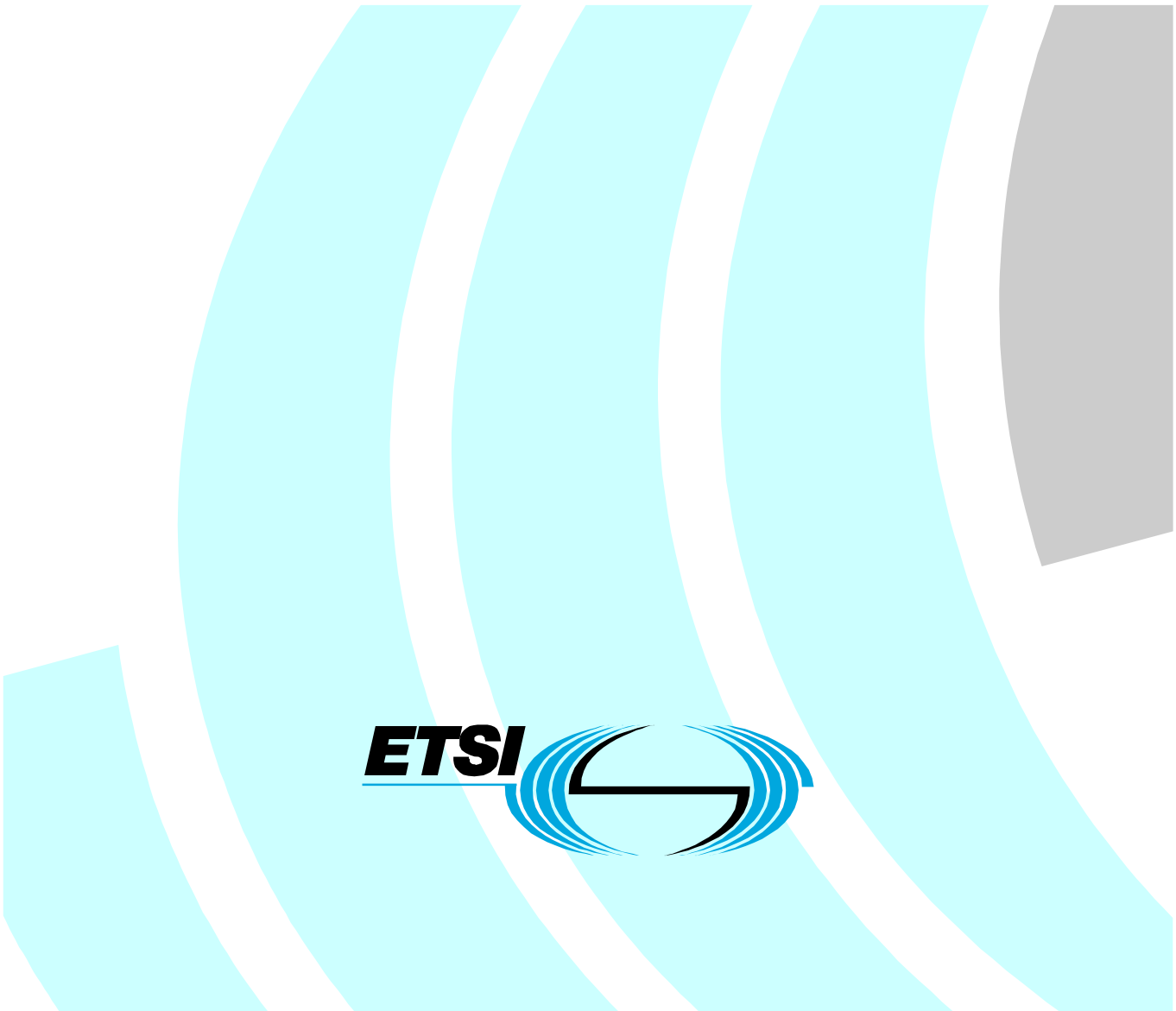
ETSI TS 102 232 V1.1.1 (2004-02)

Technical Specification

Telecommunications security;
Lawful Interception (LI);
Handover specification for IP delivery



Reference
DTS/LI-00002

Keywords
handover, IP, lawful interception, security

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

Introduction

The objective of the present document is to form the basis for a standardized handover interface for use by both telecommunications service providers and network operators, including Internet Service Providers, that will deliver the interception information required by Law Enforcement Authorities under various European treaties and national regulations.

The present document describes how to handover intercepted information via IP-based networks from a CSP to an LEMF. The present document covers the transportation of traffic, but does not specify functionality within CSPs or LEMF (see clause 4.1). It handles the transportation of intercepted traffic (HI3) and intercept-related information (HI2) but not the tasking and management of Lawful Interception (HI1).

The present document is intended to be general enough to be used in a variety of situations: it is not focussed on a particular IP-based service. The standard therefore provides information that is not dependent on the type of service being intercepted. In particular the present document describes delivery mechanisms (clause 6), and the structure and header details (clause 5) for both HI2 and HI3 information.

1 Scope

The present document specifies the general aspects of HI2 and HI3 interfaces for handover via IP based networks.

The present document:

- specifies the modular approach used for specifying IP based handover interfaces;
- specifies the header(s) to be added to IRI and CC sent over the HI2 and HI3 interfaces respectively;
- specifies protocols for the transfer of IRI and CC across the handover interfaces;
- specifies protocol profiles for the handover interface.

The present document is designed to be used where appropriate in conjunction with other deliverables that define the service-specific IRI data formats (including TS 102 227, TS 101 909-20-2, TS 102 233 [5] and TS 102 234 [6]). Where possible, the present document aligns with TS 133 108 [9] and ES 201 671 [3] and supports the requirements and capabilities defined in TS 101 331 [1] and TR 101 944 [7].

For the handover of intercepted data within GSM/UMTS PS domain, the present document does not override or supersede any specifications or requirements in TS 133 108 [9], ES 201 671 [3] and TS 101 671 [4].

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

[1] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies".

[2] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[3] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

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

[5] ETSI TS 102 233: "Telecommunications security; Lawful Interception (LI); Service specific details for E-mail services".

[6] ETSI TS 102 234: "Telecommunications Security; Lawful Interception (LI); Service-specific details for internet access services".

[7] ETSI TR 101 944: "Telecommunications Security; Lawful Interception (LI); Issues on IP Interception".

[8] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[9] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 5.5.0 Release 5)".

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

[11] ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[12] ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

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

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

[15] IETF RFC 0792: "Internet Control Message Protocol".

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

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

[18] IETF RFC 1323: "TCP Extensions for High Performance".

[19] IETF RFC 1191: "Path MTU discovery".

[20] IETF RFC 2018: "TCP Selective Acknowledgement Options".

[21] IETF RFC 2246: "The TLS Protocol Version 1.0".

[22] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

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

[24] IETF RFC 2821: "Simple Mail Transfer Protocol".

[25] IETF RFC 2822: "Internet Message Format".

[26] IETF RFC 2923: "TCP Problems with Path MTU Discovery".

[27] IETF RFC 2988: "Computing TCP's Retransmission Timer".

[28] IETF RFC 3174: "US Secure Hash Algorithm 1 (SHA1)".

[29] IETF RFC 3268: "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[30] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[31] ISO/IEC TR 10000-1: "Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 671 [4], ES 201 671 [3], ES 201 158 [2], TS 101 331 [1] and the following apply:

Communications Service Provider (CSP): term used to cover those organizations (e.g. Service Providers (SvP), Network Operators (NWO) or Access Providers (AP)) who are obliged by law to provide interception

international standardized profile: internationally agreed-to, harmonized document which describes one or more profiles

profile: set of one or more base standards and/or International Standardized Profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or International Standardized Profiles necessary to accomplish a particular function

Transport Related Information (TRI): information which is sent across a Handover Interface in order to maintain, test or secure the interface. It does not include any CC or IRI

3.2 Abbreviations

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

3GPP	Third Generation Partnership Project
AP	Access Provider
ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
CC	Content of Communication
CID	Communication IDentifier
CIN	Communication Identity Number
CSP	Communications Service Provider
DCC	Delivery Country Code
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
ICMP	Internet Control Message Protocol
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
MD	Mediation Device
MF	Mediation Function (at CSP)
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NID	Network Identifier
NWO	Network Operator
NWO/AP/SvP	Network Operator/Access Provider/Service Provider
PDU	Protocol Data Unit
PS	Packet Switched
RTT	Round Trip Time
SvP	Service Provider
TCP	Transmission Control Protocol
TIPHON	Telecommunication and Internet Protocol Harmonization Over Networks
TLS	Transport Layer Security
TRI	Transport Related Information
UMTS	Universal Mobile Telecommunications System

4 General

4.1 Functionality

Figure 1 shows the stages in the interception chain.

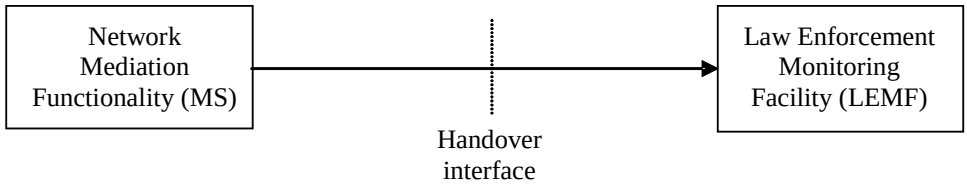


Figure 1: Stages of the interception chain

The first stage includes the creation or separation of intercepted data from the target network or target service, and the creation of IRI data. It is typically the responsibility of the CSP and is outside the scope of the present document.

The second stage ("Handover interface") consists of formatting the results of interception (except where IRI formats are specified in other standards), managing the connection between the CSP Mediation Functionality (MF) and the Law Enforcement Monitoring Facility (LEMF) and transporting the data. It should as far as possible be independent of the other stages and is the joint responsibility of the CSP and the LEA. The present document focuses on the handover interface.

The third stage includes functionality for interpreting and displaying the results of interception. It is typically the responsibility of the LEA and is outside the scope of the present document.

4.2 Intercepted data types

Interception is possible at the following network elements: access element, network connectivity element and service element (as defined in TR 101 944 [7], clause 5.1). Each method is associated with one or more OSI Layer(s) and produces intercepted data in one or more formats, as shown by table 1 (see also TR 101 944 [7] figure 3).

Table 1: Intercepted data types

Component	OSI Layer(s)	Format of intercepted data
Access provider	1 (Physical)	Physical PDUs
	2 (Data link)	Data link PDUs
	3 (Network)	(IP) Datagrams
Network connectivity	3 (Network)	(IP) Datagrams
Service provider	5/7 (Application)	Application layer transactions (but see clause 4.2.2)

The present document covers the handover of data in the following two cases:

- "Network level" interception, consisting of (IP) datagrams from Network Operators or Access Providers.
- "Application level" interception, consisting of application layer transactions from Service Providers.

The present document does not cover the handover of intercepted physical PDUs or data link PDUs (OSI Layer 1 and Layer 2).

NOTE: The application level is also sometimes called the "service level"; the present document always refers to "application level" to avoid confusion over the term service.

4.2.1 Interception at network operator or access provider

The format of the information a NWO/AP/SvP can be expected to deliver is based on the level of *the service it provides*. For example, when a NWO provides Internet Access, at best, the NWO can be expected to provide a copy of the IP packets it transports. Only an E-mail service provider should be asked, for example, to have E-mail information delivered in the format of E-mail.

4.2.2 Interception at service providers

In some circumstances, service providers may find it difficult to intercept target traffic at the application level. Examples of such cases are:

- The application-level transactions are processed by off-the-shelf equipment that the service provider is unable to alter.
- There are security or maintainability issues relating to modifying the application-level code.

In these circumstances the alternative is for the service provider to intercept target traffic at the network level. This alternative is only acceptable subject to circumstances agreed by CSP and LEA.

4.3 Relationship to other standards

The present document describes those parts of the handover interface that are not service-specific i.e. that do not relate to any one service in particular. The following information is not considered to be service-specific, and is included in the present document:

- The framework for data handover.
- The generic header information to be added to HI2 and HI3 traffic.
- The transport protocol for data handover.

In most cases the present document should be used in conjunction with an additional service-specific standard. The service-specific standard fills in the remaining details, including:

- Guidance on how to intercept the service in question.
- When HI2 and HI3 shall be sent and what information it shall contain.
- Any relevant HI1 information.

The following service-specific standards have been designed to be used in conjunction with this one (other standards may also be suitable for use with the present document):

- TS 102 233 [5] "Service-specific details for E-mail".
- TS 102 234 [6] "Service-specific details for Internet Access Services".
- TS 102 227 "Information flow and reference point definitions".
- TS 101 909-20-2 "Services related to non-Voice services".

Figure 2 shows how the standards fit together and what they contain.

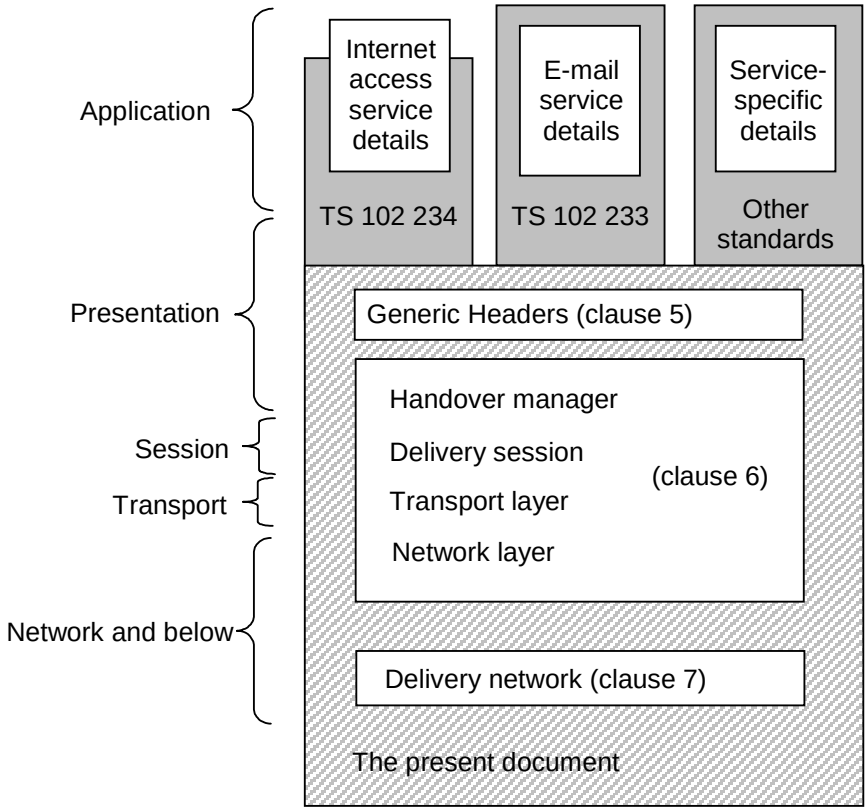


Figure 2: Contents of the present document and its relationship to other standards

4.3.1 Handover for GPRS / UMTS PS

Details for GPRS/UMTS PS are fixed within TS 133 108 [9].

However, it would be a standards compliant LI solution if a LEA, GSM/UMTS PS domain operator and LI solution vendor came to an agreement to deploy HI port definitions laid down in the present document.

5 Headers

5.1 General

All information sent over handover interfaces HI2 and HI3 shall be labelled with certain additional fields to allow the information to be identified, ordered, etc. This additional information will be called the "header" although in practice it could be added elsewhere (e.g. footer) or as part of an overall enveloping process.

Clause 5 is mandatory for HI2 and HI3 information except where stated otherwise.

The header fields are used to meet the following requirements in annex B:

- R4 (LIID);
- R5 and R7 (Communication Identifier);
- R37 and R38 (Timestamp);
- R15 and R19 (Sequence number);
- R10 (Direction);

- R9 (Payload type); and
- R8 (Interception Type).

5.2 Description and purpose of the header fields

5.2.1 Version

The header shall state which version of the handover header is in use. The version shall be set to 1.

NOTE: Some techniques (e.g. ASN.1 with BER) automatically include version numbering as part of the data encoding process. In these cases, it is not necessary to add a version number as a separate field.

5.2.2 LIID

See ES 201 671 [3], clause 6.1.

5.2.3 Authorization country code

The authorization country code states the country within which the authorization was granted. The authorization country code makes the LIID internationally unique. Two-letter codes are used as per ISO 3166-1 [10].

5.2.4 Communication identifier

The communication identifier consists of the Network Identifier (NID), Communications Identity Number (CIN) and Delivery Country Code (DCC).

The CIN is used to identify uniquely the communications session (as defined in TS 101 671 [4]). All the results of interception within a single communications session shall have the same CIN. If a single target identity has two or more communication sessions through the same operator, and through the same network element, then the CIN for each session shall be different. The CIN allows IRI and CC to be accurately associated and is mandatory.

The Network Identifier (NID) consists of the operator identifier and network element identifier (defined in TS 101 671 [4]). The operator identifier identifies the CSP performing the intercept and is mandatory. The network element identifier can be used within a CSP to identify the relevant network element carrying out the LI operations and is optional.

The delivery country code makes the Communication Identifier internationally unique. The delivery country code identifies the geographical location of the Mediation Function. The DCC will be coded according to ISO 3166-1 [10]. The DCC should be used if MF and LEMF are not located in the same country.

5.2.5 Sequence number

The sequence number (as defined in TS 101 671 [4]) counts individual intercepted protocol data units within a communications session of a target identity. This means that the counts are separate for at least:

- different sessions;
- at different network elements;
- for different target identities;
- at different operators.

In other words, counts are separate wherever the communication identifier or the LIID is different.

The sequence number is restarted from zero each time a target begins a new communications session. As a guide, the session starts at the time an IRI-BEGIN message would be sent and ends at the time an IRI-END would be sent. CC associated with a single IRI-REPORT message forms a single communications session in itself. Service-specific standards define when these IRI messages are sent.

The sequence number shall not exceed 2^{32}-1. The sequence number shall wrap to zero after 2^{32} protocol data units have been counted in the session.

The sequence number is required to preserve sequencing over the Handover Interface and to help identify missing data. It is mandatory for all interceptions where sessions can consist of more than one protocol data unit. The sequence number is required in CC and IRI; the counting for IRI messages and CC shall be independent.

5.2.6 Payload timestamp

The timestamp is mandatory for IRI for all services. CC shall also contain a timestamp (exceptions are possible for CC timestamps on a service-by-service basis).

5.2.7 Payload direction

Indicates the direction of the intercepted data (to target or from target). The payload direction is optional for CC but is not required for IRI messages.

5.2.8 Payload type

It is mandatory to know whether the payload is IRI or CC.

The payload type can also be TRI (Transport Related Information) to indicate that the payload contains information relating to the delivery of data or the maintenance of transport connections. TRI data includes Test PDUs (clause 7.3.1), Padding PDUs (clause 6.2.5), "keep-alive" PDUs (clause 6.3.4), Hash PDUs (clause 7.2.3), and First and Last Segment Flag PDUs (clause 6.2.4).

5.2.9 Interception type

It is necessary to know the profile or further standard that was used in intercepting and formatting the data. Clause 4.3 contains an explanation of additional standards that can be used in conjunction with this one. The list of valid interception types is given in annex A.

5.2.10 IRI Type

The IRI type states whether a piece of IRI is a BEGIN, CONTINUE, END or REPORT message (see ES 201 671 [3]). The IRI-Type shall not be present unless the contents of the PDU is IRI. The IRI-Type is MANDATORY for IRI messages except when the IRI contents contains an explicit statement of the type of the IRI record.

5.3 Encoding of header fields

The transferred information shall conform to the Abstract Syntax Notation One (ASN.1) specification in annex A (as per ITU-T Recommendation X.680 [11]).

The transferred messages are encoded to be binary compatible with the Basic Encoding Rules (BER) as per ITU-T Recommendation X.690 [12]. For more details see also TS 133 108 [9], clause B.1.

6 Data exchange

6.1 Introduction

Figure 3 shows the protocol stack that is maintained at the CSP and LEA.

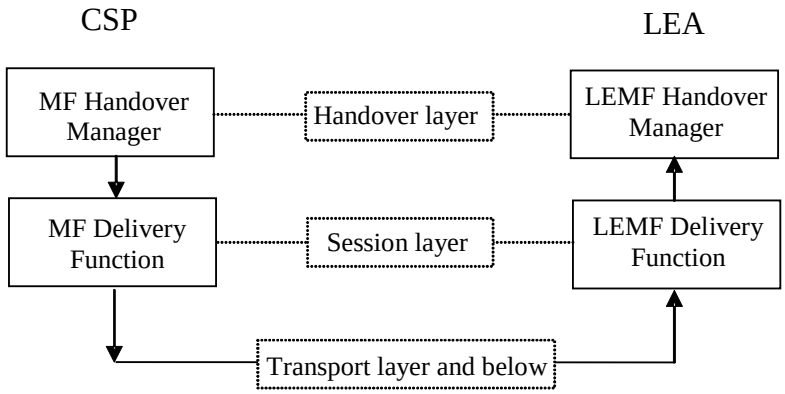


Figure 3: Protocol stack

The responsibilities of each layer are shown in table 2. The functionality provided by each box is described in clauses 6.2 to 6.5.

Table 2: Responsibilities of each layer

Layer name	OSI Layer	Clause	Responsibilities
Handover	6 and 7	6.2	Create and maintain one or more delivery functions. It is also responsible for error reporting. Also: • Aggregate PDUs • Associate header information • Create padding PDUs • Assign PDUs to Delivery Function(s)
Session	5	6.3	Create and maintain a single transport connection and monitor its status. Also: • Perform the "keep-alive" mechanism • Encode/decode PDU elements • Perform integrity mechanism • Buffer data
Transport	4	6.4	Create and maintain a network connection
Network	3	6.5	Network protocol

6.2 Handover layer

6.2.1 General

The task of the Handover Manager is to handover intercepted data of all running intercepts to the appropriate destination(s). In order to do so, the Handover Manager creates one Delivery Function (see clause 6.3) for each of the destinations.

NOTE: The CSP would typically create one Delivery Function for each LEMF. As a national option it is also acceptable to have multiple destinations (called "LEMF-Gateways") associated with one LEMF. In this case, the CSP creates a Delivery Function for each LEMF-Gateway. If LEMF-Gateways are used, the MF Handover Manager is responsible for distributing the PDUs to the appropriate Gateway. Possible techniques for PDU distribution include (but are not limited to) the following:

(i) distribute PDUs randomly across all available Gateways;

(ii) select a Gateway for the PDU on the basis of its LIID.

The choice of technique used for PDU distribution is outside the scope of the present document.

The Handover Manager is responsible for error reporting (see clause 6.2.2).

The Handover Manager performs the following operations (in order moving down the protocol stack):

- Aggregate or segment/reassemble payloads if required (see clauses 6.2.3 and 6.2.4).
- Associate header information (see clause 5.2).
- Create padding PDUs if required (see clause 6.2.5).
- Assign PDUs to a Delivery Function (see note above).

6.2.2 Error reporting

The MF Handover Manager shall collect error reports from the lower layers at the CSP. It shall report errors to the LEMF Handover Manager according to agreements between the CSP and LEA.

The LEMF Handover Manager shall collect error reports from the lower layers at the LEA.

6.2.3 Aggregation of payloads

It may be beneficial to aggregate a number of payloads to be transported within one larger unit (Protocol Data Unit or PDU). The advantage is a saving in bandwidth (one PDU header covers a number of payloads). The main disadvantage is that some payloads are delayed while waiting for the aggregation to take place; additionally there is extra processing overhead. Payload aggregation may be used if agreed by the CSP and LEA. If payload aggregation is used, it shall be implemented as follows.

To aggregate payloads, they may only have different timestamps, directions (for CC payloads) or IRI-types (for IRI payloads). Payloads may not be aggregated if their associated information differs in other ways (e.g. different LIID, or different operator). One aggregated PDU then has a single sequence number (i.e. aggregated payloads are not assigned individual sequence numbers). The order of packets in the aggregated PDU shall be in the same sequence as they arrived at the Handover Manager. It is acceptable either to assign one timestamp to the whole PDU (in the PDU header) or, if more detailed timestamp information is required, then one timestamp shall be assigned to each payload as indicated in annex A.

The implementation of aggregation (i.e. when aggregation is applied and how many packets can be aggregated together) shall be subject to the agreement of CSP and LEA to meet national requirements.

6.2.4 Sending a large block of application-level data

When a large self-contained block of application-level data has to be transferred over the HI, in order not to choke the connection to the LEMF for a prolonged period of time, the data should be divided over multiple PDUs.

If segmentation is applied, the application-level data is divided into smaller segments and each segment is sent as CC-payload with its own set of header-fields, where, as for regular PDUs, the sequence number increments for each PDU being sent.

At transfer of the first PDU containing a segment of the application-data, the DF must sent a TRI of the type "FirstSegmentFlag", containing a header with a communication identifier, an authorization country code, an LIID and a sequence number identical to the of the first data PDU being sent. Timestamp should not be present.

After sending the last segment of the application-data the DF must sent a TRI of the type "LastSegmentFlag", containing a header with a communication identifier, an authorization country code, an LIID and a sequence number identical to that of the last data PDU being sent. Timestamp should not be present.

NOTE: The header values of the two TRIs (the sequence numbers in particular) will allow the LEMF to reassemble the segmented data.

6.2.5 Padding data

By agreement, it is permitted to transfer "padding" data over the Handover Interface. The purpose of padding data is to change the data flow rate to prevent analysis of patterns in data flows. If required, padding data shall be created at the MF Handover Manager and shall be removed by the LEMF Handover Manager. The padding data shall be sent as Transport-Related Information of type Padding-PDU (see annex A for details). The PDU shall have correct Object ID, Operator ID and (optionally) Network Element ID but all other fields shall contain any value. There is no constraint on the payload contents, although a Padding-PDU shall not be used to carry meaningful data.

6.3 Session layer

6.3.1 General

The Delivery Function is responsible for maintaining a single transport connection as described in clause 6.3.2. The transport connection can be a TCP socket, a TLS RFC 2246 [21] session or other transport connection. When using TLS, a TCP socket is opened by TLS. TCP details are given in clause 6.4; the specification for other transport connections is outside the scope of the present document.

The Delivery Function performs the following operations (in order moving down the protocol stack):

- Perform the "keep-alive" mechanism if required (see clause 6.3.4).
- Encode/decode PDU elements (see clause 5.3).
- Perform integrity mechanism if required (see clause 7.2.3).
- Buffer data (see clause 6.3.3).

6.3.2 Opening and closing connections

When it is created, the MF Delivery Function shall immediately attempt to open a transport connection. It is acceptable for the MF or LEMF Delivery Function to terminate the transport connection if they require. If the transport connection terminates for any reason, the MF Delivery Function shall immediately attempt to reopen it.

If the attempt to open a connection is not successful, the MF Delivery Function shall continue to attempt to open the transport connection with a configurable time interval (e.g. 30 s) between attempts (i.e. between the indication of failure of the previous attempt and initiation of new attempt). Failure to open a transport connection shall be reported to the MF Handover Manager.

NOTE: Under some circumstances (e.g. if there are extended periods with no data to be sent and there are costs associated with maintaining a transport connection) it is also acceptable to operate the transport connection on an "as required" basis. This means that if the transport connection was closed down by the MF or LEMF in a controlled and error-free manner, it should not be re-opened until there is further data to be transported. If "keep-alives" are still required while the connection is still closed, the connection should be re-established.

6.3.3 Buffering

It is required that no data is lost due to unexpected termination of the transport connection and that no traffic is dropped during very short system outages. Therefore the MF Delivery Function shall be able to buffer traffic for short periods. In order to do so, each Delivery Function keeps a *cyclic buffer*. When a PDU is received by the Delivery Function, if a transport connection is open, the PDU is sent to the open connection. If the PDU is not a "keep-alive", it will also been written to the cyclic buffer. The transport connection returns information on how much data it successfully sent and, using the FIFO principle, the Delivery Function deletes the PDUs from the buffer that fit into that amount of data. The Delivery Function will only accept PDUs for transport if there is room for them in the cyclic buffer. If the buffer becomes full, the Delivery Function reports this to the Handover Manager; the Delivery Function then discards data by overwriting the oldest data in the buffer.

NOTE 1: If TCP is used, the cyclic buffer size shall minimally be that of the TCP send buffer and shall cover the time it takes to re-start a TCP connection.

Whenever a transport connection is re-opened, once the transport connection is re-established, the MF Delivery Function will r*esynchronize the data* by re-sending the PDUs that are still stored in the cyclic buffer before any new data is transferred.

NOTE 2: Since it is uncertain whether the data in the buffer was delivered or not, the LEMF shall be able to deal with duplicate delivery of PDUs.

Buffering to cover longer outages is outside the scope of the present document.

6.3.4 Keep-alives

To meet requirement R16 (see annex B) it is recommended to use session-layer "keep-alives". If used, "keep-alives" shall be implemented as described in this clause.

The MF Delivery Function starts a timer when the connection is established, and is reset whenever data is sent. When the timer reaches TIME1, the MF Delivery Function shall send a "keep-alive" message. It is acceptable for the "keep-alive" message to be sent before TIME1 if required. The LEMF Delivery Function shall respond to this "keep-alive" message within TIME2. If the MF does not receive a response in TIME3, the MF shall terminate the connection at the Transport Layer and attempt to establish a new one.

NOTE: The CSP and the LEA should agree on values for TIME1, 2 and 3. A typical value for TIME1 would range from 120 s to 360 s. A typical value for TIME2 would be 30 s. The value for TIME3 should be long enough to allow for the transport connection to recover from transient failures (e.g. to cover TCP retransmissions including exponential back-off). A typical value for TIME3 would be 60 s. Note that TIME3 will need to be larger than TIME2.

The "keep-alive" message is sent as Transport-Related Information of type "keep-alive" (see annex A for details). The sequence number increments for each "keep-alive" sent within the same instance of the Delivery Function. The timestamp and domain ID shall be set appropriately. All other header fields shall be filled in with any value. The "keep-alive" response message is sent as TRI, of type "keep-alive" Response. The sequence number of the response is the sequence number of the "keep-alive" PDU that generated the response. The timestamp shall be updated to the appropriate value by the LEMF Delivery Function. All other header fields shall be filled in with any value.

6.4 Transport layer

6.4.1 Introduction

Clause 6.4 describes a transport layer that is based on the Transport Control Protocol. TCP is implemented according to RFC 0793 [16], RFC 2581 [23], RFC 2988 [27] and clause 4.2 of RFC 1122 [17]. The MF is the TCP sender and the LEMF is the TCP receiver.

6.4.2 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 CSP. The allocation of the destination port number is outside the scope of the present document.

TCP "keep-alive" (RFC 1122 [17]) should not be used. If "keep-alives" are required, they should be sent at the session layer (see clause 6.3.4).

NOTE: Annex C provides further guidance on setting up and tuning TCP.

6.4.3 Acknowledging data

The Delivery Function shall be informed when data has been successfully sent. One of the following three options shall be chosen:

1) Data is considered to be successfully sent once TCP-acknowledgements have been received.

2) Data is considered to be successfully sent once a further N kB of data has passed through the TCP socket (where N is the size of the TCP send buffer).

3) Data is considered to be successfully sent as soon as it is passed to an open TCP socket.

Under option 3 some data may be lost during network outages; option 3 is only acceptable subject to the agreement of the CSP and LEA.

6.5 Network layer

The Network layer implements the Internet Protocol according to RFC 0791 [14].

7 Delivery networks

7.1 Types of network

7.1.1 General

The network used for data exchange influences how the handover requirements from annex B should be met. The choice of the network will be made on a national basis for legal and pragmatic reasons.

This clause orders the networks in three generic categories to consider their influence on the implementation of the requirements in the data exchange.

7.1.2 Private networks

The first category of networks, private networks, are dedicated for one task (or a limited set of tasks) only. The access control is limited to the involved LEA and CSP.

Accidental access to content or access points by third parties is possible by static configuration failures. It is possible but very unlikely. Active access by third parties is possible by brute force or physical intrusion.

A typical example of a Private Network is lease lines.

7.1.3 Public networks with strict control

This second category of networks is public networks under strong control of the CSP offering this network service.

The network facilities give rather strong protection against access to content or access points by third parties. Accidental access is possible due to configuration or addressing mistakes. The opportunities for active access by third parties depend mainly on the order of management and reliability of the network (back doors) or brute force.

A typical example of a public network with strict control is the public X.25 network.

7.1.4 Public networks with loose control

The third category of networks is public networks with very little control by the CSP offering the network as to who communicates with whom.

The network provides open communication between endpoints with very loose control over access to the network. This provides little inherent protection from access to an endpoint by any other endpoint.

A typical example of a public network with loose control is the Internet.

7.2 Security requirements

7.2.1 General

In annex B, requirements are identified for Confidentiality, Authentication and Integrity. These requirements can be met by use of a private, managed delivery mechanism (clause 7.1.2). However, if the underlying mechanism is based on a public network (clauses 7.1.3 and 7.1.4), then further security mechanisms are strongly recommended.

The requirements for Confidentiality, Authentication and Handover Integrity can be met by using a VPN application. VPN applications provide secure, network-to-network, host-to-network, or host-to-host tunnels - virtual point-to-point connections. The technical details for the VPN applications including IPSec are outside the scope of the present document.

Alternatively the requirements for Confidentiality, Authentication and Integrity can be addressed as described in clauses 7.2.2 and 7.2.3.

7.2.2 Confidentiality and authentication

To support the requirement for confidentiality (requirement R26) and authentication (requirement R28), the recommended technology is to use TLS RFC 2246 [21]. TLS is applied at the Transport Layer, instead of opening a TCP socket (clause 6.4.2), a TLS session is opened. The TLS session opens its own, single TCP socket.

Encryption should be based on either TLS_RSA_WITH_RC4_128_SHA or TLS_RSA_WITH_AES_256_CBC_SHA RFC 3268 [29].

X.509 certificates RFC 3280 [30] should be used for authentication as described in RFC 2246 [21], clauses A.4.2 and A.4.3.

7.2.3 Integrity

In order to allow the authorities to verify the integrity of the received data, periodically, hashes over the data PDUs may be inserted into the HI3 data stream. The use of integrity checks is configurable over HI1, but should be used when the collected data is planned for evidential purposes. The hash shall not include any TRI data. A hash will only be created if at least one PDU packet was sent since startup or since the previous hash was created.

A SHA-1 hash (see RFC 3174 [28]) is generated:

- for every <predefined number of> PDU packets; or
- when <predefined number of> seconds have passed; or
- when the intercept on the target is terminated.

The SHA-1 Hash is calculated over the PDU packets sent since startup or since the last SHA-1 hash was sent. All the PDUs within the hash shall have the same LIID and CID (e.g. PDUs with different LIIDs cannot be combined within the same PDU hash) as the sequence number is only unique within the same CID. Separate hashes shall be maintained for HI2 and HI3. SHA-1 hashes are computed over the PS-PDU structure including header and contents. The SHA-1 hash is sent as Transport-Related Information in an IntegrityCheck PDU (see annex A), where the checkType is set to 1 and the dataType indicates whether the hash contains IRI or CC. The array IncludedSequenceNumbers contains the sequence number of every data PDU that was included in the hash. The LIID and Communications Identifier shall be set correctly. The timestamp should be present. The sequence number increments for every hash sent for this intercept (i.e. counts the number of hashes sent with the same LIID and Communications Identifier; hashes of IRI and CC data shall increment the *same* counter).

NOTE 1: Note that the LEA must wait for the hash to be able to integrity check the data. If due to link failure, the hash PDU is not transmitted, some data may be impossible to validate. Decreasing the number of packets and the timeout of the hash can reduce the risk, but that will have a performance impact on the interception equipment.

Periodically, a digital signature will be inserted into the HI3 data stream that allows the authorities to verify the authenticity and integrity of the received SHA-1 hashes for a particular CIN and to prove (with hindsight) that the data originated from the sender. If evidential quality of the intercepted data was ever challenged, the digital signatures can be used to prove the authenticity of the hashes and the hashes to proof the integrity of the data.

A DSS/DSA Signature FIPS PUB 186 [13] is created:

- for every <predefined number of> Integrity packets; or
- when <predefined number of> seconds have passed; or
- when the intercept on the target is terminated.

The digital signature is calculated with DSS/DSA from a SHA-1 hash over the combined SHA-1 integrity hashes that were created since startup or since the previous signature was sent. The digital signature is sent as Transport Related Information in an IntegrityCheck PDU (see annex A), where the checkType is set to 2 and the dataType field is not present. The array IncludedSequenceNumbers contains the sequence number of every hash PDU that was included in the hash that was signed. The LIID and Communications Identifier shall be set correctly. The timestamp should be present. The sequence number increments for every digital signature sent for this intercept (i.e. counts the number of digital signatures sent with this LIID and Communications Identifier).

NOTE 2: Note that the LEA must wait for the hash and signature PDUs to be able to authenticate and integrity check the data. If due to link failure, the hash and/or signature PDUs are not transmitted some data may be impossible to validate. Decreasing the number of packets and the timeout of the hash and signatures can reduce the risk, but that will have a performance impact on the interception equipment.

NOTE 3: The distribution of the DSS/DSA public key is outside the scope of the present document.

7.3 Further delivery requirements

7.3.1 Test data

To meet requirement R17, the network and/or the data exchange mechanisms shall have the possibility to transfer Test-PDUs. Test data should be sent end-to-end (from the CSP interception point to the LEA data viewing point) where possible. The test PDUs should be transferred at the activation of the intercept and may be transferred at other times.

The Test-PDU is sent as Transport Related Information (TRI) (see annex A for details). Appropriate values shall be filled in for LIID, Country Code, Communications Identifier and Timestamp. Sequence number shall be set to zero.

7.3.2 Timeliness

The timeliness requirement is that the results of interception are not delayed unnecessarily (R14), with no requirement to preserve the real-time nature of CC in LI delivery. Under normal conditions, all the network types in clause 6.2 will meet this timeliness requirement when using the delivery mechanism in clause 7.

NOTE: Under conditions of heavy loading the performance of TCP can degrade. The LEA and CSP should consider transporting the time-critical traffic on a separate, managed network. The network should have sufficient bandwidth and should meet suitable performance criteria.

Annex A (normative): ASN.1 syntax trees

A.1 ASN.1 syntax tree for HI2 and HI3 headers

Figure A.1 shows the object identifier tree from the point of view of packet-switched lawful interception.

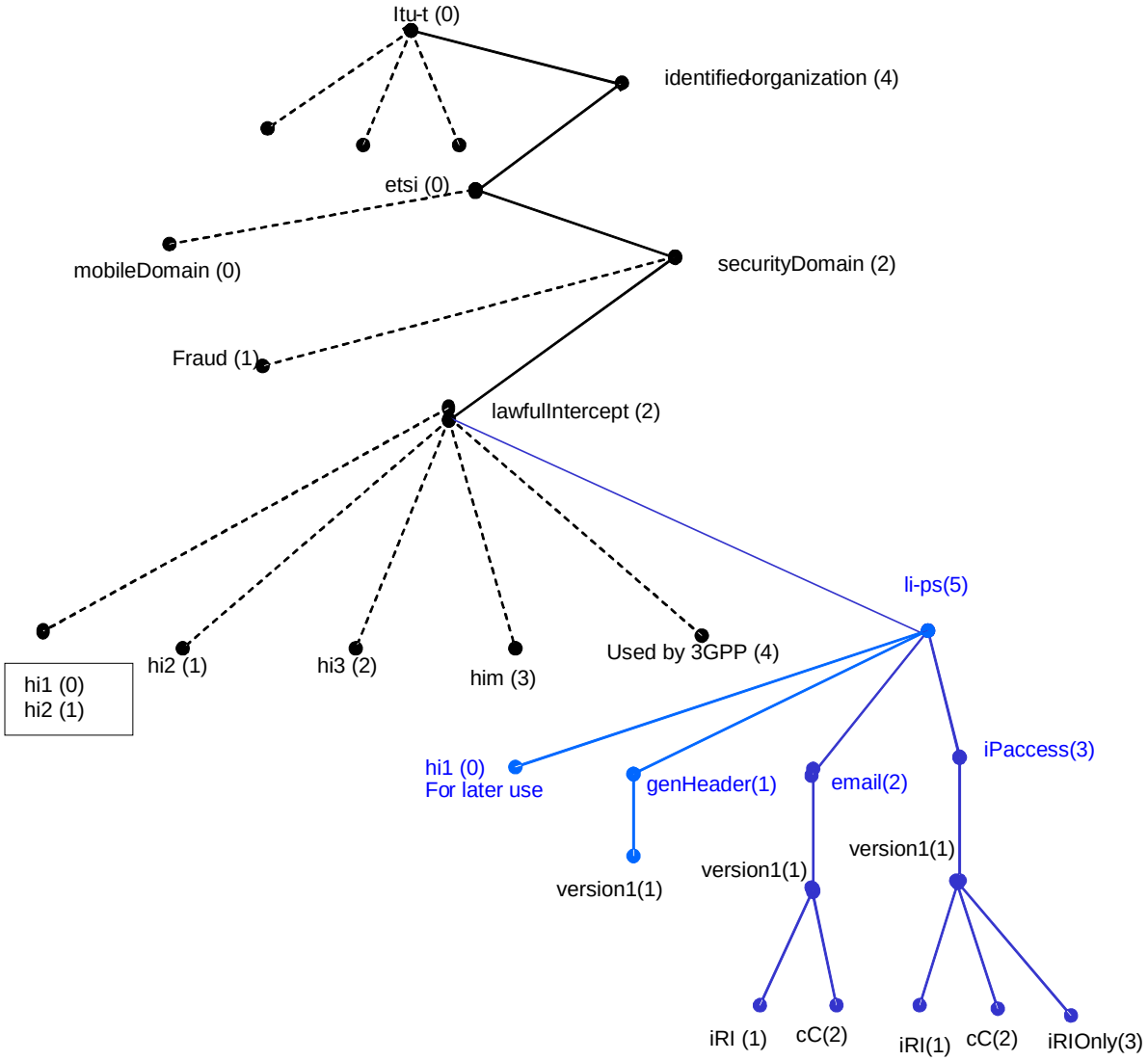


Figure A.1: Object identifier tree

A.2 ASN.1 specification

The ASN.1 (ITU-T Recommendation X.680 [11]) module that represents the information in the present document and meets all stated requirements is shown below:

```
LI-PS-PDU {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
genHeader(1) version1(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS
    -- Any of the IMPORTs may be commented out if they are not used (see clause A.3)

    -- From ETSI HI2Operations TS 101 671
    LawfulInterceptionIdentifier, IRI-Parameters, IRIsContent
        FROM HI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version4(4)}

    -- from ETSI TS 102 233
    EmailIRI, EmailCC
        FROM EmailPDU
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
email(2) version1(1)}

    -- from ETSI TS 102 234
    IPIRI, IPCC, IPIRIOnly
        FROM IPAccessPDU
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
iPAccess(3) version1(1)}

    -- from ETSI TS 133 108
    IRI-Parameters, UmtsIRIsContent
        FROM UmtsHI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2(1) version-2(2)};

    -- end of IMPORTS

--================================--
-- Object Identifier Definitions --
--================================--

lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

li-psDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId li-ps(5) genHeader(1) version1(1)}

--======================--
-- Top-level definition --
--======================--

PS-PDU          ::= SEQUENCE
{
    pSHeader    [1] PSHeader,
    payload     [2] Payload
}

PSHeader        ::= SEQUENCE
{
    li-psDomainId                   [0] OBJECT IDENTIFIER,
    lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
    authorizationCountryCode        [2] PrintableString (SIZE (2)) OPTIONAL,
        -- see clause 5.2.3
    communicationIdentifier         [3] CommunicationIdentifier,
    sequenceNumber                  [4] INTEGER (0..4294967295),
    timeStamp                       [5] GeneralizedTime OPTIONAL,
        -- see clause 5.2.6
    ...
}
```

```
Payload ::= CHOICE
{
    iRIPayloadSequence      [0] SEQUENCE OF IRIPayload,
    cCPayloadSequence       [1] SEQUENCE OF CCPayload,
        -- Clause 6.2.3 explains how to include more than one payload in the same PDU
    tRIPayload              [2] TRIPayload,
    ...
}
```

```
--=====================================--
-- Items contained within the PS-Header --
--=====================================--
```

```
CommunicationIdentifier     ::= SEQUENCE
{
    networkIdentifier               [0] NetworkIdentifier,
    communicationIdentityNumber     [1] INTEGER (0..65535),
    deliveryCountryCode             [2] PrintableString (SIZE (2)) OPTIONAL,
         -- see clause 5.2.4,
    ...
}
```

```
NetworkIdentifier   ::= SEQUENCE
{
    operatorIdentifier          [0] OCTET STRING (SIZE(1..16)),
    networkElementIdentifier    [1] OCTET STRING (SIZE(1..16)) OPTIONAL,
    ...
}
```

```
--============================--
-- Definitions for CC Payload --
--============================--
```

```
CCPayload   ::= SEQUENCE
{
    payloadDirection    [0] PayloadDirection OPTIONAL,
    timeStamp           [1] GeneralizedTime OPTIONAL,
        -- For aggregated payloads (see clause 6.2.3)
    cCContents          [2] CCContents,
    ...
}
```

```
PayloadDirection ::= ENUMERATED
{
    fromTarget      (0),
    toTarget        (1),
    ...
}
```

```
CCContents ::= CHOICE
    -- Any of these choices may be commented out if they are not being used, see clause A.3
{
    undefinedCC     [0] OCTET STRING,
    emailCC         [1] EmailCC,
    iPCC            [2] IPCC,
    uMTSCC          [4] OCTET STRING,
    eTSI671CC       [5] OCTET STRING,
    ...
}
```

```
--============================--
-- Definitions for IRI Payload --
--============================--
```

```
IRIPayload ::= SEQUENCE
{
    iRIType         [0] IRIType OPTIONAL,
        -- See clause 5.2.10
    timeStamp       [1] GeneralizedTime OPTIONAL,
        -- For aggregated payloads (see clause 6.2.3)
    iRIContents     [2] IRIContents,
    ...
}
```

```
IRIType     ::= ENUMERATED
{
    iRI-Begin       (1),
    iRI-End         (2),
    iRI-Continue    (3),
    iRI-Report      (4)
}
```

```
IRIContents     ::= CHOICE
    -- Any of these choices may be commented out if they are not being used (see clause A.3)
{
    undefinedIRI    [0] OCTET STRING,
    emailIRI        [1] EmailIRI,
    iPIRI           [2] IPIRI,
    iPIRIOnly       [3] IPIRIOnly,
    uMTSIRI         [4] UMTSIRI,
    eTSI671IRI      [5] ETSI671IRI,
    ...
}
```

```
UMTSIRI         ::= CHOICE
    -- This structure may be commented out if not used
{
    iRI-Parameters  [0] UmtsHI2Operations.IRI-Parameters,
    umtsIRIsContent [1] UmtsIRIsContent,
    ...
}
```

```
ETSI671IRI      ::= CHOICE
    -- This structure may be commented out if not used
{
    iRI-Parameters  [0] HI2Operations.IRI-Parameters,
    iRIsContent     [1] IRIsContent,
    ...
}
```

```
--==============================--
-- Definitions for TRI Payload --
--==============================--
```

```
TRIPayload      ::= CHOICE
{
    integrityCheck      [0] IntegrityCheck,
    testPDU             [1] NULL,
    paddingPDU          [2] OCTET STRING,
        -- Undefined contents (will be discarded)
    keep-alive          [3] NULL,
    keep-aliveResponse  [4] NULL,
    firstSegmentFlag    [5] NULL,
    lastSegmentFlag     [6] NULL,
    ...
}
```

```
IntegrityCheck      ::= SEQUENCE
{
    includedSequenceNumbers [0] SEQUENCE OF INTEGER (0..4294967295),
        -- gives the order the PDUs were processed
    checkType               [1] CheckType,
    dataType                [2] DataType OPTIONAL,
        -- Required for hashes, not present for signatures (see clause 7.2.3)
    checkValue              [3] OCTET STRING (SIZE (20)),
        -- Network byte order
    ...
}
```

```
CheckType   ::= ENUMERATED
{
    hash        (1),
        -- SHA-1 hash value
    signature   (2),
        -- DSS/DSA signature
    ...
}
```

```
DataType    ::= ENUMERATED
{
    iRI     (1),
    cC      (2),
    ...
}

END     -- of LI-PS-PDU
```

A.3 Importing parameters from other standards

The present document is designed to transport CC and IRI from a range of different services. Consequently, it imports CC and IRI structures from a number of other standards. If only one service is being used, it might be inconvenient to import CC and IRI structures from all of the other service-specific standards. It is acceptable to comment out (i.e. add "--" to the start of the corresponding lines) any IMPORTS statements that are not being used. The corresponding alternatives of the CHOICEs within IRI Payload and CC Payload structures should then also be commented out.

Annex B (informative): Requirements

B.1 Types of intercepted information

R1) The interface shall be able to handover communications content in the form of:

- one or more datagrams (as per RFC 0791 [14] or RFC 2460 [22]);
- one or more application level PDUs (e.g. messages conforming to RFC 2821 [24] or RFC 2822 [25]).

R2) The interface shall be able to handover:

- intercept-related information associated with the CC noted above;
- intercept-related information which is not associated with CC (i.e. the interface should support IRI-only interception; see ES 201 671 [3], clause 7.1.4).

R3) The handover interface shall be flexible and extensible.

B.2 Identification of traffic

R4) The results of interception shall be (internationally) uniquely associated with a target identity (ES 201 671 [3], clause 6.1, TS 101 331 [1], clauses 4.2.f and 4.10, f)). For security reasons, it shall be possible to make this association without explicitly adding the target identity to the results of interception.

R5) When IRI relates to CC, then such IRI shall be associated with the relevant CC (TS 101 331 [1], clause 4.10, g), ES 201 158 [2], clause 5.6).

R6) It shall be possible to distinguish between multiple communications from the same target identity (ES 201 671 [3], clause 6.2). This includes the following cases:

- two communications sessions which overlap in time (e.g. target is logged on twice to an internet access provider);
- two "single-shot" communications occurring almost simultaneously (e.g. target receives two e-mails within a very short space of time).

R7) The parties involved in the exchange of information (CSP and LEMF) can be identified uniquely on an international basis (ES 201 158 [2], clause 4.3.1).

R8) The handover interface shall contain a parameter indicating the service being intercepted.

R9) IRI and CC shall be differentiated.

R10) The handover interface shall indicate whether intercepted CC was travelling to or from the target (or that the direction was indeterminate).

B.3 Performance

R11) The HI2 delivery mechanism will support an appropriate minimum sustained traffic rate.

R12) The HI3 delivery mechanism will support an appropriate minimum sustained traffic rate.

R13) The handover interface shall accommodate multiple LEMFs (ES 201 158 [2], clause A.2).

B.4 Timeliness

R14) The handover interface shall not delay the results of interception unnecessarily (for more details see ES 201 671 [3], clauses 8 and 10.1, TS 101 331 [1], clause 4.5, d), ES 201 158 [2], clause 5.4).

NOTE: There is no requirement to preserve the real-time nature of CC in LI delivery such as that required by interactive multimedia applications (e.g. see TS 123 107). Priority is given to the reliable delivery of data.

R15) The handover interface shall support the preservation of the sequencing of the PDUs.

B.5 Reliability and availability

R16) CSP and LEMF shall be able to detect when the transfer of IRI or CC is unavailable (TS 101 671 [4], clause D.4) and shall provide fault reports (ES 201 158 [2], clause 7.2).

R17) It should be possible to test the correct operation of the lawful interception functionality and HI (ES 201 158 [2], clause 5.7).

R18) The interface shall be reliable (TS 101 331 [1], clause 4.2, b), 3), TR 101 944 [7], clause 8.2).

R19) Under normal operating conditions, each and every PDU shall be transferred unaltered across the interface.

R20) The protocols adopted shall be resilient to transmission impairment.

B.6 Discarding information

R21) IRI shall not be discarded during transport mechanism outages for a negotiated period (see also ES 201 158 [2], clause 5.4, TS 101 331 [1], clause 4.2, b), 3).

R22) Order of discarding information: all HI3 information should be dropped before discarding any HI2.

R23) For connection-oriented protocols, CC shall be buffered to cover transient link failure, subject to capacity and security limitations (e.g. there shall be CC buffering to cover the time it takes to establish a connection).

R24) CC shall be buffered to cover longer link failures if required nationally (TS 101 331 [1], clause 4.2, b), 4)).

R25) The HI2 and HI3 (logical) link must have the ability to consist of one or more paths/routes if required nationally.

B.7 Security

NOTE: Security at CSP and LEMF (e.g. of security clearance of CSPs own staff, physical security at LEMF, etc) is outside scope of the present document. A full security analysis (e.g. threat model) is beyond the scope of the present document.

R26) The handover interface shall support confidentiality (ETR 232 [8], TR 101 944 [7], clauses 7.1 and 8.2, TS 101 331 [1], clause 4.7, j)).

R27) The handover interface shall support measures to prove the integrity of transported data. It shall be possible to incorporate techniques that identify if data has been added, removed or altered (ETR 232 [8], TS 101 331 [1], clauses 4.2, b), 3) and 4.2, b), 4)).

R28) The interface shall support the establishment of the communicating identities in each direction (TS 101 331 [1], clauses 4.7, g), 4.7, h) and 4.7, i), ES 201 158 [2], clause 8.3, TR 101 944 [7], clause 7.1).

R29) Nothing within the handover interface should compromise national security.

B.8 Other

R30) The interface shall be based upon open, standardized and widely-used data communication protocols and coding principles (ES 201 671 [3], clauses 5.2 and 8.1).

R31) The interface shall support the use of generally-available transmission paths (TS 101 331 [1], clauses 4.10, e) and 4.10, h)).

R32) The interface shall be designed to be low in cost (for specification, design, implementation, verification and testing, configuration and adaptation at CSP and LEA).

R33) The standard should contain a minimum of choices and options.

R34) The standard should use all applicable details from ES 201 671 [3].

R35) The interface should be capable of ready adaptation to national requirements (TS 101 331 [1], clause 4.1, ES 201 158 [2], clause 4.2).

R36) The interface should support the delivery of the result of interception between an operator's technical facility in one country and an LEMF in another.

R37) All IRI shall contain a timestamp (ES 201 671 [3], clause 8).

R38) CC shall in general contain timestamps; exceptions are possible on service-by-service basis.

R39) The interface should do nothing to prejudice the introduction of the result of interception passed across it as evidence in a court of law.

R40) The interface should be able to support any necessary mechanisms that may be required to support the introduction of the result of interception passed across it as evidence in a court of law.

Annex C (informative): Notes on TCP tuning

C.1 Implement RFC 2581

It is recommended to deploy a TCP stack, both at the sending and receiving end of the connection, that implements RFC 2581 [23]. This RFC defines, amongst others, "fast retransmit" and "fast recovery" options, which greatly improve performance in case of packet-loss or network congestion.

C.2 Minimize roundtrip times

It is recommended to optimize the network connection between MF and the LEMF especially in terms of roundtrip time. The TCP Roundtrip Time (RTT) is the elapsed time between sending a data octet with a particular sequence number and receiving an acknowledgement that covers that sequence number, i.e. in every RTT, data of the size of the window size can be transported. Thus, with a window size of 64 K and a RTT of 20 ms, the throughput is about 3,28 Mbit/s (or 26 Mbit/s).

C.3 Enable maximum segment size option

It is recommended to deploy a TCP stack, both at the sending and receiving end of the connection, that supports the Maximum Segment Size (MSS) option and follows the usage defined in clause 4.2.2.6 of RFC 1122 [17]. This allows the receiver to announce the maximum size of the TCP data segments it can receive. If the receiver is connected using Ethernet, and the underlying IP layer allows for it, the announced Segment size will typically be 1 460 bytes. If the MSS is not announced, the sender reverts to the default segment size of 536 bytes (the default IP datagram size of 576 bytes - 40 bytes for IP and TCP header).

C.4 Path MTU discovery

The MF may utilize Path MTU Discovery RFC 1191 [19]. This allows the MF to discover the largest possible packet size for the session. The issues discussed in RFC 2923 [26] should be taken into account if Path MTU Discovery is used.

For Path MTU Discovery to work, all network equipment in the path between the MF and the LEMF must be able to forward and/or generate Internet Control Message Protocol (ICMP) RFC 0792 [15] "too big" packets. If this is not the case, the MF must be able to function without Path MTU Discovery.

NOTE: Internet Control Message Protocol packets are often blocked on firewalls for security reasons.

C.5 Selective acknowledgement

It is recommended to utilize TCP SACK RFC 2018 [20] to improve the efficiency of TCP in the face of congestion and for high bandwidth links.

C.6 High speed options

If the link between the MF and LEMF has a high bandwidth × delay product, the MF and LEMF may utilize the Large Windows option defined in RFC 1323 [18].

C.7 PUSH flag

If the application uses the PUSH flag, it should follow the recommendations in clause 4.2.2.2 of RFC 1122 [17].

C.8 Nagle's algorithm

To reduce the transmission delay experienced by small packets, it is recommended to turn off Nagle's algorithm.

NOTE: The TCP socket option named TCP_NODELAY is provided for enabling or disabling Nagle's algorithm. This Boolean option is set to TRUE to disable Nagle's algorithm.

C.9 Buffer size

It is recommended to configure TCP, on both the MF and LEMF, with a send/receive buffer size that is at least the bandwidth × delay product of the link. The window size used by TCP will typically equal the size of the receive buffer. In case of overrun of the receiving party, sender and receiver will autonomously negotiate a smaller window. The Large Windows option in RFC 1323 [18] shall be used if a window size larger than 64 K/bytes is to be used. On the other hand, if a low bandwidth link is being used between the MF and LEMF (e.g. dial-up modem), reducing the receive buffer (e.g. to 8 K) can increase the efficiency and decrease the latency in the connection.

Annex D (informative): IRI-only interception

D.1 Introduction

In certain countries it is easier to obtain lawful authorizations for HI2-only intercepts in other situations these lawful authorizations are considered for proportionality. If lawful authorizations allow only HI2 traffic, then the precise definitions of HI2 and HI3 are clearly important.

This annex focuses on IP as target service (not E-mail, etc.).

D.2 Definition HI information

As an example of one country operating under this system the following definitions are used:

IRI: Dialling, signalling or addressing information that identifies the origin, direction, destination or termination of each communication generated or received by the subscriber by means of any equipment, facility or service of a service provider. This includes, but is not limited to, parameters of the signalling information that can be used as a means to subscribe to or activate features of the service, or establish and control a communication attempt.

CC: Any information concerning the substance, purport or meaning of that communication.

In general IP based networks have facilities to generate the HI2 as described above.

D.3 IRI deriving

In practice the facilities that generate the IRI information are not always switched on or network wide activated. A major reason seems to be the chance they influence the performance of the network element in busy moments if activated broadly. This could than influence the overall network performance (quality).

Another aspect of HI2 in IP-networks is that more or less all networks element could be involved in the traffic of one user. The configuration of network element in a network is less hierarchical and more autonomous distributed then in circuit switched networks costing the collection of IRI information more effort.

Although the information is available in the network it might not always be desirable to derive and collect the information there.

In IP-networks almost each network element that passes through traffic has access to most of the IRI information of that traffic. This means HI3 has the opportunity to access the HI2 information, IRI as well.

The log on, log off and mobility management are in most situations handled in the networks as IRI from the start and delivered to the mediator to be delivered via HI2 directly.

This concludes that the major set of IRI information can gained from:

a) Primary network elements involved in the communication.

b) The traffic itself for instance as it is passing through the HI3.

The decision where this is done depends on network issues and national requirements. Combinations of both are likely to be needed to cover the needs.

D.4 IRI by post and pre processing HI3 information

This clause focuses the deriving of IRI by the HI3 for IP-access only (not e-mail).

The handover interface and so HI3 has two sides: the CP or mediator side and the LE or LEMF side.

Deriving the IRI from the HI3 information can therefore be done by post processing at the mediator or pre processing at the law enforcement monitoring facility.

NOTE: The terms "pre" and "post" have been chosen from the perspective of the law enforcement domain and the perspective of the providers' domain. After the mediator has done its normal processing to create HI3 information additional post processing is needed to generate HI2 information and to discard the HI3 information. Similar at the LEMF before the HI3 information enters the normal process of storage and interpretation pre processing has to take place to generate the HI2 information and discard the HI3 information.

Legal systems can allow for pre processing. Details are not relevant for the scope of the present document as they can be dealt with in the law enforcement domain.

Not all countries would allow for this solution particularly as initially all information is sent.

If post processing is required the level of processing influences the performance of the mediator and legal use of the information. An exchange can be made here on a national basis.

Taking the effort as an important parameter the Post processing could be done in different ways like:

i) Fixed header length assumption.

ii) Protocol headers extraction.

iii) Strict IRI extraction.

iv) Blanking payload.

It is a national mainly legal issue to allow for one or more of these options. Some considerations for each option include:

i) Protocol headers have dynamic lengths. Assuming a certain length minimizes the processing power needed but can give incomplete headers in some cases and clippings of content in other cases.

ii) There is more processing power needed here. Especially if not only the IP-header but also the next protocol (TCP/UDP...) is to be extracted.

iii) In a strict sense not all information in the protocol header is considered IRI. Compared to ii) more processing power will be needed and required equipment will be more complicated. The management of what items are IRI and what is not gives an extra complication.

iv) Compared to ii) the part law enforcement is not entitled to is not removed, but blanked. This gives the same load to the capacity of the delivery network etc as a full delivery of IRI and CC.

The options show it would be desirable for IRI only delivery that the HI2 and HI3 use very similar mechanisms to allow "HI3-mediator" to deliver IRI.

Annex E (informative): Purpose of profiles

The use of profiles is introduced at length in ISO/IEC TR 10000-1 [31]. These notes offer an explanation of the utility of profiles, and are inspired by a Library of Congress document Z39.50 profiles.

E.1 Formal definitions

The formal definitions used in ISO/IEC TR 10000-1 [31] are quoted below:

Profile: A set of one or more base standards and/or International Standardized Profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or International Standardized Profiles necessary to accomplish a particular function.

International Standardized Profile: An internationally agreed-to, harmonized document which describes one or more profiles.

Interoperability: The ability of two or more IT systems to exchange information and to make mutual use of the information that has been exchanged.

E.2 Purpose of profiles

Again selectively quoting from ISO/IEC TR 10000-1 [31], the purposes of profiles are:

- "identifying the standards and ISPs, together with appropriate classes, conforming subsets, options and parameters, which are necessary to accomplish identified functions (e.g. interoperability) or to support a class of applications (e.g. Transaction Processing applications)"; and
- "providing a means to enhance the availability for procurement of consistent implementations of functionally defined groups of standards and ISPs, which are expected to be the major components of real IT systems, and which realize the intentions of the corresponding reference models or frameworks with which the standards are associated".

In other words a profile may:

- offer some specific operational function, such as the handover of datagrams generated by a 2 Mbit/s to 10 Mbit/s access;
- allow any arbitrary Mediation Device (MD) and LEMF to communicate with a minimum of further configuration;
- reference several standards, and choices within these, to allow the above to be achieved.

So a profile will specify:

- some application, or some group of applications;
- selections from a base standard, such as ES 201 671 [3], in terms of choices to be made and values to be assigned to parameters;
- other supporting standards to be used, such as RFC 0793 [16], and their (layered) relationship to one another;
- the choices to be made and values to be assigned to parameters in these supporting standards.

The advantages of the use of a (carefully designed) profile then become:

- confidence that the base standard will support the nominated application(s) addressed by a specific profile;
- confidence in procuring conformant equipment, both MD and LEMF;
- confidence in interworking between conformant equipment;
- reduced effort in procuring equipment;
- reduced effort in preparing test specifications;
- release of effort from law enforcement, manufacturers and operators for other tasks;
- simplicity.

Annex F (informative): Bibliography

- ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Services not related to E.164 Voice Telephony".
- ETSI TS 102 227: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception".
- Library of Congress document Z39.50 (http://www.loc.gov/z3950/agency/).
- ETSI TS 123 107: "Universal Mobile Telecommunications System (UMTS); Quality of Service (QoS) concept and architecture (3GPP TS 23.107)".

History

Document history		
V1.1.1	February 2004	Publication