Technical Specification Group Services and System Aspects
Meeting #17, Biarritz, France, 9-12 September 2002

TSGS#17(02)0512

Source: **SA WG3**

Title: **1 CR to 33.108: Corrections to TS 33.108 (Rel-5)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020512	33.108	001		Rel-5	Corrections to TS 33.108	F	5.0.0	SEC1-LI	S3-020351

3GPP TSG SA WG3 Security — S3#23 **S3-020351**

9 - 12 July 2002

Helsinki, Finland

3GPP TSG-SA WG3 LI Meeting #11
Budapest, Hungary. 04 – 06 June 2002

Tdoc S3LI02_116 R3

CR-Form-v4

CHANGE REQUEST

⌘	**33.108**	**CR**	**001**	⌘	rev	**-**	⌘	Current version:	**5.0.0**	⌘

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

Proposed change affects: ⌘ (U)SIM □ ME/UE □ Radio Access Network □ Core Network ☒

Title:	⌘	Corrections to TS 33.108		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1-LI	***Date:*** ⌘	04 July 2002
Category:	⌘	**F**	***Release:*** ⌘	Rel-5
		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)*

Reason for change:	⌘	Correct inconsistencies.
Summary of change:	⌘	Miscellaneous corrections.
Consequences if not approved:	⌘	Possible misinterpretation and misimplementation of specification.

Clauses affected:	⌘	2, 4.4, 4.5, 6.5, 6.5.1.1, 6.5.1.2, 6.5.1.3, 6.5.1.4, B.1, B.2, B.3, B.4, C.1.3, C.2.4.2, Annex E, G.4,	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

2 References

[21] 3GPP TS 24.008: “3GPP Technical Specification Group Core Network; Mobile radio interface layer 3 specification “.

[22] ES 201 671 Edition 2: "Handover Interface for the lawful interception of telecommunications traffic".

[23] J-STD-25-A: Standard, "Lawfully Authoriz~~s~~ed Electronic Surveillance".

[24] TS 101 671 Edition 3: "Handover Interface for the lawful interception of telecommunications traffic".

[25] TS 23.003 "Numbering, addressing, and identification".

[26] RFC 2543 SIP: Session Initiation Protocol

[27] RFC 1006 ISO Transport Service on top of the TCP

[28] RFC 2126 ISO Transport Service on top of TCP (ITOT)

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 ~~2~~ 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) and the Intercept Related Information (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.

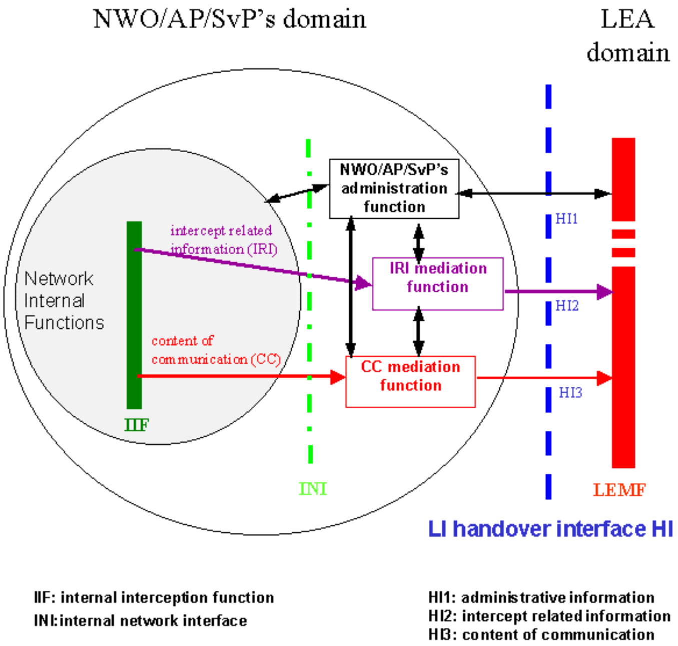

NWO/AP/SvP's domain
LEA domain
NWO/AP/SvP's administration function
intercept related information (IRI)
Network Internal Functions
IRI mediation function
content of communication (CC)
CC mediation function
IIF
INI
HI1
HI2
HI3
LEMF
LI handover interface HI
IIF: internal interception function
INI: internal network interface
HI1: administrative information
HI2: intercept related information
HI3: content of communication

Figure 4-1: Functional block diagram showing handover interface HI

NOTE 1: Figure ~~2~~ 4-1 shows only a reference configuration, with a logical representation of the entities involved in lawful interception and does not mandate separate physical entities.

NOTE 2: The mediation functions may be transparent.

4.4.1 Handover interface port 2 (HI2)

The handover interface port 2 shall transport the IRI from the NWO/AP/SvP's IIF to the LEMF.

The delivery shall be performed via data communication methods which are suitable for the network infrastructure and for the kind and volume of data to be transmitted.

The delivery can in principle be made via different types of lower communication layers, which should be standard or widely used data communication protocols.

The individual IRI parameters shall be coded using ASN.1 and the basic encoding rules (BER). The format of the parameter's information content shall be based on existing telecommunication standards, where possible.

The individual IRI parameters have to be sent to the LEMF at least once (if available).

The IRI records shall contain information available from normal network or service operating procedures. In addition the IRI records shall include information for identification and control purposes as specifically required by the HI2 port.

The IIF is not required to make any attempt to request explicitly extra information which has not already been supplied by a signa~~l~~ling system.

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 signal~~l~~ing 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 signa~~l~~ling 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 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.

6.5 IRI for packet domain

Table 6-2: Mapping between Events information and IRI information

parameter	description	HI2 ASN.1 parameter
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber).	partyInformation (party-identiity)
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber).	partyInformation (party-identity)
observed IMEI	Target Identifier with the IMEI of the target subscriber (monitored subscriber)	partyInformation (party-identity)
observed PDP address	PDP address used by the target..	partyInformation (services-data-information)
event type	Description which type of event is delivered: PDP Context Activation, PDP Context Deactivation,GPRS Attach, etc.	gPRSevent
event date	Date of the event generation in the xGSN	timeStamp
event time	Time of the event generation in the xGSN	
access point name	The APN of the access point	partyInformation (services-data-information)
PDP type	This field describes the PDP type as defined in TS GSM 09.60, TS GSM 04.08, TS GSM 09.02	partyInformation (services-data-information)
initiator	This field indicates whether the PDP context activation, deactivation, or modification is MS directed or network initiated.	initiator
correlation number	Unique number for each PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI.	gPRSCorrelationNumber
lawful interception identifier	Unique number for each lawful authorization.	lawfulInterceptionIdentifier
location information	This field provides the service area identity, RAI and/or location area identity that is present at the SGSN at the time of event record production.	locationOfTheTarget
SMS	The SMS content with header which is sent with the SMS-service	sMS
failed context activation reason	This field gives information about the reason for a failed context activation of the target subscriber.	gPRSOperationErrorCode
failed attach reason	This field gives information about the reason for a failed attach attempt of the target subscriber.	gPRSOperationErrorCode
service center address	This field identifies the address of the relevant server within the calling (if server is originating) or called (if server is terminating) party address parameters for SMS-MO or SMS-MT.	serviceCenterAddress
umts QOS	This field indicates the Quality of Service associated with the PDP Context procedure.	qOS
context deactivation reason	This field gives information about the reason for context deactivation of the target subscriber.	gPRSOperationErrorCode
network identifier	Operator ID plus SGSN or GGSN address.	networkIdentifier
iP assignment	Observed PDP address is statically or dynamically assigned.	iP-assignment
SMS originating address	Identifies the originator of the SMS message.	DataNodeAddress
SMS terminating address	Identifies the intended recipient of the SMS message.	DataNodeAddress
SMS initiator	Indicates whether the SMS is MO, MT, or Undefined	sms-initiator
serving SGSN number	An E.164 number of the serving SGSN.	~~S~~servingSGSN-Number
~~Serving~~ serving SGSN address	An IP address of the serving SGSN.	~~S~~servingSGSN-Address

NOTE: LIID parameter must be present in each record sent to the LEMF.

6.5.1.1 REPORT record information

Table 6-5: PDP Context Activation (unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN observed IMSI observed IMEI	C	Provide at least one and others when available.
observed PDP address	C	Provide to identify either the: - static address requested by the intercept subject's MS in association with a subject-initiated PDP context activation request for unsuccessful PDP context activation requests; or - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS rejects the network-initiated PDP context activation.
iP assignment	C	Provide to indicate observed PDP address is statically or dynamically assigned.
event type	C	Provide PDP Context Activation event type.
event date event time	M	Provide the date and time the event is detected.
access point name	C	Provide to identify either the: - packet data network to which the intercept subject requested to be connected when the intercept subject's mobile station is unsuccessful at performing a PDP context activation procedure (MS to Network); or - access point of the packet data network that requested to be connected to the MS when the intercept subject's mobile station rejects a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
failed context activation reason	C	Provide information about the reason for failed context activation attempts of the target subscriber.
umts QOS	C	Provide to identify the QOS parameters.

Table 6-8: Serving System REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
~~observed IMEI~~		
event type	C	Provide Serving System event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Network identifier of the HLR reporting the event.
lawful intercept identifier	M	Shall be provided.
s~~S~~ervingSGSN-Number	C	Provide to identify the E.164 number of the serving SGSN
s~~S~~ervingSGSN-Address	C	Provide to identify the IP address of the serving SGSN

6.5.1.2 BEGIN record information

Table 6-~~8~~9: PDP Context Activation (successful) BEGIN Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed IMEI		
observed PDP address	C	Provide to identify one of the following: - static address requested by the intercept subject’s MS, and allocated by the Network for a successful PDP context activation; - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e., address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address; or - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject’s MS accepts the network-initiated PDP context activation request.
iP assignment	C	Provide to indicate observed PDP address is statically or dynamically assigned.
event type	C	Provide PDP Context Activation event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject’s MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject’s MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF and to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject’s MS.
umts QOS	C	Provide to identify the QOS parameters.

Table 6-910: Start Of Interception (with PDP Context Active) BEGIN Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed IMEI		
observed PDP address	C	Provide to identify the: - static address requested by the intercept subject's MS, and allocated by the Network for a successful PDP context activation. - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e., address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address. - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS accepts the network-initiated PDP context activation request.
event type	C	Provide Start Of Interception With PDP Context Active event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject's MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject's MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF and to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
umts QOS	C	Provide to identify the QOS parameters.

6.5.1.3 CONTINUE record information

Table 6-~~10~~11: PDP Context Modification CONTINUE Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed IMEI		
observed PDP address	C	The observed address after modification Provide to identify the: - static address requested by the intercept subject's MS, and allocated by the Network for a successful PDP context activation. - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e., address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address. - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS accepts the network-initiated PDP context activation request.
event type	C	Provide the PDP Context Modification event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject's MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject's MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF used to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
umts QOS	C	Provide to identify the QOS parameters.

6.5.1.4 END record information

Table 6-~~11~~12: PDP Context Deactivation END Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed IMEI		
observed PDP address	C	Provide to identify the PDP address assigned to the intercept subject, if available.
event type	C	Provide PDP Context Deactivation event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the packet data network to which the intercept subject is connected.
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context deactivation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEM and to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject’s MS.
context deactivation reason	C	Provide to indicate reason for deactivation.

B.1 Syntax definitions

The transferred information and messages are encoded to be binary compatible with [5] (Abstract Syntax Notation One (ASN.1)) and [6] (Basic Encoding Rules (BER)).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type*, in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE.

The UNIVERSAL class is reserved for international standards such as [5] and [6]. Most parameter type identifiers in the HI ROSE operations are encoded as CONTEXT specific class. Users of the protocol may extend the syntax with PRIVATE class parameters without conflict with the present document, but risk conflict with other users' extensions. APPLICATION class parameters are reserved for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

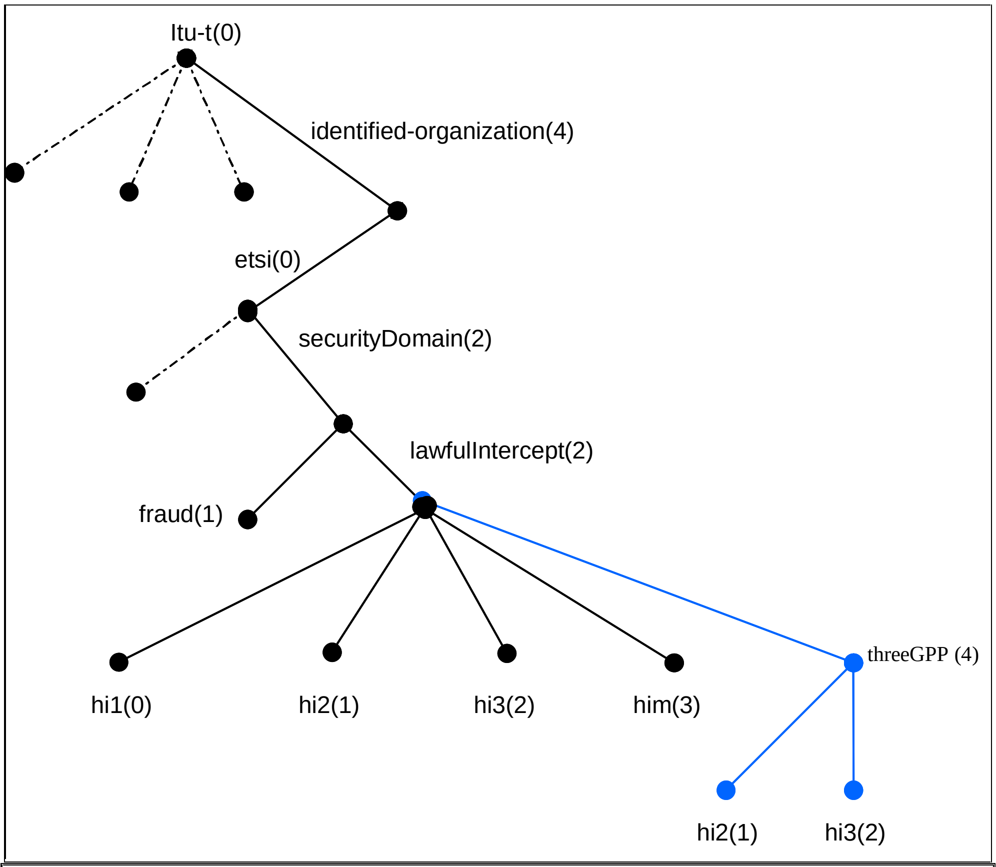
A *parameter* in the present document is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be IMPLICIT or EXPLICIT. An IMPLICIT type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. EXPLICIT types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the *Number* tag, where an EXPLICIT number of type INTEGER would have the *INTEGER* tag within the *Number* tag. The present document uses IMPLICIT tagging for more compact message encoding.

For the coding of the value part of each parameter the general rule is to use a widely use a standardized format when it exists (ISUP, DSS1, MAP, …).

As a large part of the information exchanged between the user's may be transmitted within ISUP/DSS1 signa~~l~~ling, the using of the coding defined for this signa~~l~~ling guarantee the integrity of the information provided to the LEMF and the evolution of the interface. For example if new values are used within existing ISUP parameters, this new values shall be transmitted transparently toward the LEMF.

B.2 3GPP object tree



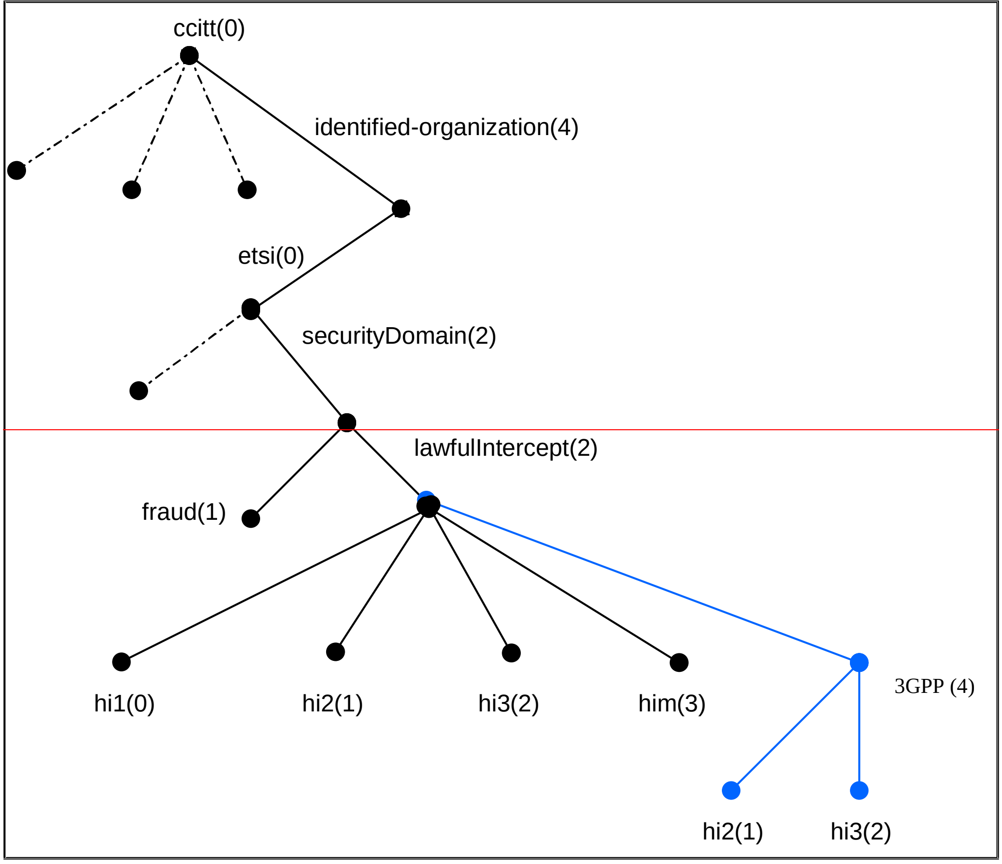


Figure B-1: 3GPP object tree

B.3 Intercept related information (HI2)

```
IRI-Parameters      ::= SEQUENCE
{
    hi2DomainId             [0] OBJECT IDENTIFIER,  -- 3GPP HI2 domain
    iRIversion              [23] ENUMERATED
    {
        version2(2),
        …
    } OPTIONAL,
        -- if not present, it means version 1 is handled
    lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    timeStamp               [3] TimeStamp,
        -- date and time of the event triggering the report.)
    initiator               [4] ENUMERATED
    {
        not-Available       (0),
        originating-Target  (1),
            -- in case of GPRS, this indicates that the PDP context activation
            -- or deactivation is MS requested
        terminating-Target  (2),
            -- in case of GPRS, this indicates that the PDP context activation or
            -- deactivation is network initiated
    ...
    } OPTIONAL,

    locationOfTheTarget     [8] Location OPTIONAL,
        -- location of the target subscriber
    partyInformation        [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party, the identiy(ies) of the party
        --)and all the information provided by the party.

    serviceCenterAddress    [13] PartyInformation OPTIONAL,
        -- e.g. in case of SMS message this parameter provides the address of  the relevant
        -- server within the calling (if server is originating) or called (if server is
        -- terminating) party address parameters
    sMS                     [14] SMS-report OPTIONAL,
        -- this parameter provides the SMS content and associated information

    national-Parameters     [16] National-Parameters OPTIONAL,
    gPRSCorrelationNumber   [18] GPRSCorrelationNumber OPTIONAL,
    gPRSevent               [20] GPRSEvent OPTIONAL,
        -- This information is used to provide particular action of the target
        -- such as attach/detach
    sgsnAddress             [21] DataNodeAddress OPTIONAL,
    gPRSOperationErrorCode  [22] GPRSOperationErrorCode OPTIONAL,
    ggsnAddress             [24] DataNodeAddress OPTIONAL,
    qOS                     [25] UmtsQos OPTIONAL,
    networkIdentifier       [26] Network-Identifier OPTIONAL,
    sMSOriginatingAddress   [27] DataNodeAddress OPTIONAL,
    sMSTerminatingAddress   [28] DataNodeAddress OPTIONAL,
    iMSevent                [29] IMSEvent OPTIONAL,
    sIPMessage              [30] OCTET STRING  OPTIONAL,
    servingSGSN-number      [31] OCTET STRING (SIZE (1..20))    OPTIONAL,
    servingSGSN-address     [32] OCTET STRING (SIZE (5..17))    OPTIONAL,
                                -- Octets are coded according to 3GPP TS 23.003 [25]
    ...
}
```

```
-- PARAMETERS FORMATS
```

```
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 RFC 2543

        ...
    },

    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
    ...
}
```

< CR note: the change is to align the comment under sip-url for consistency>

B.4 HI3 CC definition

< CR note: the change is to resize thefollowing box for consistency>

```
IMPORTS

GPRSCorrelationNumber
    FROM UmtsHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
    threeGPP(4)     hi2(1) version-1(1)}    -- from 3GPP UmtsHI2Operations

LawfulInterceptionIdentifier,

TimeStamp
    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
    version3(3)};  -- from ETSI HI2Operations TS 101 671 Edition 3
```

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:

- ULIC header version (version)
  set to version1

- lawful interception identifier (lIID, optional)
  sending of lawful interception identifier is application dependant; it is done according to national requirements

- correlation number (correlation-Number)
  As defined in clause 6.1.3

~~As defined in clause 6.1.3~~

- time stamp (timeStamp, optional),
  sending of time stamp is application dependant; it is done according to national requirements

- sequence number (sequence-number)
  Sequence Number is an increasing sequence number for tunneled T-PDUs. Handling of sequence number is application dependent; it is done according to national requirements (e.g. unique sequence number per PDP-context).

~~Sequence Number is an increasing sequence number for tunneled T-PDUs. Handling of sequence number is application dependent; it is done according to national requirements (e.g. unique sequence number per PDP-context)~~.

- TPDU direction (t-PDU-direction)
  indicates the direction of the T-PDU (from the target or to the target).

The ULIC header is followed by a subsequent payload information element. Only one information element is allowed in a single signa~~l~~ling message (see annex B.4).

C.2.4.2 Information element syntax

In ~~f~~Figure C.6, the TLV structure for UMTS HI3 transfer is presented for the case that there is just one intercepted packet inside the CC message. (There can be more CC Header IEs and CC Payload IEs in the CC, if there are more intercepted packets in the same CC message.)

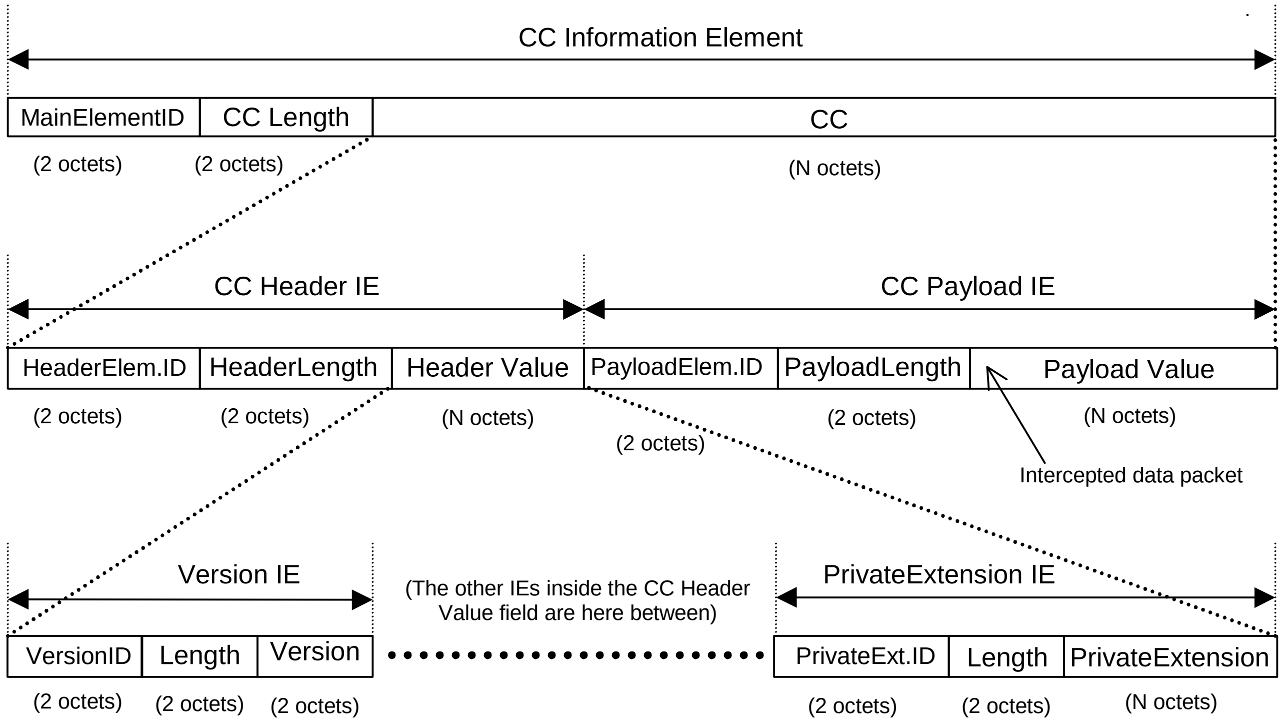


Figure C-6: IE structure of a CC message that contains one intercepted packet

Annex E (informative): Bibliography

23. TR 101 876 “Telecommunications security; Lawful Interception (LI); Description of GPRS HI3”

~~24. ETSI ES 201 671 Edition 2, Telecommunications security; Lawful Intercept (LI); Handover interface for the lawful interception of telecommunications traffic.~~

~~25. TIA/EIA J-STD-025 Lawfully Authorized Electronic Surveillance, September 2000.~~

G.4 Cross r~~R~~eference of t~~T~~erms between J-STD-025-A and 3GPP

Table G-1: Cross Reference of Terms between J-STD-025-A and 3GPP

J-STD-025-A		3GPP LI Specifications [18] [19]	
-	Call Content	CC	Content of Communication
CCC	Call Content Channel	-	Handover Interface port 3
CDC	Call Data Channel	-	Handover Interface port 2
CF	Collection Function	LEMF	Law Enforcement Monitoring Facility
-	Call-identifying Information	IRI	Intercept Related Information
-	Call-identifying message	-	IRI record
DF	Delivery Function	-	Delivery Function / Mediation Function
-	a-interface	-	X1_1 interface
-	b-interface	-	HI1 interface
-	c-interface	-	X1_2 and X1_3 interfaces
-	d-interface	-	X2 and X3 interfaces
-	e-interface	HI	Handover Interface (HI2 and HI3)
IAP	Intercept Access Point	ICE+INE	Intercepting Control Element + Intercepting Network Element
-	Intercept subject	-	Target
LAES	Lawful Authorized Electronic Surveillance	LI	Lawful Intercept
-	CaseIdentity	LIID	Lawful Interception IDentifier
LEAF	Law Enforcement Administration Function	ADMF	Administration Function
SPAF	Service Provider Administration Function	ADMF	Administration Function
-	SystemIdentity	NID	Network IDentifier
TSP	Telecommunication Service Provider	NWO/AP/SvP	Network Operator/Access Provider/Service Provider