Source: **SA3**

Title: **CRs to 33.108 for Handover interface for Lawful Interception (Rel-7)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050259	33.108	070	1	Rel-7	B	Clarifications to the timing issue	7.0.0	7.1.0	S3-050317
SP-28	SP-050259	33.108	071	-	Rel-7	B	Clarification pertaining to the filtering of SDP for IRI-only cases	7.0.0	7.1.0	S3-050200
SP-28	SP-050259	33.108	076	-	Rel-7	D	Obsolete Import Statement in Annex B.6	7.0.0	7.1.0	S3-050207

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.108** **CR** **070** ⌘ **rev** **1** ⌘ Current version: **7.0.0** ⌘

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

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

Title:	⌘	Clarifications to the timing issue
Source:	⌘	SA3 (LI)
Work item code:	⌘	SEC-LI
Date:	⌘	07/04/2005
Category:	⌘	**B**
Release:	⌘	**Rel-7**

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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change: ⌘

LI fora have been discussing for a long period of time how precise an IRI timestamp should be. That is, how many digits after the decimal dot should have the number, which represents the timestamp value.

The matter is further complicated by different interpretations of legislations in different countries. However, recent discussions yield an important common understanding that single approach to resolving the problem is not appropriate. Therefore, separate timing requirements should be defined for each network type.

Partial consensus can be summarized as follows:

- One-second precise IRI timestamp generated by an intercepting GSN is sufficient to accurately report the sequence of events for the given LI target. Implementation may opt to have higher precision, of course.
- Concerning the IRI timestamp generated by an intercepting CSCF, one-second precise IRI timestamp may not be sufficient. In order to accurately report the sequence of events for the given LI target in a given CSCF, implementation should use higher precision timestamp than one second. This requirement however is subject to national regulations.

The CR proposes necessary modifications to the packet data domain clause.

The CR proposes to add to the multi-media domain the missing subclauses:

		"Performance, reliability, and quality", "Security aspects", "Quantitative aspects".
Summary of change:	⌘	Timing matters are clarified for packet data domain and for multi-media domain.
Consequences if not approved:	⌘	Ambiguity, which leads to multiple interpretations.

Clauses affected:	⌘	6.2.1; 7.			
Other specs affected:	⌘	**Y** / **N**		⌘	
			X Other core specifications		
			X Test specifications		
			X O&M Specifications		
Other comments:	⌘	The subclauses in 7.x have been renumbered to maintain alignment between PS and IMS interception domains.			

6.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of 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. The timestamp precision should be at least 1 second [24]. Defining the required precision of an IRI timestamp however is subject to national requirements.

*** Next Modification ***

7 Multi-media domain

This clause deals with IRI reporting in the IMS. See Annexes C and G for CC interception at the SGSN/GGSN.

According to TS 33.107 [19], interception has to be supported in P-CSCF and S-CSCF. For the identification of the intercepted traffic only the SIP-URL and TEL-URL are available. In the intercepting nodes (CSCF's) the relevant SIP-Messages are duplicated and forwarded to the MF HI2.

For clarification see following Figure 7.1. If P-CSCF and S-CSCF are in the same network the events are sent twice to the LEMF.

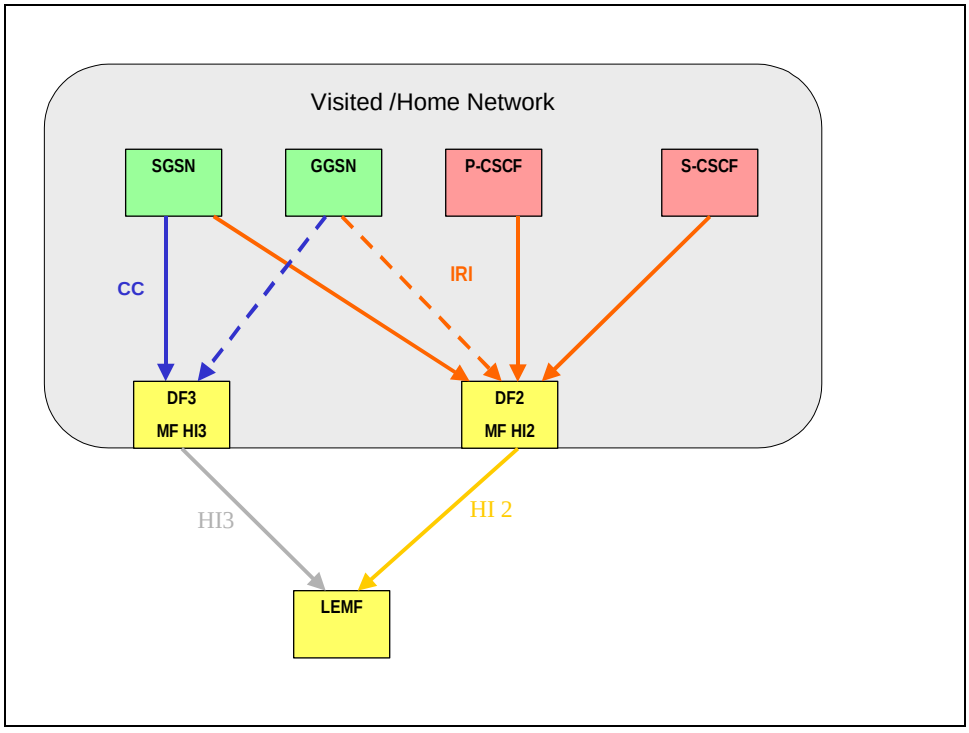

Figure 7.1: IRI Interception at a CSCF

7.1 Identifiers

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsections below.

For the delivery of CC and IRI the SGSN, GGSN and CSCF's provide correlation numbers and target identities to the HI2 and HI3. The correlation number is unique per PDP context and is used to correlate CC with IRI and the different IRI's of one PDP context.

Interception is performed on an IMS identifier(s) associated with the intercept subject including identifiers such as SIP-URL and Tel-URL [30].

7.1.1 Lawful interception identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and theoperator (NO/AN/SP).

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific interception target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter a unique LIID for each target identity of the interception subject or a single LIID for multiple target identities all pertaining to the same interception subject.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

7.1.2 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

   A network element identifier may be an IP address or other identifier.

7.1.3 Correlation number

The Correlation Number is unique per PDP context and used for the following purposes:

- correlate CC with IRI,

- correlate different IRI records within one PDP context.

As an example, in the UMTS system, the Correlation Number may be the combination of GGSN address and charging ID.

7.2 Performance, reliability, and quality

7.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of 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. Subject to national requirements, IMS specific IRI timestamp should have higher precision than 1 second.

7.2.2 Quality

QoS is not applicable to SIP signalling and hence not to IMS specific IRI records.

NOTE: The QoS class in PS domain is defined only for user plane data (CC); refer to subclause 6.2.2.

7.2.3 Reliability

The reliability associated with the result of interception should be (at least) equal to the reliability of the original SIP signalling. Reliability from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

7.3 Security aspects

Security is defined by national requirements.

7.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the interception subject;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same interception subject while maintaining unobtrusiveness, including between agencies;
- The ability of the network to simultaneously support a number of separate (i.e. multiple interception subjects) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content when SIP message also contains content).

7.5~~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 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.

Table 7.1: Mapping between IMS Events and HI2 Records Type

Event	IRI Record Type
SIP-Message	REPORT

A set of information is used to generate the record. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the CSCF or DF2 MF, if new IEs are available and if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

Table 7.2: Mapping between IMS Events Information and IRI Information

Parameter	Description	HI2 ASN.1 parameter
Observed SIP URI	Observed SIP URI	partyInformation (sip-uri)
Observed TEL URL	Observed TEL URL	partyInformation (tel-url)
Event type	IMS Event	iMSevent
Event date	Date of the event generation in the CSCF	timeStamp
Event time	Time of the event generation in the CSCF	
Network identifier	Unique number of the intercepting CSCF	networkIdentifier
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
SIP message	Either whole SIP message, or SIP message header. SIP message header is used if warrant requires only IRI. In such case, specific content in the SIPMessage (e.g. 'Message', etc.) must be deleted.	sIPMessage

NOTE 1: LIID parameter must be present in each record sent to the LEMF.
NOTE 2: Details for the parameter SIP message. If the warrant requires only signaling information, specific content in the parameter 'SIP message' like IMS (Immediate Messaging) has to be deleted/filtered.

7.52.1 Events and information

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawfully Authorized Electronic Surveillance (LAES). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 7-1 Mapping between IMS Events and HI2 Records Type and Annex B.3 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI Record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 7-1: Mapping between the IMS Event and HI2 Record Type and Table 7-2: Mapping between IMS Events Information and IRI Information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

Table 7.3: SIP-Message REPORT Record

Parameter	MOC	Description/Conditions
observed SIP-URI	C	SIP URI of the interception target (if available).
observed TEL-URL	C	TEL URL of the interception target (if available).
event type	M	Provide IMS event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	C	If available and not included in the SIP-message.
SIP message	M	The relevant SIP message or SIP message header.

TSG-SA WG1 #38 **S3-050200**
Geneva, Switzerland, 26th to 29th April 2005 **Agenda Item:**

3GPP TSG-SA3 LI Meeting #17 ***Tdoc ⌘S3LI05_039r2***
Sophia Antipolis, France, 5 – 7 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	33.108	CR	071	⌘rev	-	⌘	Current version:	7.0.0	⌘

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

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

Title:	⌘	Clarification pertaining to the filtering of SDP for IRI-only cases
Source:	⌘	SA3 LI
Work item code:	⌘	SEC1-LI
Date:	⌘	05/04/2005
Category:	⌘	**B**
Release:	⌘	**Rel-7**

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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The current text pertaining to IRI-only cases is not clear with respect to what information should be deleted before reporting the SIP message to law enforcement. Some might interpret the current statement to mean that all SIP bodies are to be deleted. Doing this, however, would also cause SDP (Session Description Protocol) information to be deleted. SDP, which could carry potentially valuable information about the media streams established by the user, should be considered connection control information and not user content. Thus, the information should be provided to law enforcement even for IRI-only cases.
Summary of change:	⌘	Clarify that SDP should be reported even in IRI-only cases.
Consequences if not approved:	⌘	Ambiguity, which leads to multiple interpretations.

Clauses affected:	⌘	3.2, 7.2

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

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [13] and the following apply:

3GPP MS	3rd Generation Mobile Communication System
3G GGSN	3rd Generation Gateway GPRS Support Node
3G GSN	3rd Generation GPRS Support Node (GGSN/SGSN)
3G MSC	3rd Generation Mobile Switching Center
3G SGSN	3rd Generation Serving GPRS Support Node
3G UMSC	3rd Generation Unified Mobile Switching Centre
AAA	Authentication, Authorization, and Accounting
ADMF	Administration Function
CC	Content of Communication
DF	Delivery Function
ECT	Explicit Call Transfer
GPRS	General Packet Radio Service
HI	Handover Interface
IA	Interception Area
ICEs	Intercepting Control Elements (3G MSC Server, 3G GMSC Server, P-CSCF, S-CSCF, SGSN, GGSN, HLR, AAA Server, PDG)
IMS	IP Multimedia Core Network Subsystem
INEs	Intercepting Network Elements (3G MSC Server, 3G GMSC Server, P-CSCF, S-CSCF, SGSN, GGSN, MGW, HLR, AAA Server, PDG)
IP	Internet Protocol
IRI	Intercept Related Information
I-WLAN	Interworking WLAN
LDI	Location Dependent Interception
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
PDG	Packet Data Gateway
RA	Routing Area
RAI	Routing Area Identity
SAI	Service Area Identity
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TEL URL	"tel" URL, as defined in [9]
URI	Universal Resource Identifier
URL	Universal Resource Locator

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 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.

Table 7.1: Mapping between IMS Events and HI2 Records Type

Event	IRI Record Type
SIP-Message	REPORT

A set of information is used to generate the record. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the CSCF or DF2 MF, if new IEs are available and if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

Table 7.2: Mapping between IMS Events Information and IRI Information

Parameter	Description	HI2 ASN.1 parameter
Observed SIP URI	Observed SIP URI	partyInformation (sip-uri)
Observed TEL URL	Observed TEL URL	partyInformation (tel-url)
Event type	IMS Event	iMSevent
Event date	Date of the event generation in the CSCF	timeStamp
Event time	Time of the event generation in the CSCF	
Network identifier	Unique number of the intercepting CSCF	networkIdentifier
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
SIP message	Either whole SIP message, or SIP message header (plus SDP body, if any). SIP message header (plus SDP) is used if warrant requires only IRI. In such cases, specific content in the SIP Message (e.g. 'Message', etc.) must be deleted.	sIPMessage

NOTE 1: LIID parameter must be present in each record sent to the LEMF.
NOTE 2: Details for the parameter SIP message. If the warrant requires only signaling information, specific content in the parameter 'SIP message' like IMS (Immediate Messaging) has to be deleted/filtered. It should be noted that SDP content within SIP messages is reported even for warrants requiring only IRI.

3GPP TSG-SA3-LI Meeting #16 ***Tdoc ⌘S3LI05_026r1***
Barcelona, Spain, 18-20 January 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.108** **CR** **076** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

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

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

Title:	⌘	Obsolete Import Statement in Annex B.6
Source:	⌘	SA3-LI
Work item code:	⌘	SEC1-LI
Date:	⌘	19/01/2005
Category:	⌘	**D**
Release:	⌘	Rel-7

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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Annex B.6 contains an import statement for the **hi3CircuitLISubDomainId**. However, an Object Identifier which is intended for the same purpose is defined within the module itself. Therefore this import should be deleted.
Summary of change:	⌘	Deletion of the import statement for the **hi3CSDomainId**
Consequences if not approved:	⌘	Possible confusion about the use of the OID.

Clauses affected:	⌘	B.6

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

Other comments:	⌘	Note this CR was agreed in the LI SWG held on 18-20 January 2005 but was not provided in the last SA3 (#37) meeting in Sophia Antipolis.

B.6 User data packet transfer (HI3 CS)

Declaration of ROSE operations circuit-Call-related-Services and no-circuit-Call-related-Services are ROSE delivery mechanism specific. When using FTP delivery mechanism, data Content-Report must be considered.

ASN.1 description of circuit data transfer operation (HI3 interface)

```
UMTS-HI3CircuitLIOperations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
hi3CS(4) r6(6) version2(2)}


DEFINITIONS IMPLICIT TAGS ::=

-- The following operations are used to transmit user data, which can be exchanged via the DSS1,
-- ISUP or MAP signalling (e.g. UUS).

BEGIN

IMPORTS OPERATION,
    ERROR
        FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

    hi3CircuitLISubDomainId
        FROM
        SecurityDomainDefinitions
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2)}

    LawfulInterceptionIdentifier,
    CommunicationIdentifier,
    TimeStamp,
    OperationErrors,
    Supplementary-Services

        FROM HI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version7(7)} -- Imported from TS 101 671v2.11.1

SMS-report
        FROM UmtsHI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi2(1) version-2(2)};

-- Object Identifier Definitions

-- Security DomainId

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

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3CSDomainId OBJECT IDENTIFIER  ::= {threeGPPSUBDomainId hi3CS(4) r6(6) version-2(2)}
```

```
uMTS-circuit-Call-related-Services  OPERATION ::=
{
    ARGUMENT    UMTS-Content-Report
    ERRORS      { OperationErrors }
    CODE        global:{ hi3CSDomainId circuit-Call-Serv (1) version1 (1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
uMTS-no-Circuit-Call-related-Services   OPERATION ::=
{
    ARGUMENT    UMTS-Content-Report
    ERRORS      { OperationErrors }
    CODE        global:{ hi3CSDomainId no-Circuit-Call-Serv (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 10s and 120s.
-- The timer default value is 60s.
```

```
UMTS-Content-Report     ::= SEQUENCE
{
    hi3CSDomainId                   [0] OBJECT IDENTIFIER OPTIONAL, -- 3GPP HI3 CS Domain.
        --  When FTP is used this parametr shall be sent to LEMF.
    version                         [23] ENUMERATED
    {
        version1(1),
        ...
    } OPTIONAL,
    lawfulInterceptionIdentifier    [6] LawfulInterceptionIdentifier OPTIONAL,
    communicationIdentifier         [1] CommunicationIdentifier,
        -- Used to uniquely identify an intercepted call: the same as used for the relevant IRI.
        -- Called "callIdentifier" in edition 1 ES 201 671.
    timeStamp                       [2] TimeStamp,
    initiator                       [3] ENUMERATED
    {
        originating-party(0),
        terminating-party(1),
        forwarded-to-party(2),
        undefined-party(3),
        ...
    } OPTIONAL,
    content                         [4] Supplementary-Services OPTIONAL,
        -- UUI are encoded in the format defined for the User-to-user information parameter
        -- of the ISUP protocol (see EN 300 356 [30]). Only one UUI parameter is sent per message.
    sMS-report                      [5] SMS-report OPTIONAL,
    ...
}
```

```
END –- UMTS-HI3CircuitLIOperations
```