CR-Form-v7

CHANGE REQUEST

⌘ **33.108** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	Changes to TS 33.108 for U.S. LI Requirements
Source:	⌘	SA3
Work item code:	⌘	Security
Date:	⌘	19/11/2002
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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	TS 33.108 must be clarified with respect to U.S. LI requirements.
Summary of change:	⌘	Correction to text to meet U.S. LI Requirements.
Consequences if not approved:	⌘	Will impact implementations if not corrected.

Clauses affected:	⌘	Introduction, 3, 4, 6, Annex C, Annex F, new Annex I.

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

Introduction

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

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

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

3.1 Definitions

intercept related information: collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data ~~(e.g. service profile management by subscriber)~~ and location information.

4.1 Basic principles for the handover interface

Lawful interception may require~~s~~ functions to be provided in ~~some, or all of,~~ the switching or routing nodes of a telecommunications network.

The specification of the handover interface is subdivided into three logical ports each optimised to the different purposes and types of information being exchanged.

The interface is extensible (i.e., the interface may be modified in the future as necessary).

4.3 Functional requirements

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

4.4 Overview of handover interface

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

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

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

The IIF provides the Content of Communication (CC) 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.

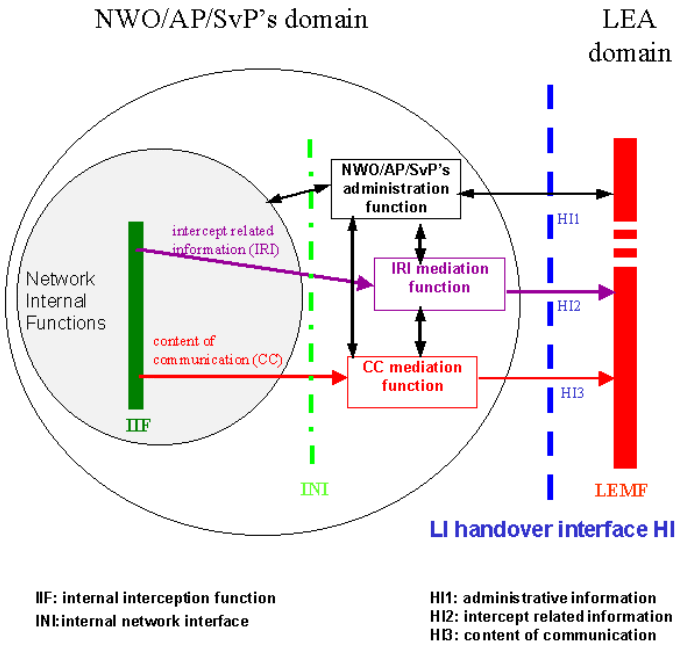

Figure 4.1: Functional block diagram showing handover interface HI

NOTE 1: Figure 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.

NOTE 3: The LEMF is responsible for collecting and analyzing IRI and CC information. The LEMF is the responsibility of the LEA.

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 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/SvPs 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 shall contain information available from normal NWO/APs/SvP/ ~~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.

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 [7]. The QoS used from the NWOs/APs/SvPs 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 to the LEMF is determined by what law enforcement procures.

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	When authorized, t~~T~~his field provides ~~the service area identity, RAI and/or location area identity~~ the location information of the target 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.	ServingSGSN-Number
Serving SGSN address	An IP address of the serving SGSN.	ServingSGSN-Address

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

C.1.2 Definition of ULIC header version 0

The correlation number consist of 8 octets. ~~and guarantees a unique identification of the tunnel to the LEA over a long time.~~ The requirements for this ~~identification~~ correlation number are similar to that defined for charging in [12], chapter 5.4. Therefore it is proposed to use the Charging-ID, defined in [12] , chapter 5.4 as part of correlation number. The Charging-ID is signaled to the new SGSN in case of SGSN-change so the tunnel identifier could be used “seamlessly” for the HI3 interface.

Annex F ~~(informative):~~
~~Profiles for FTP~~Void

~~For further study.~~

Annex I (normative):
United States lawful interception

With respect to the handover interfaces they must be capable of delivering intercepted communications and IRI information to the government in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier.

With respect to location information 'when authorized' means the ability to provide location information on a per-surveillance basis.

The delivery methods described in this document are optional methods and no specific method is required in the U.S..

The specification of lawful intercept capabilities in this document does not imply that those services supported by these lawful intercept capabilities are covered by CALEA. Inclusion of a capability in this document does not imply that capability is required by CALEA. This document is intended to satisfy the requirements of section 107 (a) (2) of the Communications Assistance for Law Enforcement Act, Pub. L. 103-414 such that a telecommunications carrier, manufacturer, or support service provider that is in compliance with this document shall have "Safe Harbor".

In the United States surveillance on the GGSN is not required, but is an option that may be negotiated between the service provider and law enforcement.

A TSP shall not be responsible for decrypting or decompressing, or ensuring the government's ability to decrypt or decompress, any communication encrypted or compressed by a subscriber or customer, unless the encryption or compression was provided by the TSP and the TSP possesses the information necessary to decrypt or decompress the communication. A TSP that provides the government with information about how to decrypt or decompress a communication (e.g., identifying the type of compression software used to compress the communication, directing the government to the appropriate vendor that can provide decryption or decompression equipment, or providing the encryption key used to encrypt the communication) fully satisfies its obligation under the preceding sentence.