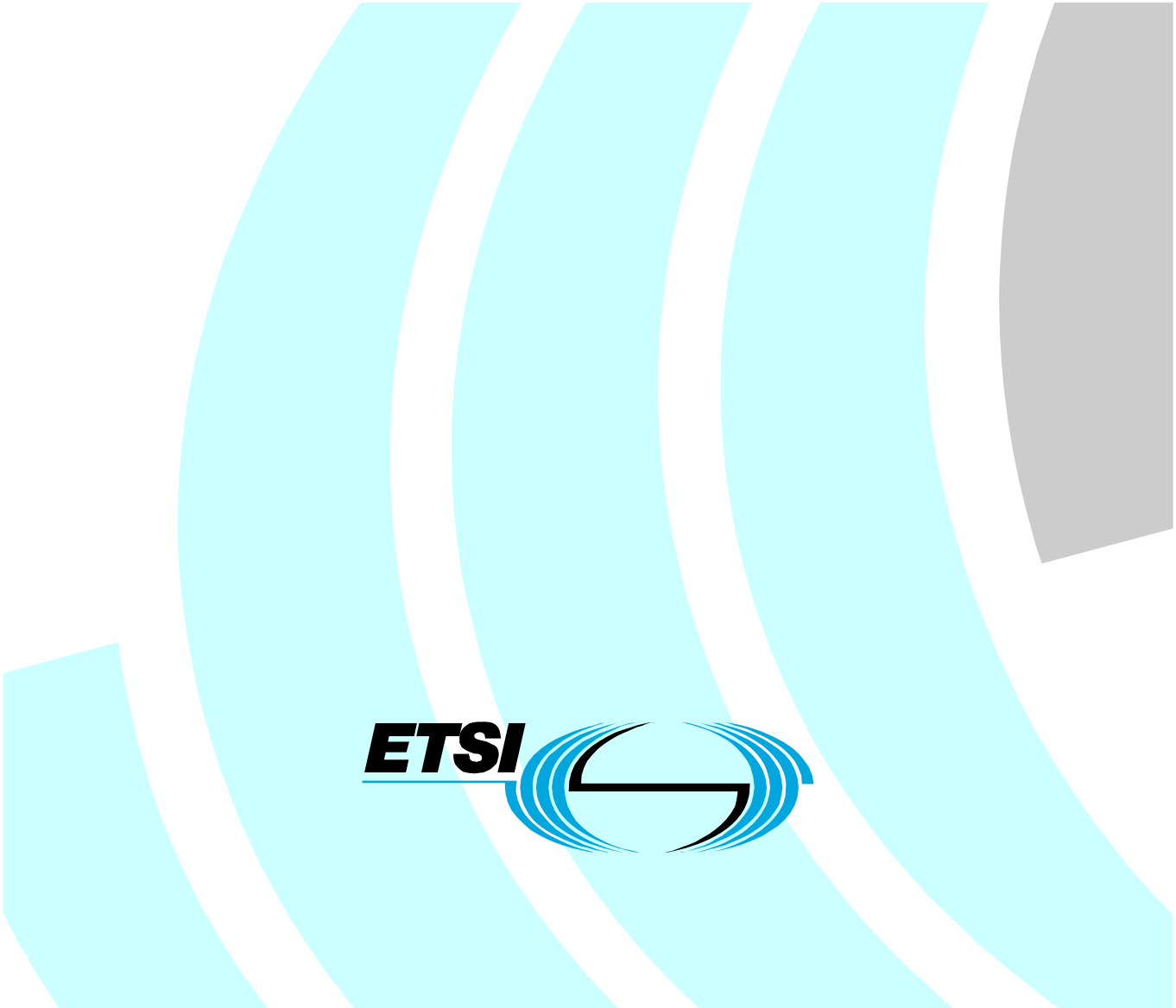
ETSI TR 103 657 V1.1.1 (2011-05)

Technical Report

Lawful Interception (LI);
Retained data handling;
System Architecture and Internal Interfaces



Reference
DTR/LI-00068

Keywords
retention, handover, architecture

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/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

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

Pursuant to the ETSIIPR 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 Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Introduction

The objective of the present document is to provide guidelines and considerations to CSPs that can be useful for implementation of their internal data retention system.

1 Scope

The present document elaborates on RD system architecture and assigns and describes internal interfaces to specific services and functional entities on the CSP side. It provides guidance on implementation issues that CSPs have to deal with.

The document contains:

- A reference model in the network operator and communication service provider domain.
- A high level description of Internal Network Functions and Interfaces.
- Application of the reference model to some typical CSPs.

It does not intend to replace any existing document which specifies network operator and communication service provider's architecture and internal network interfaces. The present document does not override or supersede any specifications or requirements for the Retained Data. In particular, it does not override any clauses in TS 102 656 [i.2] and TS 102 657 [i.3].

2 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 reference document (including any amendments) applies.

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 necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.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.

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

[i.3] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[i.4] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

[i.5] IETF RFC 5424: "The Syslog Protocol".

3 Definitions and abbreviations

3.1 Definitions

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

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: 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

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:

AF	Administrative Function
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CPE	Customer Premises Equipment
CSP	Communications Service Provider
DCF	Data Collection Function
DSF	Data Store Function
DSMF	Data Store Management Function
GSM	Global System for Mobile communications
HI	Handover Interface
HTTP	HyperText Transfer Protocol
ID	Identifier
IHI	Internal Handover Interface
IP	Internet Protocol
LI	Lawful Interception
MF	Mediation Function
RD	Retained Data
RDHI	Retained Data Handover Interface
TCP	Transmission Control Protocol
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

4 Reference model

The overall retained data framework is extended from the model described in clause 4 of TS 102 657 [i.3] (see figure 1).

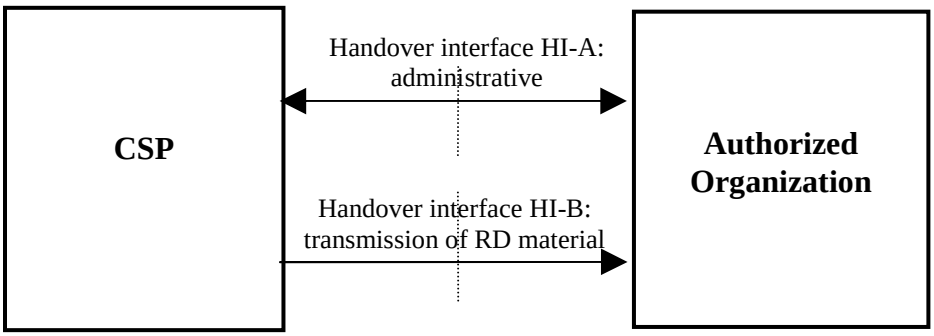


Figure 1: Functional diagram showing handover interface HI (from TS 102 657 [i.3])

Furthermore, TS 102 657 [i.3] identifies two functions as part of the Authorized Organization (AO): an *issuing authority* responsible for initiating new Retained Data Handover Interface (RDHI) requests and a *receiving authority* to accept the RDHI responses, respectively. However, the focus of the present document is not on the Authorized Organizations, but on the element marked "Communications Service Provider (CSP)" in figure 1. A generic reference model for this functional element is given in figure 2.

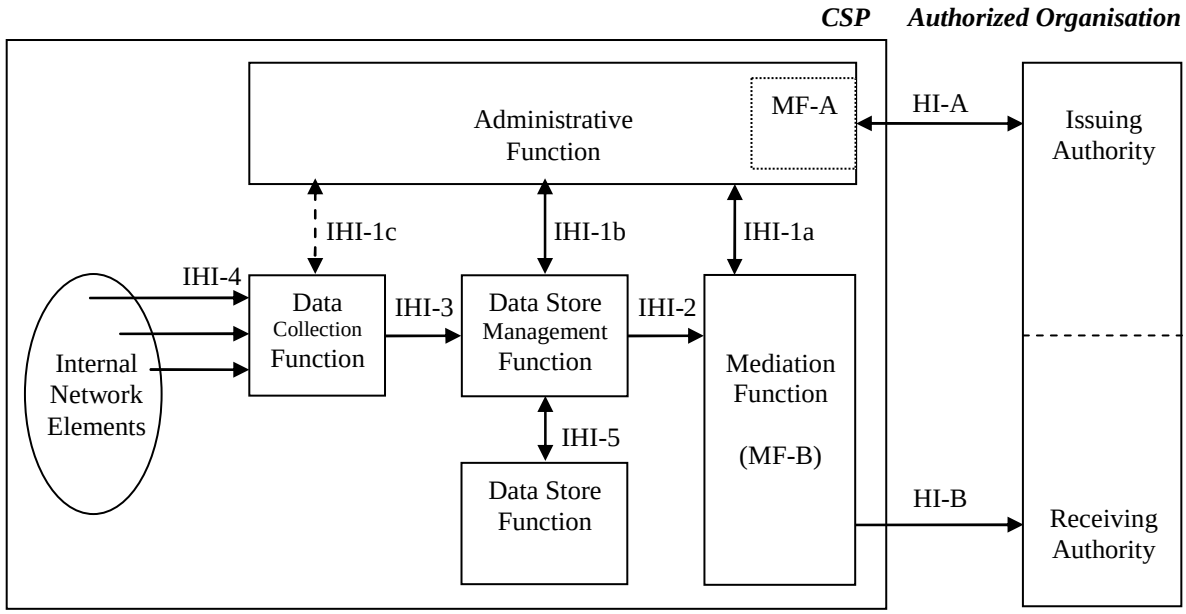


Figure 2: Retained Data reference model

In this reference model, five internal CSP functions can be identified:

- an administrative function (AF) to manage the RD requests and responses;
- a data collection function (DCF) to collect data from the various internal network elements and prepare the data for retention;
- a data store management function (DSMF) to execute queries, and eventually erase RD after the mandatory retention period;
- a data store function (DSF) to store the data;
- a mediation function (MF) to implement the handover interfaces A and B.

These functions will be further explained in clause 4.2.

Also, the reference model shows four internal CSP interfaces:

- Internal Handover Interface 1 (IHI-1a, IHI-1b, IHI-1c) to manage and monitor the Data Collection Function, Data Store Management Function, and the Mediation Function;
- Internal Handover Interface 2 (IHI-2) to deliver the results of RD queries from the DSMF to the MF;
- Internal Handover Interface 3 (IHI-3) to let the DCF add new RD records to the DSMF;
- Internal Handover Interface 4 (IHI-4) to let the DCF collect data from the various network elements;
- Internal Handover Interface 5 (IHI-5) to let the DSMF operate the DSF.

These internal interfaces will be further explained in clause 5.

In addition to these internal interfaces, it is assumed that the Issuing Authority and the Receiving Authority share a communication channel. This internal interface is not specified in the present document.

4.1 Design principles

In summary, the design principles discussed here are:

- Storage:
  Retained data may either be kept in a separate storage or secured in regular network nodes during the retention period.
- Availability:
  Data to be retained will be made available to law enforcement as soon as it is at hand in network nodes.
- Storage format:
  Retained data may be stored either in a free format or a format according to RDHI specifications.

4.1.1 Choice of storage for Retained Data

The alternatives considered here are:

1) Separate storage:
   Data is extracted from network nodes and transferred to an area that is dedicated for retained data.
2) Integrated storage:
   The set of data that is to be retained is labelled and protected against deletion from network nodes during the time of retention.

The pros and cons for these alternatives may be listed as follows:

	Pros	Cons
Separate storage	• Data is protected against volatility of storage formats due to modifications of the business critical systems. • Special security measures can be applied to protect integrity of the retained data. • It may be less costly to query the data base of retained data, compared to having it spread out in the regular network data bases.	• Since only a small fraction of the retained data will ever be requested by law enforcement, it will be unnecessarily costly to move all retained data to separate storage. • Keeping retained data in separate storage increases risk of exposure of logs and queries to hackers.
Integrated storage	• Nothing needs to be moved; it will be sufficient to label relevant data for protection during the retention period.	• The procedures for management of retained data in network nodes have to be modified when business critical systems are upgraded. • Retained data will be kept along with operational data, so there may be an increased risk for information leaks. • Requests for retained data will have to be forwarded to storage and/or data bases outside the RD system. This would disclose what LEAs are looking for and also call for additional interfaces between the RD system and network nodes.

4.1.2 Prompt delivery

The word "prompt" is to be understood as "without undue delay" and means that data to be retained should be made available to law enforcement as soon as regular operative procedures of the CSP allow. The issue of defining what "promptly" means varies from case to case, depending on technical facilities and operational conditions. This is an issue for national requirements and agreements with CSPs. According to the Directive [i.1], CSPs are obliged to retain only the data that they generate or process for business purposes. Implicitly this would mean that data could not be extracted before it is available according to standard routines.

4.1.3 Storage format

The alternatives considered here are:

1) Native format:
   Data are kept as-is in the format it occurs in network nodes. Before delivery it will be converted to RDHI format by the MF.

2) RDHI format:
   The flow of data from network nodes over IHI-4 is pre-processed by the MF before separate storage.

The pros and cons for these alternatives may be listed as follows:

	Pros	Cons
Native format	• Storage is made as simple as possible; a minimum of processing power will be spent for storage. • No extra processing power will be spent on the majority of data that never will be requested by law enforcement.	• Searches may become complicated, since queries will have to be mapped onto the native storage format. • Search routines and mediation functions will have to be maintained to match possible changes in the native formats. There would be version issues. • There would be an extra delay in delivery to law enforcement due to conversion processing.
RDHI format	• Data can be checked for consistency at the time of storage. Irregularities in conversion to the RDHI format can be detected right away. • Query delivery can be done faster.	• More processing power would be spent on the majority of data that never has to be delivered to law enforcement. • Storage space may increase, especially if data is stored in XML format. • Might make it easier for hackers • Query times may be longer than for database optimized storage formats.

4.2 Functional elements

4.2.1 Administrative Function

The Administrative Function (AF) contains interfaces (HI-A) and security provisions for communicating with authorities for reception of and feedback on requests for retained data. It also manages internal interfaces on the CSP side for setting up delivery of results to authorities (IHI-1a), for intermediary storage of retained data (IHI-1b) and for collection of data from internal network elements (IHI-1c).

The communication over HI-A should follow the RD standard as specified in TS 102 657 [i.3]. Requests may be received optionally in ASN.1/BER or XML. Security issues are subject to national preferences, but TR 102 661 [i.4] may be used for guidance. The AF should be able to store all requests and related feedback for auditing purposes, according to what is required on a national basis.

The AF provides the Mediation Function (MF-B) with information about where and how to send results of each query based on information given in the request received over HI-A.

The AF will order the Data Store Management Function (DSMF) to deliver retained data to the MF according to what is being requested over HI-A. The result of such an order will be reported back to the issuing authority over HI-A. The AF will also control purging of data from the DSMF according to regulations.

The AF may control the data collection function (DCF) on a system level above individual requests, e g to check for completeness of retained data or manage connections to network nodes.

4.2.2 DCF

One function of the Data Collection Function (DCF) is to hide the complexities of the Internal Network Elements, so that the Data Store Management Function is presented with a uniform interface IHI-3. The DCF will have access to network nodes where data that are to be retained are generated and/or stored. The DCF will receive such data, either push or pull, normalize them and forward to the Data Store Management Function (DSMF).

4.2.3 DSMF

The Data Store Management Function (DSMF) handles the addition, retrieval, and destruction of all retained data during the period of retention. It will be able to receive data on a normalized form and insert them into a data store, from which data can be retrieved at a later time in an efficient manner. The examples given in Annex F of TS 102 657 [i.3] may be used as a guidance for how to set up indexing of a data base.

4.2.4 DSF

The Data Store Function (DSF) handles the (large) storage of all retained data during the period of retention, including online as well as offline storage and backups.

4.2.5 MF

The Mediation Function (MF) will handle delivery of results of requests for retained data according to standard. It will be set up with delivery data from requests over interface IHI-1a and thus be prepared to deliver results to designated destinations according to the related request. Results may be delivered in either ASN.1/BER or XML encoding.

4.3 Operational considerations

4.3.1 Cancelling a request

When the Issuing Authority cancels a request, the Cancel message will be sent via HI-A to the Administrative Function. The AF will then inform the Data Store Management Function and/or the MF-B as necessary.

The Receiving Authority cannot cancel requests.

4.3.2 Expiry of RD records

When the maximum retention period has been reached, records have to be destroyed (including any backups). The DSMF is responsible for destruction of records.

The DSMF will destroy records autonomously.

Destruction of records can be a continuous activity. Alternatively, destruction may be performed at regular intervals, e.g. once daily or once per month. The interval will be determined by national regulations and/or by operational considerations by the CSP. For example, when the data store is "dual purpose" the purging may be scheduled so as not to interfere with other business activities.

When purging is not done continuously, it may happen that some records are delivered in response to an RD request despite having reached their retention period. If this situation is not permitted by national regulations, the DSMF has to perform a post-query clean-up of records, before passing the records on to the Mediation Function.

4.4 Message types for HI-A and HI-B

The reference model in figures 1 and 2 allows for a different delivery point for HI-A and HI-B messages. For some message types, TS 102 657 [i.3] states whether those messages are to be transmitted over HI-A or HI-B. This clause summarizes the information on the relation between message types and handover interface ports from TS 102 657 [i.3], and expands on issues on which TS 102 657 [i.3] remains silent.

Note that in the expanded reference model the MF-A 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. Note that the Issuing Authority and the Receiving Authority are functional entities. Particular implementations may choose to combine the Issuing and Receiving Authorities.

- requestMessage:
  used to instruct the CSP about a new request for RD information. Always sent using HI-A.

- requestAcknowledgement:
  sent by the CSP to confirm to the Issuing Authority that the request is now active. Always sent using HI-A.

- responseMessage, status Complete:
  sent by the CSP to deliver RD information to the Receiving Authority, and to inform the Receiving Authority that no further information is available. Always sent using HI-B.

- responseMessage, status Incomplete:
  sent by the CSP to deliver RD information to the Authorized Organisation, and to inform the Authorized Organisation that further information may be available. Always sent using HI-B.

- responseMessage, status Unavailable:
  sent by the CSP to indicate, in response to a getResultsMessage, that no results are yet available. Always sent using HI-B.

- responseMessage, status Failed:
  sent by the CSP to indicate that a request (requestMessage, cancelMessage, getstatusMessage, or getResultsMessage) could not be handled. This can be for a variety of reasons, including insufficient authorization or the MaxHits parameter being exceeded. Whether HI-A or HI-B is used depends on the request being responded to. Failure responses are always sent via the same port as the request being responded to. Failure responses for requestMessage and cancelMessage are thus returned via HI-A; failure responses for getstatusMessage and getResultsMessage are returned via HI-B.

- responseAcknowledgement:
  sent by the Authorized Organisation to confirm reception of a response message. Whether HI-A or HI-B is used depends on the response being acknowledged. Acknowledgements are always sent via the same port as the response being acknowledged. Acknowledgements for responses with status Complete, Incomplete, and Unavailable are thus returned via HI-B; acknowledgements for failure responses can be returned either via HI-A or HI-B, depending on the failure. When the response message being acknowledged contains the status "Complete" or "Failed", the Receiving Authority will inform the Issuing Authority that the request is now closed.

- errorMessage:
  sent by the CSP to indicate that a request (requestMessage, cancelMessage, getstatusMessage, getResultsMessage, or any badly formatted request) could not be handled at all. Whether HI-A or HI-B is used depends on the request being responded to. Error messages are always sent via the same port as the request being responded to.

- cancelMessage:
  sent by the Issuing Authority to inform the CSP that a previously issued request is no longer relevant, and that processing on that request may be terminated immediately.

- cancelAcknowledgement:
  sent by the CSP to confirm reception of a cancel message. Such acknowledgements are always sent via HI-A.

- getstatusMessage:
  sent by the Receiving Authority to poll the CSP for available results. Always sent via HI-B. Only used in the Authorized-Organization-initiated scenario.

- statusMessage:
  sent by the CSP in response to a getstatus message. Always sent via HI-B. Only used in the Authorized-Organization-initiated scenario.

- getResultsMessage:
  sent by the Receiving Authority to trigger delivery of available results. Always sent via HI-B. Only used in the Authorized-Organization-initiated scenario.

Table 1 summarizes this information.

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

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

5 Internal Handover Interfaces

This clause describes the functional aspects of the Internal Handover Interfaces (IHI).

For each of these interfaces implementation is possible using HTTP. See TS 102 657 (clause 7.2.4) [i.3] for additional information on using HTTP for data exchange.

5.1 IHI-1

IHI-1 is used by the Administrative Function to manage and monitor the other functional elements. IHI-1 is split into IHI-1a (for the Mediation Function), IHI-1b (for the Data Store Management Function), and IHI-1c (for the Data Collection Function).

5.1.1 IHI-1a

IHI-1a manages and monitors the MF-B. IHI-1a can be used to relay the following types of information.

- *RD-results:*
  Results of RD requests can either be sent from the DSMF to the MF-B directly, or indirectly via the AF. In the latter situation, the RD-results message transfers the results from the AF to the MF-B.

- *Status:*
  When partial results or the final results have been sent to the Receiving Authority and an acknowledgement has been received, the MF-B will update the AF on the status of the request using the Status message.

IHI-1a can be implemented using HTTP on top of the standard TCP/IP stack. This can be configured either as a single client/server configuration, or a mutual client/server configuration. In the single client/server configuration, the MF-B will act as HTTP server, and the AF will act as HTTP client. All communication has then to be initiated by the AF. This implies that the AF has to poll the MF-B at regular intervals about status updates. In the mutual client/server situation, both the DCF and AF will act as client as well as server. In either case, messages can be encoded using XML, or any other appropriate format.

When HTTP is not used, IHI-1a can be implemented using any other standard or proprietary protocol. For example, the RD-results message can be implemented using BER encoded structures using the ASN.1 definitions from TS 102 657 [i.3], and the Status message can be sent to the AF using Syslog.

5.1.2 IHI-1b

IHI-1b manages and monitors the Data Store Management Function (DSMF). It is used to initiate RD requests and, if applicable, expiry of RD records. Depending on the RD architecture used, IHI-1b also transfers the RD query results back to the AF. IHI-1b can be used to relay the following types of information.

- *RD-request:*
  When the AF has received and accepted a new RD request, the RD-request message will instruct the DSMF on the query to be executed. In addition to the request itself, this message also contains all required administrative information, such as the request ID and HI-B delivery point.

- *RD-results:*
  Results of RD requests can either be sent from the DSMF to the MF-B directly, or indirectly via the AF. In the latter situation, the RD-results message transfers the results from the DSMF to the MF-B. This message can also be used to indicate fault and error situations when an RD request cannot be processed, e.g. when the MaxHits parameter is exceeded.

- *RD-cancel:*
  It is possible that the Authorized Organisation cancels an open RD request. If the AF receives a Cancel message, it will forward this message to the DSMF.

IHI-1b can be implemented using HTTP on top of the standard TCP/IP stack. This can be configured either as a single client/server configuration, or a mutual client/server configuration. In the single client/server configuration, the DSMF will act as HTTP server, and the AF will act as HTTP client. All communication has then to be initiated by the AF. This is inconvenient for error messages sent by RD-results, and especially so for the Purge-request/ reply messages. If these two messages are used, the mutual client-server configuration is advisable. In the mutual client/server situation, both the DSMF and AF will act as client as well as server. The RD-request and RD-results can be XML-encoded using the same scheme used for HI-A and HI-B.

When HTTP is not used, IHI-1b can be implemented using any other standard or proprietary protocol. The BER encoding of the ASN.1 version of HI-A and HI-B can be used for RD-request and RD-results.

5.1.3 IHI-1c

IHI-1c manages and monitors the Data Collection Function (DCF). It is used to notify the DCF of changes in the network configuration, and to inform the AF of errors during collection of data to be retained. IHI-1c can be used to relay the following types of information.

- *Configuration:*
  When network elements are added, modified, moved, or removed the AF will provision the DCF with a Configuration message.

- *Error:*
  In case of errors, the DCF will inform the AF with an Error message, e.g. when the DCF is unable to contact some network element, or in case of authentication failures.

IHI-1c can be implemented using HTTP on top of the standard TCP/IP stack. This can be configured either as a single client/server configuration, or a mutual client/server configuration. In the single client/server configuration, the DCF will act as HTTP server, and the AF will act as HTTP client. All communication has then to be initiated by the AF. This implies that the AF has to poll the DCF at regular intervals about error situations. In the mutual client/server situation, both the DCF and AF will act as client as well as server. In either case, messages can be encoded using XML, or any other appropriate format.

When HTTP is not used, IHI-1c can be implemented using any other standard or proprietary protocol. For example, the Configuration message can be implemented using FTP, and the Error message can be sent to the AF using Syslog.

5.2 IHI-2

IHI-2 is used by the Data Store Management Function (DSMF) to submit the results of an RD request to the Mediation Function, for onwards transmission to the Receiving Authority. This interface is optional. If it is not used, then RD results will be relayed from the DSMF to the MF-B via the AF, using interfaces IHI-1b and IHI-1a respectively. In addition to the RD records, the results will contain an indication of whether the result is final or not. When using multi-part delivery (see TS 102 657 (clause 5.1.7) [i.3]), only the last result will be marked as final.

When IHI-2 is used, it can be implemented using HTTP on top of the standard TCP/IP stack. The MF-B will act as HTTP server, and the DSMF will act as HTTP client. The RD results can be XML-encoded using the same scheme used for HI-B.

When HTTP is not used, IHI-2 can be implemented using any other standard or proprietary protocol. For example, a direct TCP connection can be used, using the BER encoding of the ASN.1 version of HI-B.

5.3 IHI-3

IHI-3 is used by the DCF to submit new records to the DSMF for inclusion in the RD store. The DCF receives all required information, and presents it in a format that is suitable for inclusion in the RD store without further conversion.

Data on the IHI-3 interface can be identified with the corresponding RDHI record type, but no further structuring should be necessary on that interface; the DSMF will be aware of how to handle the information related to each record type. There could also be proprietary record types, which would be known to the DSMF.

The information included in IHI-3 might typically be:

- RDHI record type:
  e.g. "Telephony Service Usage" or "Message Service usage", c.f. definitions in TS 102 657 [i.3]. There might also be a record type ‘Other’ referring to a proprietary format record type.
- Information about encoding:
  i.e. ASN.1, XML or "other".
- Reference for encoding:
  Version number for RDHI format records or a reference to specification of "other" format, known within the specific RD system.
- Record contents as an octet string.

5.4 IHI-4

IHI-4 is used by the DCF to collect data from the various network elements. All collected data is normalized and sent out via IHI-3 for storage on the DSMF. Since data has to be collected from a wide variety of different network elements, the DCF will have to implement various "types" of IHI-4 interfaces. The type of IHI-4 interface that is best suited depends on the layout of Customer Premises Equipment (CPE) network and the supported interfaces in the network element; in reality a DCF will have to implement multiple distinct IHI-4 interfaces.

Examples of possible IHI-4 interfaces include:

- TS 102 657 [i.3];
- Call Detail Records (CDRs) push/pull via FTP/HTTP;
- Passive Probing (for example; extracting assigned ip-addresses from DHCP);
- Simple Network Management Protocol (SNMP) Views;
- Syslog (RFC 5424 [i.5]) based (record) push;
- Direct database access;
- XML based push/pull via FTP/HTTP;

- Proprietary interface.

In some cases it may not be possible to collect a complete dataset using a single IHI-4 interface; data collected via multiple distinct IHI-4 interfaces may need to be aggregated by the DCF. The level of aggregation needed depends on the used IHI-4 and IHI-3 interfaces.

5.5 IHI-5

IHI-5 is used by the DSMF for retrieval and storage of retained data in the DSF. The DSF can be a standalone database for retained data inside the RD system and/or storage space inside network nodes, where retained data is kept in proprietary format.

5.5.1 Storage in and retrieval from internal database

The DSMF will have transformed the flat RDHI-style data into formats that are compatible with the chosen database properties. The interface might for instance apply SQL commands to store and retrieve data. The interface would be designed accordingly, based on requirements for interaction with the chosen database mechanisms.

5.5.2 Retrieval from external data storage

The DSMF will not have to concern itself with storage of data to external storage in network nodes, since this is done internally within the nodes, based on the set of data that is controlled by the node and the rules for retention, related to each set of data.

Retrieval of retained data from network nodes to the DSMF will be based on incoming requests, from the AF to the DSMF, which will transform them to search procedures suitable for each respective node, where retained data are stored.

5.6 Message flows

The following clauses illustrate the interactions between the functional elements, and the use of internal handover interfaces. Only the most common scenarios are outlined. Clause 5.6 does not give an exhaustive overview of all possible message flows.

5.6.1 Standard scenario

The message flows in figure 3 correspond to the "general situation" as described in the RDHI.

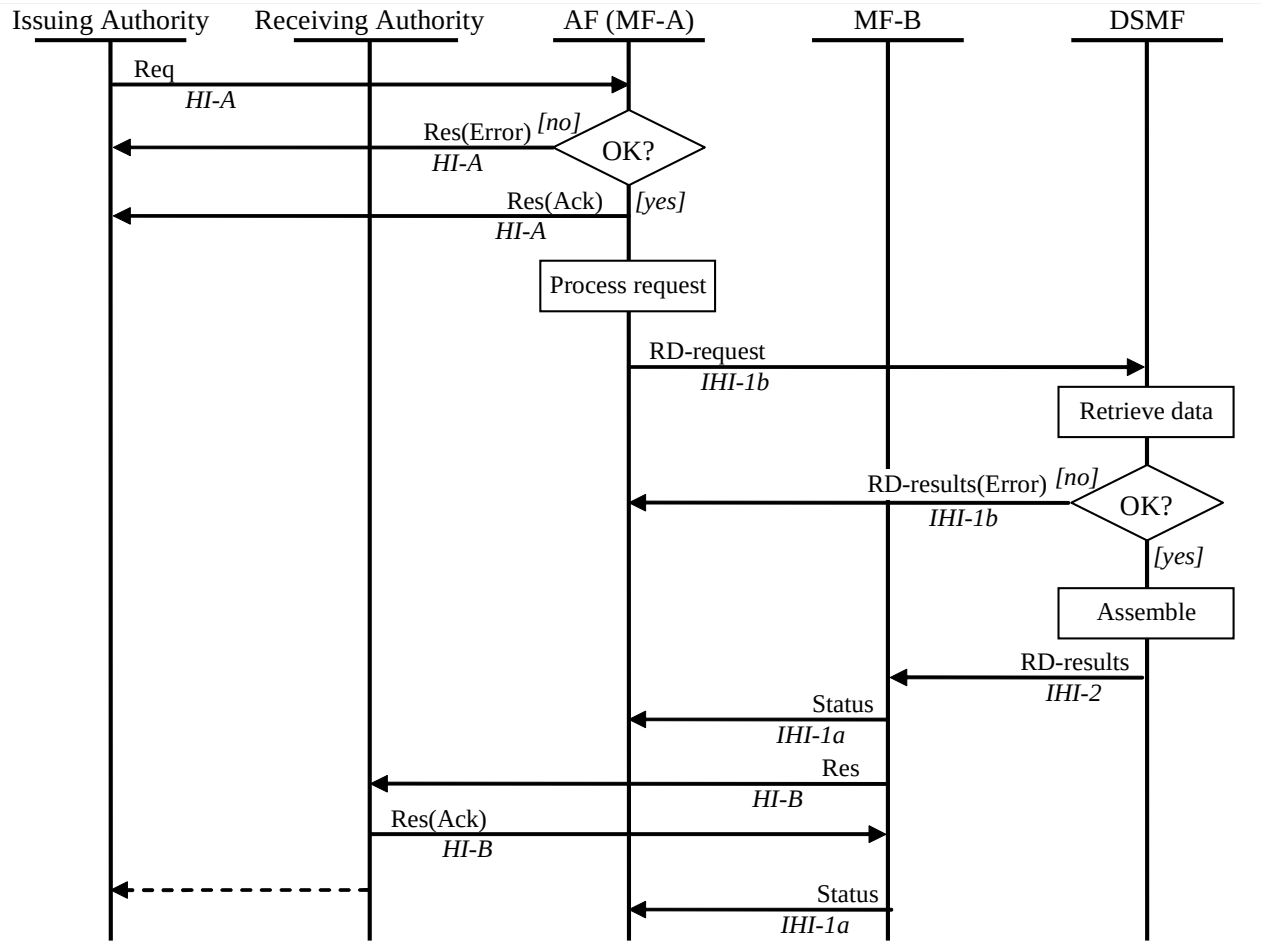


Figure 3: Message flows for the standard scenario

The communication between the Receiving Authority and the Issuing Authority (indicated by a dashed arrow) is not part of the present document.

5.6.2 Multi-part delivery scenario

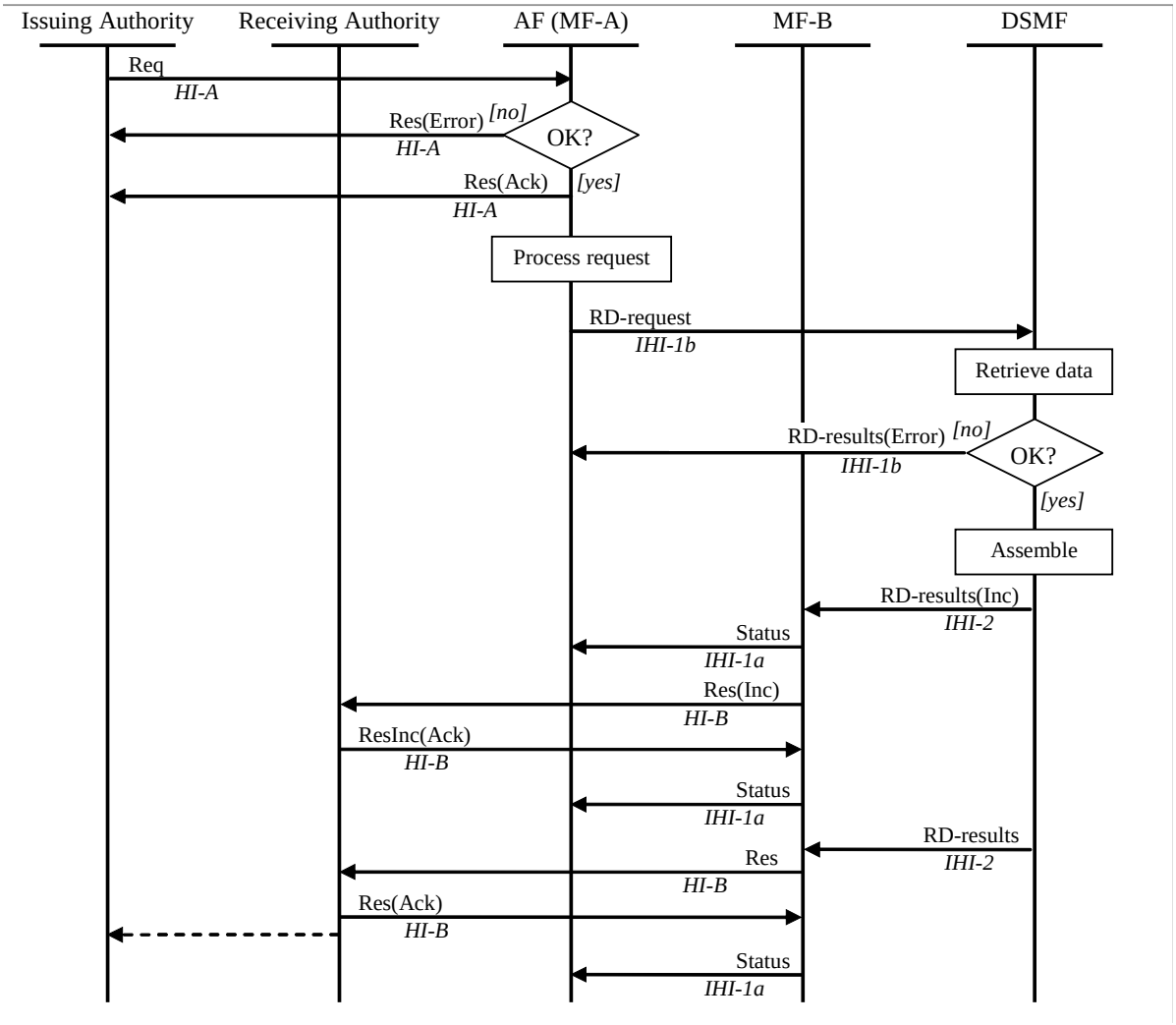


Figure 4: Message flows for multi-part delivery

In the example in figure 4, results are sent in two batches. Each batch is individually acknowledged. When the last batch has been received by the Receiving Authority, the Receiving Authority informs the Issuing Authority that all results have been received. This message is not described in the present document; in figure 4 it is indicated by a dashed arrow.

5.6.3 Authorized Organisation initiated scenario

The message flows in figure 5 correspond to the "Authorized-Organisation-initiated scenario" as described in the RDHI.

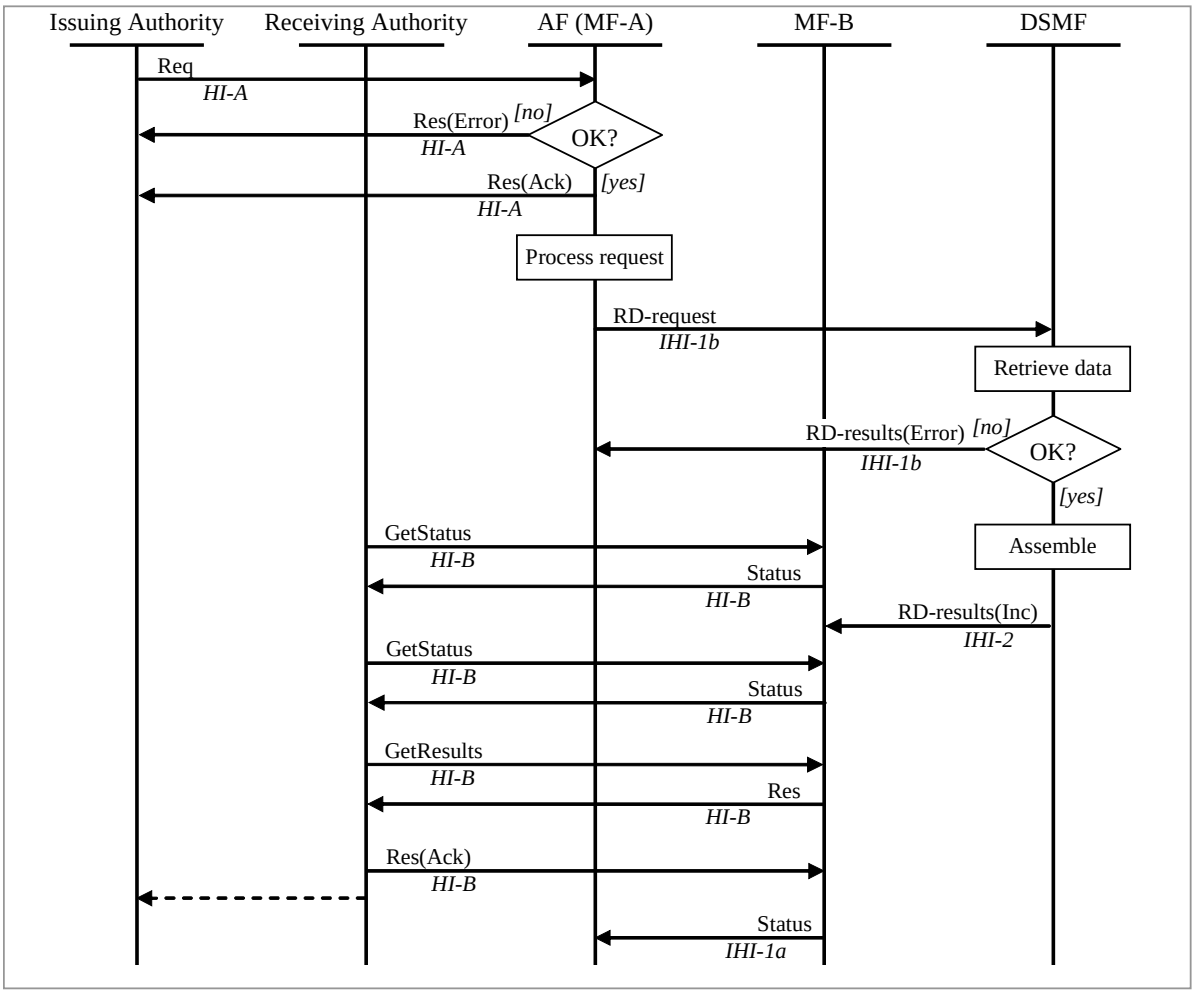


Figure 5: Message flows for the Authorized-Organization-initiated scenario

In the Authorized-Organisation-initiated scenario, the MF-A and MF-B cannot initiate the sending of messages to the Issuing Authority or Receiving Authority (see the RDHI for details). After the DSMF has sent RD results to the MF-B, the MF-B has to wait for a GetResults message from the Receiving Authority before it can transmit the RD results. The Receiving Authority periodically issues GetStatus messages, to determine whether RD results are ready for transmission at the MF-B.

5.6.4 Collection and destruction of retained data

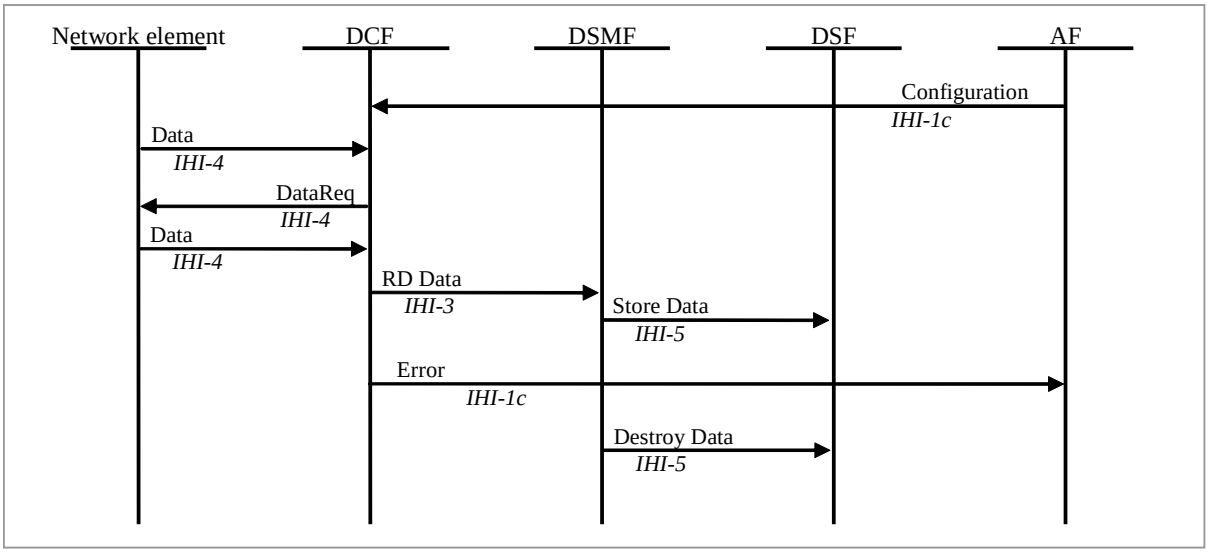


Figure 6: Message flows for collection and destruction of data

Annex A:
Change request history

Status of the present document: TR 103 657 Retained data handling; System Architecture and Internal Interface		
Date	**Version**	**Remarks**
February 2011	1.1.1	First publication of the TR after approval by ETSI/TC LI#26 (15-17 February 2011 in Sophia Antipolis) Version 1.1.1 prepared by Eelco Vriezekolk (Agentschap Telecom) (rapporteur TR)

History

Document history		
V1.1.1	May 2011	Publication