
Source: SA WG3
Title: 6 Release 6 CRs to 33.108 (Rel-6)
Document for: Approval
Agenda Item: 7.3.3

Meet	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SAWG3 Doc
SP-21	SP-030480	33.108	017	-	Rel-6	D	Correct Abbreviations in TS 33.108	6.2.0	6.3.0	S3-030352
SP-21	SP-030480	33.108	020	-	Rel-6	D	Inconsistency in Annex B.3	6.2.0	6.3.0	S3-030352
SP-21	SP-030480	33.108	021	-	Rel-6	F	Data Link Establishment and Sending part for ROSE operation	6.2.0	6.3.0	S3-030352
SP-21	SP-030480	33.108	022	-	Rel-6	F	Correction on the usage of Lawful Interception identifiers	6.2.0	6.3.0	S3-030352
SP-21	SP-030480	33.108	023	-	Rel-6	F	Subscriber controlled input clarification	6.2.0	6.3.0	S3-030352
SP-21	SP-030480	33.108	024	-	Rel-6	D	Field separator in subaddress	6.2.0	6.3.0	S3-030352

CHANGE REQUEST

⌘ **33.108 CR 017** ⌘ rev - ⌘ Current version: **6.1.0** ⌘

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:	⌘ Correct Abbreviations in TS 33.108		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC-LI	Date:	⌘ 20/05/03
Category:	⌘ D	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2 (GSM Phase 2)	
	A (corresponds to a correction in an earlier release)	R96 (Release 1996)	
	B (addition of feature),	R97 (Release 1997)	
	C (functional modification of feature)	R98 (Release 1998)	
	D (editorial modification)	R99 (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	⌘ Incorrect abbreviations for NWOs/APs/SvPs		
Summary of change:	⌘ Changes to all occurrences in the specification.		
Consequences if not approved:	⌘ Inconsistencies in use of terminology with respect to other 3GPP specifications.		

Clauses affected:	⌘ 3.2, 4.4, 4.4.1, 4.5.1, 4.5.2, 5.1.1, 5.1.2.1, 5.2.2.1, 5.3.1, 5.4.1, 6.1.1, 6.1.2, 6.2.2, 6.2.3, 7.1.1, 7.1.2, Annex B, Annex D, G.4										
Other specs Affected:	<table border="1" style="border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
		Test specifications									
		O&M Specifications									
Other comments:	⌘										

3.2 Abbreviations

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

AP AN	Access Provider Network
ASN.1	Abstract Syntax Notation, Version 1
ASE	Application Service Element
BER	Basic Encoding Rules
CC	Content of Communication
CSCF	Call Session Control Function
DF	Delivery Function
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GLIC	GPRS LI Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSN	GPRS Support Node (SGSN or GGSN)
GTP	GPRS Tunnelling Protocol
HI	Handover Interface
HI1	Handover Interface Port 1 (for Administrative Information)
HI2	Handover Interface Port 2 (for Intercept Related Information)
HI3	Handover Interface Port 3 (for Content of Communication)
HLC	High Layer Compatibility
IA	Interception Area
IA5	International Alphabet No. 5
IAP	Interception Access Point
ICI	Interception Configuration Information
IE	Information Element
IIF	Internal Interception Function
IMEI	International Mobile station Equipment Identity
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identity
INI	Internal network interface
IP	Internet Protocol
IPS	Internet Protocol Stack
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
LLC	Lower layer compatibility
LSB	Least significant bit
MAP	Mobile Application Part
MF	Mediation Function
MS	Mobile Station
MSB	Most significant bit
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NEID	Network Element Identifier
NID	Network Identifier
NW NO	Network Operator
OA&M	Operation, Administration & Maintenance
P-CSCF	Proxy Call Session Control Function
PDP	Packet Data Protocol

PLMN	Public land mobile network
PSTN	Public Switched Telephone Network
ROSE	Remote Operation Service Element
R _x	Receive direction
S-CSCF	Serving Call Session Control Function
SGSN	Serving GPRS Support Node
SMAF	Service Management Agent Function
SMF	Service Management Function
SMS	Short Message Service
SvP SvPSP	Service Provider
TCP	Transmission Control Protocol
TI	Target identity
TP	Terminal Portability
T-PDU	tunneled PDU
T _x	Transmit direction
UI	User Interaction
UMTS	Universal Mobile Telecommunication System
VPN	Virtual Private Network

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~~
Operator's (NO/AN/SP) 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~~
Operator's (NO/AN/SP) domain boundary.

4.4.1 Handover interface port 2 (HI2)

The handover interface port 2 shall transport the IRI from the [NWO/AP/SvPoperator's \(NO/AN/SP\)](#) IIF to the LEMF.

The delivery to the handover interface port 2 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. From the [NWOs/APs/SvPsoperator \(NO/AN/SP\)](#) to LEMF delivery is subject to the facilities procured by the government.

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 are transmitted individually. As an option, IRI records can be aggregated for delivery to the same LEA (i.e. in a single delivery interaction). As there are time constraints associated with the delivery of IRI, the use of this optional feature is subject to national or regional requirements. As a general principle, IRI records shall be sent immediately and shall not be withheld in the MF/DF in order to use the IRI record aggregation option.

The IRI records shall contain information available from normal [NWO/APs/SvPprovider \(NO/AN/SP\)](#) operating procedures. In addition the IRI records shall include information for identification and control purposes as specifically required by the HI2 port.

4.5.1 Data transmission protocols

The protocol used by the "LI application" for the encoding and the sending of data between the MF and the LEMF is based on already standardized data transmission protocols like ROSE or FTP.

The specified data communication methods provide a general means of data communication between the LEA and the [NWO/AP/SvP's operator's \(NO/AN/SP\)](#) mediation function. They are used for the delivery of:

- HI2 type of information (IRI records);
- Certain types of content of communication (e.g., SMS).

The present document specifies the use of the two possible methods for delivery: ROSE or FTP on the application layer and the BER on the presentation layer. The lower layers for data communication may be chosen in agreement with the [NWO/AP/SvP operator \(NO/AN/SP\)](#) and the LEA.

The delivery to the LEMF should use the internet protocol stack.

4.5.2 Application for IRI (HI2 information)

The handover interface port 2 shall transport the intercept related information (IRI) from the [NWO/AP/SvP's operator's \(NO/AN/SP\)](#) 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.

5.1.1 Lawful Interception IDentifier (LIID)

For each target identity related to an interception measure, the authorized [NWO/AP/SvP operator \(NO/AN/SP\)](#) shall assign a special Lawful Interception IDentifier (LIID), which has been agreed between the LEA and the [NWO/AP/SvP operator \(NO/AN/SP\)](#). It is used within parameters of all HI interface ports.

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 [NWO/AP/SvP operator \(NO/AN/SP\)](#) and the handling agents at the LEA.

The Lawful Interception IDentifier 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 (or digit string for sub-address option, see annex J). It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized [NWO/AP/SvP operator \(NO/AN/SP\)](#) shall enter for each target identity of the interception subject a unique LIID.

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

5.1.2.1 Network Identifier (NID)

The Network Identifier is a mandatory parameter; it should be internationally unique. It consists of one or both of the following two identifiers.

- **NWO/AP/SvPOperator- (NO/AN/SP)-** identifier (mandatory):
Unique identification of network operator, access [network](#) provider or service provider.
- 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 E.164 international node number
- an X.25 address;
- an IP address.

5.2.2.1 Control Information for HI2

The main purpose of this information is the unique identification of records related to a target identity, including their unique mapping to the links carrying the Content of Communication. In general, parameters of this category are mandatory, i.e. they have to be provided in any record.

The following items are identified (in brackets: ASN.1 name and reference to the ASN.1 definition or clause B.3a):

- 1) Record type (*IRIContent*, see clause B.3a)
IRI-BEGIN, IRI-CONTINUE, IRI-END, IRI-REPORT-record types.
- 2) Version indication (*iRIversion*, see clause B.3a)
Identification of the particular version of the HI2 interface specification.
- 3) Communication Identifier (*CommunicationIdentifier*, see clauses 5.1.2 and B.3a).
- 4) Lawful Interception Identifier (*LawfulInterceptionIdentifier*, see clauses 5.1.1 and B.3a).
- 5) Date & time (*TimeStamp*, see clause B.3a)
Date & time of record trigger condition.
The parameter shall have the capability to indicate whether the time information is given as Local time without time zone, GMT with time zone, or UTC. Normally, the **NWO/AP/SvPOperator (NO/AN/SP)** shall define these options.
- 6) CC Link Identifier (*CC-Link-Identifier*, see clause 5.1.3 for definition and clause B.3a for ASN.1 definition).

5.3.1 Delivery of Content of Communication

CC will be delivered as described in annex J.

Exceptionally, SMS will be delivered via HI2.

The transmission media used to support the HI3 port shall be standard ISDN calls, based on 64 kbit/s circuit switched bearer connections. The CC links are set up on demand to the LEMF. The LEMF constitutes an ISDN DSS1 user function, with an ISDN DSS1 basic or primary rate access. It may be locally connected to the target switching node, or it may be located somewhere in the target network or in another network, with or without a transit network in between.

For network signalling, the standard ISDN user part shall be used. No modifications of the existing ISDN protocols shall be required. Any information needed for LI, like to enable correlation with the IRI records of a call, can be inserted in the existing messages and parameters, without the need to extend the ETSI standard protocols for the LI application.

For each LI activation, a fixed LEMF address is assigned; this address is, within the present document, not used for any identification purposes; identification and correlation of the CC links is performed by separate, LI specific information, see clause 5.1.

The functions defined in the ISDN user part standard, Version 1 (ETSI ISUP V1) are required as a minimum within the target network and, if applicable, the destination and transit networks, especially for the support of:

- Correlation of HI3 information to the other HI port's information, using the supplementary service user-to-user signalling 1 implicit (UUS1).
- Access verification of the delivery call (see clause 5.3.3).

The bearer capability used for the CC links is 64 kbit/s unrestricted digital information; this type guarantees that the information is passed transparently to the LEMF. No specific HLC parameter value is required.

| The CC communication channel is a one-way connection, from the [NWO/AP/SvPoperator's \(NO/AN/SP\) IIF](#) to the LEMF, the opposite direction is not switched through in the switching node of the target.

5.4.1 General

In general, LI shall be possible for all connections and activities in which the target is involved. The target shall not be able to distinguish alterations in the offered service. It shall also not be possible to prevent interception by invoking supplementary services. Consequently, from a supplementary services viewpoint, the status of interactions with LI is "no impact", i.e. the behaviour of supplementary services shall not be influenced by interception.

Depending on the type of supplementary service, additional CC links to the LEA may be required, in addition to already existing CC links.

Within the IRI records, the transmission of additional, supplementary service specific data may be required.

Supplementary services, which have an impact on LI, with respect to CC links or IRI record content, are shown in table 5.7. The table is based on UMTS services, it considers the services which have been standardized at the time of finalizing the present document. Future services should be treated following the same principles.

NOTE 1: Co-ordination of handling of new services should be performed via 3GPP SA WG3-LI. If required, additions will be included in a subsequent version of the present document.

The question of Lawful Interception with Intelligent Networks is not covered in this version (see note 2).

NOTE 2: The general principle is, that LI takes place on the basis of a technical identity, i.e. a directory number. Only numbers which are known to the [NWO/AP/SvPoperator \(NO/AN/SP\)](#), and for which LI has been activated in the standard way, can be intercepted. No standardized functions are available yet which would enable an SCF to request from the SSF the invocation of LI for a call.

6.1.1 Lawful interception identifier

For each target identity related to an interception measure, the authorized [NWO/AP/SvPoperator \(NO/AN/SP\)](#) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the [NWO/AP/SvPoperator \(NO/AN/SP\)](#).

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 [NWO/AP/SvPoperator \(NO/AN/SP\)](#) operators 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 [NWO/AP/SvPoperator \(NO/AN/SP\)](#) 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.

6.1.2 Network identifier

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

- 1) [NWO/AP/SvP 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. For GSM and UMTS systems deployed in the U.S., the network element identifier is required.

6.2.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the quality of service of the original content of communication. This may be derived from the QoS class used for the original intercepted session [20]. However, when TCP is used as an OSI layer 4 protocol across the HI3, real time delivery of the result of the interception cannot be guaranteed. The QoS used from the [NWOs/APs/SvPs operator \(NO/AN/SP\)](#) to the LEMF is determined by what law enforcement procures.

6.2.3 Reliability

The reliability associated with the result of interception should be (at least) equal to the reliability of the original content of communication. This may be derived from the QoS class used for the original intercepted session [7].

Reliability from the [NWOs/APs/SvPs operator \(NO/AN/SP\)](#) to the LEMF is determined by what law enforcement procures.

7.1.1 Lawful interception identifier

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

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/SvPoperator's \(NO/AN/SP\)](#) 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);
- interface port HI3: records containing content of communication (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/SvPoperator's \(NO/AN/SP\)](#) 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.

Annex D (informative): LEMF requirements - handling of unrecognised fields and parameters

During decoding of a record at the LEA, the following exceptional situations may occur:

- 1) Unrecognized parameter: The parameter layout can be recognized, but its name is not recognized:
The parameter shall be ignored, the processing of the record proceeds.
- 2) The parameter content or value is not recognized or not allowed:
The parameter shall be ignored, the processing of the record proceeds.
- 3) The record cannot be decoded (e.g. it seems to be corrupted):
The whole record shall be rejected when using ROSE delivery mechanism or ignored.

NOTE: In cases 2 and 3, the LEMF may wish to raise an alarm to the [NWO/AP/SvPoperator \(NO/AN/SP\)](#) administration centre. For case 1, no special error or alarm procedures need be started at the LEA, because the reason may be the introduction of a new version of the specification in the network, not be an error as such security aspects.

G.4 Cross reference of terms 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
-	CasIdentity	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	NW/O/AP/SvP <u>NO/AN/SP</u>	Network Operator/Access Provider/Service Provider <u>Network Operator, Access Network Provider, Service Provider</u>

CHANGE REQUEST

⌘ **33.108 CR 020** ⌘ rev - ⌘ Current version: **6.1.0** ⌘

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:	⌘ Inconsistency in Annex B.3		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC1-LI	Date:	⌘ 21/05/03
Category:	⌘ D	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2	(GSM Phase 2)
	A (corresponds to a correction in an earlier release)	R96	(Release 1996)
	B (addition of feature),	R97	(Release 1997)
	C (functional modification of feature)	R98	(Release 1998)
	D (editorial modification)	R99	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	⌘ Inconsistency of the ASN1 wording between ETSI TS 101 671 and 3GPP 33.108 in the ASN1 definition of Annex B.3
Summary of change:	⌘ With FTP as well as with ROSE the ASN.1 encoding should start with 'UmtsIRIsContent'.
Consequences if not approved:	⌘ Implementors might assume that aggregation of IRI records is not permitted when using ROSE as long as the ASN1 script source of TS 33.108 makes mention to the File terminology, as there is no File notation in ROSE, but only in FTP.

Clauses affected:	⌘ Annex B.3										
Other specs Affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> </table>	Y	N		X		X		X	Other core specifications	⌘
Y	N										
	X										
	X										
	X										
		Test specifications									
		O&M Specifications									
Other comments:	⌘										

B.3 Intercept related information (HI2)

Declaration of ROSE operation umts-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data **UmtsIRIsContent** must be considered.

ASN1 description of IRI (HI2 interface)

```
UmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) threeGPP(4) hi2(1) version-2(2)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

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

LawfulInterceptionIdentifier,
TimeStamp,
Network-Identifier,
National-Parameters,
DataNodeAddress,
IPAddress,
IP-value,
X25Address

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

```
-- 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)}
hi2DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2(1) version-2(2)}
```

```
umts-sending-of-IRI OPERATION ::=
```

```
{
    ARGUMENT    UmtsIRIsFileContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2(1) opcode(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.
```

```
UmtsIRIsFileContent ::= CHOICE
```

```
{
    umtsIRIContent          UmtsIRIContent,
    umtsIRIFileSequence    UmtsIRIFileSequence
}
UmtsIRIFileSequence ::= SEQUENCE OF UmtsIRIContent
```

```
-- Aggregation of UmtsIRIContent is an optional feature.  
-- It may be applied in cases when at a given point in time  
-- several IRI records are available for delivery to the same LEA destination.  
-- As a general rule, records created at any event shall be sent  
-- immediately and not withheld in the DF or MF in order to  
-- apply aggregation.  
-- When aggregation is not to be applied,  
-- UmtsIRIContent needs to be chosen.
```

CHANGE REQUEST

⌘ **33.108 CR 021** ⌘ rev - ⌘ Current version: **6.1.0** ⌘

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:	⌘ Data Link Establishment and Sending part for ROSE operation		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC1-LI	Date:	⌘ 21/05/03
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2 (GSM Phase 2)	
	A (corresponds to a correction in an earlier release)	R96 (Release 1996)	
	B (addition of feature),	R97 (Release 1997)	
	C (functional modification of feature)	R98 (Release 1998)	
	D (editorial modification)	R99 (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	⌘ TS 33.108 sections A.1.2.3 (Data Link Management) and A.1.2.1 (Sending part) related to ROSE operations can be considered as confusing. That CR gives a rewording for clarification of that ambiguity with more accuracy. When separation between those both parts becomes more clearly the TS 33.108 makes clear the data link establishment shall be initiated either by MF or by LEMF. That CR doesn't intend to restrict the behaviour to only one side initiation and therefore, for backward compatibility reasons, proposes that both currently allowed options shall be maintained.		
Summary of change:	⌘ Modified text in section A.1.2.3 and A.1.2.1		
Consequences if not approved:	⌘ Implementors might assume that there are restrictions for data link management between MF and LEMF.		

Clauses affected:	⌘ A.1.2.3, A.1.2.1 and A.1.2.3.1										
Other specs Affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
		Test specifications	⌘								
		O&M Specifications	⌘								
Other comments:	⌘										

A.1.2.1 Sending part

To request the sending of data to a peer entity, the LI_Application provides the ASE_HI, the address of the peer entity, the nature of the data and the data.

On receiving a request of the LI_Application:

- If the data link toward the peer entity address is active, the ASE_HI, from the nature of the data provided, encapsulates this data in the relevant RO-Invoke operation.
- If the data link toward the peer entity address isn't active, the ASE_HI ~~establishes this data link (see annex A.1.2.3). Then, depending on the nature of the data provided, the ASE_HI encapsulates this data in the relevant RO-Invoke operation.~~ [reports the data link unavailability to LI-Application.](#)

Note: Until the data link is established according to A.1.2.3.1, the request of the LI_Application cannot be successfully processed by ASE_HI.

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

A.1.2.3 Data link management

This function is used to establish or release a data link between two peer LI_Applications entities (MF and LEMF). ~~Depending on a per destination address configuration data, the data link establishment may be required either by the LEMF LI_Application or by the MF LI_Application.~~

A.1.2.3.1 Data link establishment

Depending on a per destination address configuration data, the data link establishment may be requested either by the LEMF LI_Application or by the MF LI_Application.

To request the establishment of a data link toward a peer entity, the LI_Application provides, among others, the destination address of the peer entity (implicitly, this address defined the protocol layers immediately under the ASE_HI: TCP/IP, X25, ...). On receipt of this request, the ASE_HI request the establishment of the data link with respect of the rules of the under layers protocol.

CHANGE REQUEST

33.108 CR 022 # rev **-** # Current version: **6.1.0**

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:	# Correction on the usage of Lawful Interception identifiers		
Source:	# SA WG3		
Work item code:	# SEC1-LI	Date:	# 12/05/2003
Category:	# F	Release:	# Rel-6
	<i>Use one of the following categories:</i> 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 .		<i>Use one of the following releases:</i> 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:	# The current version of TS 33.108 (rel-6) describes how the identifiers for Lawful Interception are exchanged between the mediation function and the LEMF and includes as possible option the interception of Call Content only. This is not according to 3GPP Lawful Interception Requirements TS 33.106, which states (clause 5.2.1.1) that "As a result of the activation (of a warrant) it shall be possible to request for the specified target, either IRI, or both the IRI and the CC and designate the LEA destination addresses for the delivery of the CC and IRI if required. These shall be selectable on a 3GMS basis according to national options".
Summary of change:	# The description of usage of identifiers applicable to the "CC only" option is removed.
Consequences if not approved:	# Lawful Interception Handover Interface would be not according to Lawful Interception Requirements. Misalignment between 3GPP TSs 33.106 and 33.108.

Clauses affected:	# 5.1.5										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> </table>	Y	N	#	#	#	#	#	#	Other core specifications Test specifications O&M Specifications	#
Y	N										
#	#										
#	#										
#	#										
Other comments:	#										

***** FIRST MODIFIED SECTION *****

5.1.5 Usage of Identifiers

The identifiers are exchanged between the mediation function and the LEMF via the interfaces HI1, HI2 and HI3. There exist several interface options for the exchange of information. Tables 5.1 and 5.2 define the usage of numbers and identifiers depending on these options.

NOTE: X in tables 5.1 and 5.2: Identifier used within parameters of the interface.

Table 5.1: Usage of identifiers, IRI and CC transmitted; options A, B (see clause 5.4.4)

Identifier	IRI and CC transmitted (option A)			IRI and CC transmitted (option B)		
	HI1	HI2	HI3	HI1	HI2	HI3
LIID	X	X	X	X	X	X
NID		X	X		X	X
CIN		X	X		X	X (see note 1)
CCLID					X	X (see note 2)

NOTE 1: The CIN of the 1st call for which this CC link has been set-up.
 NOTE 2: The CCLID may be omitted, see clause 5.1.3.

Table 5.2: Usage of identifiers, only IRI ~~or only CC~~ transmitted

Identifier	Only IRI transmitted		Only CC transmitted	
	HI1	HI2	HI1	HI3
LIID	X	X	X	X
NID		X		X
CIN		X		X
CCLID				

Identifier	Only IRI transmitted	
	HI1	HI2
LIID	X	X
NID		X
CIN		X
CCLID		

***** END OF MODIFICATIONS *****

CHANGE REQUEST

33.108 CR 023 # rev **-** # Current version: **6.1.0**

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:	# Subscriber controlled input clarification		
Source:	# SA WG3		
Work item code:	# SEC1-LI	Date:	# 12/05/2003
Category:	# F	Release:	# Rel-6
	<i>Use one of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)		<i>Use one of the following releases:</i> 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)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		

Reason for change:	# The current version of the specification states that "At the exchange, where the subscriber data of a target shall be modified via a remote control procedure, an IRI-REPORT record shall be generated as if the control procedure had taken place locally". This sentence, which was incorporated from ETSI ES 201 671, is applicable to wireline network, in which the subscriber is connected to a local exchange, but not to wireless networks described in 3GPP specifications, in which the subscriber profile is stored in the HLR/HSS and downloaded to the VLR.
Summary of change:	# The sentence quoted in the Reason for Change is deleted.
Consequences if not approved:	# TS 33.108 would contain a misleading sentence, not applicable to wireless networks.

Clauses affected:	# 5.4.5										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> </table>	Y	N	#	#	#	#	#	#	Other core specifications Test specifications O&M Specifications	#
Y	N										
#	#										
#	#										
#	#										
Other comments:	# The current text was incorporated by ETSI ES 201 671.										

***** FIRST MODIFIED SECTION *******5.4.5 Subscriber Controlled Input (SCI): Activation / Deactivation / Interrogation of Services**

For user procedures for control of Supplementary Services (Activation/Deactivation/Interrogation), a special IRI record type (IRI-REPORT record) is defined to transmit the required information.

The IRI-REPORT record shall contain an indicator, whether the request of the target has been processed successfully or not.

~~At the exchange, where the subscriber data of a target shall be modified via a remote control procedure, an IRI-REPORT record shall be generated as if the control procedure had taken place locally.~~

***** END OF MODIFICATIONS *****

CR-Form-v7
CHANGE REQUEST
№ 33.108 CR 024 № rev - № Current version: 6.1.0 №

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:	№ Field separator in subaddress		
Source:	№ SA WG3		
Work item code:	№ SEC1-LI	Date:	№ 21/05/2003
Category:	№ D	Release:	№ Rel-6
	Use <u>one</u> 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 <u>one</u> 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:	№ Field separator is not specified unambiguously in clause J.2.3.2. Some authorities have query interpretation of the clause J.2.3.2. Respective CR was approved in ETSI TC LI meeting in Benalmadena to TS 101 671.
Summary of change:	№ Addition to J.2.3.2 and example of usage of Field separator in table J.2.5
Consequences if not approved:	№ Misinterpretation of separated fields and misalignment with ETSI TS 101 671.

Clauses affected:	№ J.2.3.2						
Other specs affected:	<table border="1" style="font-size: x-small;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	#	X	Other core specifications	№
	Y	N					
	#	X					
Test specifications							
O&M Specifications							
Other comments:	№						

Modified section

J.2.3.2 Field order and layout

Fields shall be presented into the subaddress in the following order:

Table J.2.3: Fields in the Called Party Subaddress

Order	Field
1	Operator-ID
2	CIN
3	CCLID
4	National Parameters

Table J.2.4: Fields in the Calling Party Subaddress

Order	Field
1	Lawful Interception Identifier (LIID)
2	Direction
3	Service Octets

Each field noted above shall be included, whether empty or not, and a field separator shall separate each field. When a field is empty, that shall be indicated by two consecutive field separators ([including field separator from the previous field](#)). There shall be a field separator after the final field, too.

Table J.2.5. Example how field separator should be used when field is empty

Bits								Octets
8	7	6	5	4	3	2	1	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CCLID ①				Field separator				7
CCLID ③				CCLID ②				8
CCLID ⑤				CCLID ④				9
CCLID ⑦				CCLID ⑥				10
Field separator				CCLID ⑧				11
								12
								13
								14
								15
(see note)								16
								17
								18
								19
								20
								21
								22
								23
NOTE: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes.								

The Service Octets as available shall always be mapped into octets 19 to 23 of the Calling Party Subaddress, as appropriate. If one of the parameters TMR, BC or HLC is not available, the octet shall be fill with "FF" hex. If Mobile

Teleservice Code is not available, octet 23 shall not be transmitted. If Mobile Teleservice Code and Mobile Bearer Service Code are not available, octets 22 and 23 shall not be transmitted.

Table J.2.65 represent called party subaddress and table J.2.76 calling party subaddress with the maximum length of the identifiers.

Table J.2.65: Called Party Subaddress

Bits								Octets
8	7	6	5	4	3	2	1	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CIN ②				CIN ①				7
CIN ④				CIN ③				8
CIN ⑥				CIN ⑤				9
CIN ⑧				CIN ⑦				10
CCLID ①				Field separator				11
CCLID ③				CCLID ②				12
CCLID ⑤				CCLID ④				13
CCLID ⑦				CCLID ⑥				14
Field separator				CCLID ⑧				15
see note								16
								17
								18
								19
								20
								21
								22
								23
NOTE: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes.								

Table J.2.76: Calling Party Subaddress

Bits								Octets
8	7	6	5	4	3	2	1	
Calling party subaddress identifier								1
Length of calling party subaddress contents								2
Type of subaddress = user specified, odd/even indicator according to the amount of BCD-digits								3
LIID ②				LIID ①				4
LIID ④				LIID ③				5
LIID ⑥				LIID ⑤				6
LIID ⑧				LIID ⑦				7
LIID ⑩				LIID ⑨				8
LIID ⑫				LIID ⑪				9
LIID ⑭				LIID ⑬				10
LIID ⑯				LIID ⑰				11
LIID ⑰				LIID ⑱				12
LIID ⑲				LIID ⑳				13
LIID ⑳				LIID ㉑				14
LIID ㉒				LIID ㉓				15
Field separator				LIID ㉔				16
Field separator				Direction				17
spare				spare				18
ITU-T Recommendation Q.763 [32] TMR (see note 1)								19
ITU-T Recommendation Q.931 BC [33] octet 3 (see note 2)								20
ITU-T Recommendation Q.931 HLC [33] octet 4 (see note 3)								21
Mobile Bearer Service Code (see note 4)								22
Mobile Teleservice Code (see note 5)								23
NOTE 1: If available, the Transmission Medium Requirement according to EN 300 356 [29]. If not available, the value is "FF" hex.								
NOTE 2: If available, only octet 3 of the Bearer Capability I.E. according to EN 300 403 [30] If not available, the value is "FF" hex.								
NOTE 3: If available, only octet 4 of the High Layer Compatibility I.E. according to EN 300 403 [30]. If not available, the value is "FF" hex.								
NOTE 4: If available, the Mobile Bearer Service Code according to ETS 300 974 [34], clause 14.7.10. If not available, the octets 22 and 23 shall not be transmitted.								
NOTE 5: If available, the Mobile Teleservice Code according to ETS 300 974 [34], clause 14.7.9. If not available, the octet 23 shall not be transmitted.								