3GPP TSG SA WG3 Security — S3#32 **S3-040140**
09 - 13 February 2004
Edinburgh, Scotland, UK

3GPP TSG-SA3 LI Meeting #12 ***Tdoc ⌘S3LI04_049R1***
Miami, Florida, USA, 27 – 29 January 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.108** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **6.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Editorial Corrections
Source:	⌘	SA3 LI
Work item code:	⌘	SEC1-LI
Date:	⌘	28/01/2004
Category:	⌘	**D**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Editorial corrections.
Summary of change:	⌘	Corrections as indicated.
Consequences if not approved:	⌘	Confusion.

Clauses affected:	⌘	1,3,4,6,7,A,B,C,G

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

***** FIRST MODIFICATION *****

Introduction

This Technical Specification has been produced by 3GPP TSG SA to allow for the standardization in the area of lawful interception of telecommunications. This document addresses the handover interfaces for lawful interception of Packet-Data Services, Circuit Switched Services, and Multimedia Services within the Universal Mobile Telecommunication System (UMTS). The specification defines the handover interfaces for delivery of lawful interception Intercept Related Information (IRI) and Content of Communication (CC) to the Law Enforcement Monitoring Facility.

Laws of individual nations and regional institutions (e.g. European Union), and sometimes licensing and operating conditions define a need to intercept telecommunications traffic and related information in modern telecommunications systems. It has to be noted that lawful interception shall always be done in accordance with the applicable national or regional laws and technical regulations. Nothing in this specification, including the definitions, is intended to supplant national law.

This specification should be used in conjunction with 3GPP TS 33.106 [18] and 33.107 [19] in the same release. This specification may also be used with earlier releases of 33.106 and 33.107, as well as for earlier releases of UMTS and GPRS.

1 Scope

This specification addresses the handover interfaces for ~~lawful~~ Lawful ~~interception~~Interception (LI) of Packet-Data Services, Circuit Switched Services, and Multimedia Services within the UMTS network. The handover interface in this context includes the delivery of Intercept Related Information (HI2) and Content of Communication (HI3) to the Law Enforcement Monitoring Facility.

***** NEXT MODIFICATION *****

3.1 Definitions

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

access provider: access provider provides a user of some network with access from the user's terminal to that network.

NOTE 1: This definition applies specifically for the present document. In a particular case, the access provider and network operator may be a common commercial entity.

(to) buffer: temporary storing of information in case the necessary telecommunication connection to transport information to the LEMF is temporarily unavailable.

communication: Information transfer according to agreed conventions.

content of communication: information exchanged between two or more users of a telecommunications service, excluding intercept related information. This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

handover interface: physical and logical interface across which the interception measures are requested from network operator / access provider / service provider, and the results of interception are delivered from a network operator / access provider / service provider to a law enforcement monitoring facility.

identity: technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis.

interception: action (based on the law), performed by ~~an~~ a network operator / access provider / service provider, of making available certain information and providing that information to a law enforcement monitoring facility.

*** NEXT MODIFICATION ***

4.3 Functional requirements

A lawful authorization shall describe the kind of information ~~(Intercept Related Information (~~IRI~~)~~ only, or IRI with ~~Content of Communication (~~CC~~))~~ that is required by an LEA, the identifiers for the interception subject, the start and stop time of LI, and the addresses of the LEAs for delivery of CC and/or IRI and further information.

A single interception subject may be the subject of interception by different LEAs. It shall be possible strictly to separate these interception measures.

If two targets are communicating with each other, each target is dealt with separately.

4.4 Overview of handover interface

The generic handover interface adopts a three port structure such that administrative information (HI1), intercept related information (HI2), and the content of communication (HI3) are logically separated.

Figure 4.1 shows a block diagram with the relevant entities for Lawful Interception.

The outer circle represents the NWO/AP/SvP´s domain with respect to lawful interception. It contains the network internal functions, the internal network interface (INI), the administration function and the mediation functions for IRI and CC. The inner circle contains the internal functions of the network (e.g. switching, routing, handling of the communication process). Within the network internal function the results of interception (i.e., IRI and CC) are generated in the Internal Interception Function (IIF).

The IIF provides the ~~Content of Communication (CC)~~CC and the ~~Intercept Related Information (IRI)~~IRI, respectively, at the Internal Network Interface (INI). For both kinds of information, mediation functions may be used, which provide the final representation of the standardized handover interfaces at the NWO/AP/SvP's domain boundary.

*** NEXT MODIFICATION ***

4.4.2 Handover interface port 3 (HI3)

The port HI3 shall transport the ~~content of the communication (~~CC~~)~~ of the intercepted telecommunication service to the LEMF. The ~~content of communication~~CC shall be presented as a transparent en-clair copy of the information flow during an established, frequently bi-directional, communication of the interception subject.

As the appropriate form of HI3 depends upon the service being intercepted, HI3 is described in relevant annexes.

The HI2 and HI3 are logically different interfaces, even though in some installations the HI2 and HI3 packet streams might also be delivered via a common transmission path from a MF to a LEMF. It is possible to correlate HI2 and HI3 packet streams by having common (referencing) data fields embedded in the IRI and the CC packet streams.

4.5 HI2: Interface port for intercept related information

The HI2 interface port shall be used to transport all ~~intercept related information (~~IRI~~)~~, i.e. the information or data associated with the communication services of the target identity apparent to the network. It includes signalling information used to establish the telecommunication service and to control its progress, time stamps, and, if available, further information such as location information. Only information which is part of standard network signalling procedures shall be used within communication related IRI.

Sending of the ~~intercept related information (~~IRI~~)~~ to the LEMF shall in general take place as soon as possible, after the relevant information is available.

In exceptional cases (e.g. data link failure), the ~~intercept related information~~IRI may be buffered for later transmission for a specified period of time.

Within this section only definitions are made which apply in general for all network technologies. Additional technology specific HI2 definitions are specified in related Annexes.

*** NEXT MODIFICATION ***

4.5.2 Application for IRI (HI2 information)

The handover interface port 2 shall transport the ~~intercept related information (IRI)~~IRI from the NWO/AP/SvP's MF to the LEMF.

The individual IRI parameters shall be coded using ASN.1 and the basic encoding rules (BER). Where possible, the format of the information content shall be taken over from existing telecommunication standards, which are used for these parameters with the network already (e.g., IP). Within the ASN.1 coding for IRI, such standard parameters are typically defined as octet strings.

*** NEXT MODIFICATION ***

6.2.1 Timing

As a general principle, within a telecommunication system, ~~intercept related information (IRI)~~IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of ~~intercept related information~~IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting nodes clock, that is generated following the detection of the IRI triggering event.

*** NEXT MODIFICATION ***

6.5 IRI for packet domain

~~Intercept related information~~The IRI will in principle be available in the following phases of a data transmission:

1. At connection attempt when the target identity becomes active, at which time packet transmission may or may not occur (set up of a data context, target may be the originating or terminating party);
2. At the end of a connection, when the target identity becomes inactive (removal of a data context);
3. At certain times when relevant information are available.

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2, e.g. information on subscriber controlled input.

The ~~intercept related information (IRI)~~IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data context information, for standard data transmission between two parties.

*** NEXT MODIFICATION ***

6.5.1.3 CONTINUE record information

The CONTINUE record is used to convey events during an active packet-data communication PDP Context.

The CONTINUE record shall be triggered when:

- An active PDP context is modified;
- during the inter-SGSN RAU, when target has got at least one PDP context active, the PLMN does not change and the triggering event information is available at the DF/MF.

In order to enable the LEMF to correlate the information~~s~~ on HI3, a new correlation number shall not be generated within a CONTINUE record.

*** NEXT MODIFICATION ***

7.2 IRI for IMS

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2, e.g. information on subscriber controlled input.

The ~~intercept related information (IRI)~~IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information).
2. Basic data context information, for standard data transmission between two parties (e.g. SIP-message).

For each event, a Record is sent to the LEMF, if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

*** NEXT MODIFICATION ***

A.2.1 Introduction

At HI2 interface FTP is used over internet protocol stack for the delivery of the IRI. The FTP is defined in ~~ref~~ [13]. The IP is defined in ~~ref~~ [15]. The TCP is defined in ~~ref~~ [16].

FTP supports reliable delivery of data. The data may be temporarily buffered in the mediation function (MF) in case of link failure. FTP is independent of the payload data it carries.

A.2.2 Usage of the FTP

The MF acts as the FTP client and the LEMF acts as the FTP server . The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The MF may buffer files.

Several records may be gathered into bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing / file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms;
- frequency of transfer, based on volume trigger, e.g. X octets.

Every file shall contain only complete IRI records. The single IRI record shall not be divided into several files.

There are two possible ways as to how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (~~ref~~see: "File naming method A)"). The other

way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (~~ref~~see: "File naming method B)").

*** NEXT MODIFICATION ***

A.2.6 Other considerations

The FTP protocol mode parameters used:

Transmission Mode:	stream
Format:	non-print
Structure:	file-structure
Type:	binary

The FTP client (=user -FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), 'passive' mode is supported. The data transfer process listens to the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;
- interception file type, "1" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

Timing considerations for the HI2 FTP transmission

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of this document.

The following timers may be used within the LI application:

Table A.2: Timing considerations

Name	Controlled by	Units	Description
T1 inactivity timer	LEMF	Seconds	Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side.
T2 send file trigger	MF	Milliseconds	Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (~~Ref.~~See C.2.2).

***** NEXT MODIFICATION *****

Annex B (normative): Structure of data at the handover interface

This annex specifies the coding details at the handover interface HI for all data, which may be sent from the NWO/AP/SvP's equipment to the LEMF, across HI.

At the HI2 and HI3 handover interface ports, the following data may be present:

- interface port HI2: ~~Intercept related information (IRI)~~IRI;
- interface port HI3: records containing ~~content of communication (CC)~~CC.

The detailed coding specification for these types of information is contained in this annex, including sufficient details for a consistent implementation in the NWO/AP/SvP's equipment and the LEMF.

It must be noticed some data are ROSE specific and have no meaning when FTP is used. Those specificities are described at the beginning of each sub-annex.

***** NEXT MODIFICATION *****

B.3 Intercept related information (HI2)

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier     [0]  ENUMERATED
    {
        gPRS-Target(3),
        ...
    },
    partyIdentity       [1] SEQUENCE
    {
        imei                    [1] OCTET STRING (SIZE (8)) OPTIONAL,
            -- See MAP format [4]

        imsi                    [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [4] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code

        msISDN                  [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
            -- MSISDN of the target, encoded in the same format as the AddressString
            -- parameters defined in MAP format document ref [4], § 14.7.8

        e164-Format             [7] OCTET STRING    (SIZE (1 .. 25)) OPTIONAL,
            -- E164 address of the node in international format. Coded in the same format as
            -- the calling party number  parameter of the ISUP (parameter part:[5])

        sip-url                 [8] OCTET STRING    OPTIONAL,
            -- See [26]

        ...,
        tel-url                 [9] OCTET STRING    OPTIONAL,
            -- See [36]
    },

    services-Data-Information   [4] Services-Data-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- complementary information associated to the basic data call
    ...
}
```

```
Location    ::= SEQUENCE
{
    globalCellID        [2] GlobalCellID    OPTIONAL,
        --see MAP format (see [4])
    rAI                 [4] Rai     OPTIONAL,
        -- the Routeing Area Identifier is coded in accordance with the § 10.5.5.15 of
        -- document ~~ref~~ [9] without the Routing Area Identification IEI (only the
        -- last 6 octets are used)
    gsmLocation         [5] GSMLocation OPTIONAL,
    umtsLocation        [6] UMTSLocation OPTIONAL,
    sAI                 [7] Sai OPTIONAL,
        -- format:  PLMN-ID 3 octets (no. 1 – 3)
        --          LAC     2 octets (no. 4 – 5)
        --          SAC     2 octets (no. 6 – 7)
        --          (according to 3GPP TS 25.413)
    ...
}
```

```
UmtsQos ::= CHOICE
{
    qosIu [1] OCTET STRING (SIZE(3..11)),
        -- The qosIu parameter shall be coded in accordance with the § 10.5.6.5 of
        -- document ~~ref~~ [9] or ~~ref~~ [21] without the Quality of service IEI and Length of
        -- quality of service IE (only the last 3, or 11 octets are used. That is, first
        -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
        -- IE' shall be excluded).
    qosGn [2] OCTET STRING (SIZE(3..254))
        -- qosGn parameter shall be coded in accordance with § 7.7.34 of document ~~ref~~ [17]
}
```

***** NEXT MODIFICATION *****

C.1.3 Definition of ULIC header version 1

ULIC-header version 1 is defined in ASN.1 ~~(ref~~ [5]~~)~~ (see annex B.4) and is encoded according to BER ~~(ref~~ [6]~~)~~. It contains the following attributes:

***** NEXT MODIFICATION *****

C.2.1 Introduction

At HI3 interface FTP is used over the internet protocol stack for the delivery of the result of interception. FTP is defined in ~~ref~~ [13]. The IP is defined in ~~ref~~ [15]. The TCP is defined in ~~ref~~ [16].

FTP supports reliable delivery of data. The data may be temporarily buffered in the sending node (MF) in case of link failure. FTP is independent of the payload data it carries.

C.2.2 Usage of the FTP

In the packet data LI the MF acts as the FTP client and the receiving node (LEMF) acts as the FTP server . The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The sending entity (MF) may buffer files.

Several smaller intercepted data units may be gathered to bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing / file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms.

- frequency of transfer, based on volume trigger, e.g. X octets.

There are two possible ways how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (~~ref~~see: "File naming method A)"). The other way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (~~ref~~see: "File naming method B)").

The HI2 and HI3 are logically different interfaces, even though in some installations the HI2 and HI3 packet streams might also be delivered via a common transmission path from a MF to a LEMF. It is possible to correlate HI2 and HI3 packet streams by having common (referencing) data fields embedded in the IRI and the CC packet streams.

File naming:

The names for the files transferred to a LEA are formed according to one of the 2 available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through a particular MF node (as in method B).

The maximum set of allowed characters in interception file names are "a"…"z", "A"…"Z", "-", "_", ".", and decimals "0"…"9".

File naming method A):

<LIID>_<seq>.<ext>

LIID = See clause 7.1.

s~~S~~**eq** = integer ranging between [0..2^64-1], in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.

e~~E~~**xt** = ASCII integer ranging between ["1".."7".] (in hex: 31H…37H), identifying the file type. The possible file type codings for intercepted data are shown in table C.1. But for the HI3 interface, only the types "2", "4", and "6" are possible.

Table C.1: Possible file types

File types that the LEA may get	Intercepted data types
"2" (in binary: 0011 0010)	CC(MO)
"4" (in binary: 0011 0100)	CC(MT)
"6" (in binary: 0011 0110)	CC(MO&MT)

(The least significant bit that is '1' in file type 1, is reserved for indicating IRI data.) ~~The bit 2 of the **ext** tells whether the Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data~~.

The bit 2 of the **ext** tells whether the ~~Mobile Originated (MO) Content of Communication (CC)~~CC(MO) is included ~~to~~ in the intercepted data.

The bit 3 of the **ext** tells whether the ~~Mobile Terminated (MT) Content of Communication (CC)~~CC(MT) is included ~~to~~ in the intercepted data.

Thus, for ~~Mobile Originated Content of Communication~~CC(MO) data, the file type is "2", for ~~MT CC~~CC(MT) data "4" and for ~~MO&MT CC~~CC(MO&MT) data "6".

*** NEXT MODIFICATION ***

C.2.4.2 Information element syntax

The dynamic TypeLengthValue (TLV) format is used for ~~ist~~ its ease of implementation and good encoding and decoding performance. Subfield sizes: Type = 2 octets, Length = 2 octets and Value = 0…N octets. From Length the T and L subfields are excluded. The Type is different for every different field standardized.

The octets in the Type and Length subfields are ordered in the little-endian order, (i.e. least significant octet first). Any multioctet Value subfield is also to be interpreted as being little-endian ordered (word/double word/long word) when it

has a (hexadecimal 2/4/8-octet) numeric value, instead of being specified to have an ASCII character string value. This means that the least significant octet/word/double word is then sent before the more significant octet/word/double word.

*** NEXT MODIFICATION ***

Table C.2: Information elements in the first version of the CC header

Mode	Type	Length	Value
M	130	2	**Version** = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.
O	131	2	**HeaderLength** = Length of the CC-header up to the start of the payload in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
O	132	2	**PayloadLength** = Length of the payload following the CC-header in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
M	133	1	**PayloadType** = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g.3GPP TS 29.060 [17]). The value 255 is reserved for future PDP Types and means: "Other".
O	134	4	**PayloadTimeStamp** = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).
C	137	1	**PayloadDirection** = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (ie. downstream), or 1 if the payload data is being sent from the target (ie. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.
O	141	4	**CCSeqNumber** = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.
M	144	8 or 20	**CorrelationNumber**~~.~~ = Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see [14]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.
			<Possible future parameters are to be allocated between 145 and 250.>
O	254	1-25	**LIID** = Field indicating the LIID as defined in this document. This field has a character string value, e.g. "ABCD123456".
O	255	1-N	**PrivateExtension** = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document 3GPP TS 29.060 [17].

*** NEXT MODIFICATION ***

Table C.3: Information elements in the second version of the CC header

Mode	Type	Length	Value
M	130	2	**Version** = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.
O	131	2	**HeaderLength** = Length of the CC-header up to the start of the payload in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention).
O	132	2	**PayloadLength** = Length of the payload following the CC-header in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
M	133	1	**PayloadType** = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g.3GPP TS 29.060 [17]). The value 255 is reserved for future PDP Types and means: "Other".
O	134	4	**PayloadTimeStamp** = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).
C	137	1	**PayloadDirection** = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (ie. downstream), or 1 if the payload data is being sent from the target (ie. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.
O	141	4	**CCSeqNumber** = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.
M	144	8 or 20	**CorrelationNumber** = Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see [14]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.
			<Possible future parameters are to be allocated between 145 and 250.>
M	251	2	**MainElementID** = Identifier for the TLV element that encompasses one or more HeaderElement-PayloadElement pairs for intercepted packets.
M	252	2	**HeaderElementID** = Identifier for the TLV element that encompasses the CC-header of a PayloadElement.
M	253	2	**PayloadElementID** = Identifier for the TLV element that encompasses one intercepted Payload packet.
O	254	1-25	**LIID** = Field indicating the LIID as defined in this document. This field has a character string value, e.g. "ABCD123456".
O	255	1-N	**PrivateExtension** = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document 3GPP TS 29.060 [17].

*** NEXT MODIFICATION ***

Table C.4: Timing considerations

Name	Controlled by	Units	Description
T1 inactivity timer	LEMF	Seconds	Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side.
T2 send file trigger	MF	Milliseconds	Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (~~Ref~~see. C.2.2).

*** NEXT MODIFICATION ***

G.2.1.1 Introduction

The protocol used by the "LI application" for the encoding of IRI data and the sending of IRI data between the MF and the LEMF is based on already standardized data transmission protocols. At the HI2 interface, the "LI application" protocol is used directly over the Transmission Control Protocol (TCP), which uses the Internet Protocol (IP) for the delivery of the IRI. IP is defined in ~~ref~~ [15]. TCP is defined in ~~ref~~ [16].

TCP/IP supports reliable delivery of data. TCP is independent of the payload data it carries.