
Interception regarding SMS-MT for TS 33.108

Spec: 3GPP TS 33.108v5.0.0

Release: Rel-5

Source: Telcordia Technologies and Federal Bureau of
Investigations

Document for: Discussion & Action.

Summary

This contribution proposes changes to TS 33.108, version 5.0.0, to address SMS-MT interception at a SMS Redirecting System. In this contribution an SMS Redirecting System is a node that handles SMS packets and redirects them to the intercept subject. A companion contribution proposes compatible changes to TS 33.107.

CR-Form-v7

CHANGE REQUEST

33.108 CR CRNum # 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: UICC apps ME Radio Access Network Core Network

Title:	#	Interception of SMS Redirected Packets for TS 33.108	
Source:	#	Telcordia Technologies and Federal Bureau of Investigation	
Work item code:	#	Security	Date: # 24/09/2002
Category:	#	F	Release: # Rel-5
		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:	#	The intention of this CR is to address the shortcomings in the capability of reporting SMS packets in the case of SMS-MT in particular regarding the interception of SMS packets that are redirected from the home network to the interception subject.	
Summary of change:	#	Inclusion of SMS Redirecting System requirements.	
Consequences if not approved:	#	TS 33.108 will be deficient in the area identified and will not meet all the needs of law enforcement agencies.	

Clauses affected:	#	3.1, 6.5.1.1									
Other specs affected:	#	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	X						# TS 33.107
Y	N										
X											
Other comments:	#										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked # contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43

3.1 Definitions

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

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

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

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

communication: Information transfer according to agreed conventions.

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

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

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

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

NOTE 2: In the present document the term interception is not used to describe the action of observing communications by a law enforcement agency.

interception configuration information: information related to the configuration of interception.

interception interface: physical and logical locations within the network operator's / access provider's / service provider's telecommunications facilities where access to the content of communication and intercept related information is provided. The interception interface is not necessarily a single, fixed point.

interception measure: technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations.

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.

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted.

internal intercepting function: point within a network or network element at which the content of communication and the intercept related information are made available.

internal network interface: network's internal interface between the Internal Intercepting Function and a mediation device.

invocation and operation: describes the action and conditions under which the service is brought into operation; in the case of a lawful interception this may only be on a particular communication. It should be noted that when lawful

1 interception is activated, it shall be invoked on all communications (Invocation takes place either subsequent to or
2 simultaneously with activation.). Operation is the procedure which occurs once a service has been invoked.

3 NOTE 3: The definition is based on [8], but has been adapted for the special application of lawful interception,
4 instead of supplementary services.

5 **law enforcement agency:** organization authorized by a lawful authorization based on a national law to request
6 interception measures and to receive the results of telecommunications interceptions.

7 **law enforcement monitoring facility:** law enforcement facility designated as the transmission destination for the
8 results of interception relating to a particular interception subject.

9 **lawful authorization:** permission granted to a LEA under certain conditions to intercept specified telecommunications
10 and requiring co-operation from a network operator / access provider / service provider. Typically this refers to a
11 warrant or order issued by a lawfully authorized body.

12 **lawful interception:** see interception.

13 **lawful interception identifier:** identifier for a particular interception.

14 **location information:** information relating to the geographic, physical or logical location of an identity relating to an
15 interception subject.

16 **mediation device:** equipment, which realizes the mediation function.

17 **mediation function:** mechanism which passes information between a network operator, an access provider or service
18 provider and a handover interface, and information between the internal network interface and the handover interface.

19 **network element:** component of the network structure, such as a local exchange, higher order switch or service control
20 processor.

21 **network element identifier:** uniquely identifies the relevant network element carrying out the lawful interception.

22 **network identifier:** internationally unique identifier that includes a unique identification of the network operator,
23 access provider, or service provider and, optionally, the network element identifier.

24 **network operator:** operator of a public telecommunications infrastructure which permits the conveyance of signals
25 between defined network termination points by wire, by microwave, by optical means or by other electromagnetic
26 means.

27 **quality of service:** quality specification of a telecommunications channel, system, virtual channel, computer-
28 telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit
29 error rate, message throughput rate or call blocking probability.

30 **reliability:** probability that a system or service will perform in a satisfactory manner for a given period of time when
31 used under specific operating conditions.

32 **result of interception:** information relating to a target service, including the content of communication and intercept
33 related information, which is passed by a network operator, an access provider or a service provider to a law
34 enforcement agency. Intercept related information shall be provided whether or not call activity is taking place.

35 **service information:** information used by the telecommunications infrastructure in the establishment and operation of a
36 network related service or services. The information may be established by a network operator, an access provider, a
37 service provider or a network user.

38 **service provider:** natural or legal person providing one or more public telecommunications services whose provision
39 consists wholly or partly in the transmission and routing of signals on a telecommunications network. A service
40 provider needs not necessarily run his own network.

41 **SMS:** Short Message Service gives the ability to send character messages to phones. SMS messages can be MO
42 (mobile originate) or MT(mobile terminate).

43 **SMS Redirecting System: the NWO/AP/SvP system where SMS packets directed toward an interception subject are**
44 **processed for redirection instruction (e.g., SMS-GMSC).**

1 **target identity:** technical identity (e.g. the interception's subject directory number), which uniquely identifies a target
2 of interception. One target may have one or several target identities.

3 **target service:** telecommunications service associated with an interception subject and usually specified in a lawful
4 authorization for interception.

5 NOTE 4: There may be more than one target service associated with a single interception subject.

6 **telecommunications:** any transfer of signs, signals, writing images, sounds, data or intelligence of any nature
7 transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.

8
9

*** *Second Modification* ***

10

11 6.5.1.1 REPORT record information

12 The REPORT record is used to report non-communication related subscriber actions (events) and for reporting
13 unsuccessful packet-mode communication attempts.

14 The REPORT record shall be triggered when:

- 15 - the intercept subject's mobile station performs a GPRS attach procedure (successful or unsuccessful);
- 16 - the intercept subject's mobile station performs a GPRS detach procedure;
- 17 - the intercept subject's mobile station is unsuccessful at performing a PDP context activation procedure;
- 18 - the intercept subject's mobile station performs a cell, routing area, or combined cell and routing area update;
- 19 the intercept subject's mobile station sends an SMS-Mobile Originated (MO) communication. Dependent on
20 national requirements, the triggering event shall occur either when the 3G SGSN receives the SMS from the
21 target MS or, when the 3G SGSN receives notification that the SMS-Centre successfully received the SMS;
- 22 for GSM and UMTS systems deployed in the U.S., a REPORT record shall be triggered when the 3G SGSN
23 receives an SMS-MO communication from the intercept subject's mobile station;
- 24 - the intercept subject's mobile station receives a SMS Mobile-Terminated (MT) communication. Dependent on
25 national requirements, the triggering event shall occur either when the 3G SGSN receives the SMS from the
26 SMS-Centre or, when the 3G SGSN receives notification that the target MS successfully received the SMS;
- 27 for GSM and UMTS systems deployed in the U.S., a REPORT record shall be triggered when the 3G SGSN
28 receives an SMS-MT communication from the SMS-Centre destined for the intercept subject's mobile station;
- 29 - as a national option, a mobile terminal is authorized for service with another network operator or service
30 provider;
- 31 - unless otherwise prohibited by national requirements, an SMS Redirecting System shall intercept SMS data
32 packets redirected toward an intercept subject.

33

1

Table 6.3: GPRS Attach 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 GPRS Attach 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.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
failed attach reason	C	Provide information about the reason for failed attach attempts of the target subscriber.

2

3

Table 6.4: GPRS Detach 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 GPRS Detach 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.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.

4

1

Table 6.5: PDP Context Activation (unsuccessful) REPORT 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 either the: <ul style="list-style-type: none"> - 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	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify either the: <ul style="list-style-type: none"> - 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.
QOS	C	Provide to identify the QOS parameters.

2

3

Table 6.6: Location Information Update (with No PDP Context Active) 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 Location Information Update 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.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.

4

1

Table 6.7: SMS-MO and SMS-MT Communication 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 SMS 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.
SMS originating address	O	Provide to identify the originating and destination address of the SMS message
SMS destination address		
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
SMS	C	Provide to deliver SMS content, including header which is sent with the SMS-service.
service center address	C	Provide to identify the address of the relevant SMS-C server. If SMS content is provided, this parameter is optional.
SMS initiator	M	Indicates whether the SMS is MO, MT, or Undefined.

2

3

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.
ServingSGSN-Number	C	Provide to identify the E.164 number of the serving SGSN.
ServingSGSN-Address	C	Provide to identify the IP address of the serving SGSN.

4

5

6

Page: 2

[H1] [Document numbers](#) are allocated by the Working Group Secretary.

Page: 2

[H2] Enter the specification number in this box. For example, 04.08 or 31.102. Do not prefix the number with anything . i.e. do not use "TS", "GSM" or "3GPP" etc.

Page: 2

[H3] Enter the CR number here. This number is allocated by the 3GPP support team. It consists of at least three digits, padded with leading zeros if necessary.

Page: 2

[H4] Enter the revision number of the CR here. If it is the first version, use a "-".

Page: 2

[H5] Enter the version of the specification here. This number is the version of the specification to which the CR will be applied if it is approved. Make sure that the latest version of the specification (of the relevant release) is used when creating the CR. If unsure what the latest version is, go to <http://www.3gpp.org/specs/specs.htm>.

Page: 2

[H6] For help on how to fill out a field, place the mouse pointer over the special symbol closest to the field in question.

Page: 2

[H7] Mark one or more of the boxes with an X.

Page: 2

[H8] SIM / USIM / ISIM applications.

Page: 2

[H9] Enter a concise description of the subject matter of the CR. It should be no longer than one line. Do not use redundant information such as "Change Request number xxx to 3GPP TS xx.xxx".

Page: 2

[H10] Enter the source of the CR. This is either (a) one or several companies or, (b) if a (sub)working group has already reviewed and agreed the CR, then list the group as the source.

Page: 2

[H11] Enter the acronym for the work item which is applicable to the change. This field is mandatory for category F, B & C CRs for release 4 and later. A list of work item acronyms can be found in the 3GPP work plan. See http://www.3gpp.org/ftp/information/work_plan/ . The list is also included in a MS Excel file included in the zip file containing the CR cover sheet template.

Page: 2

[H12] Enter the date on which the CR was last revised. Format to be interpretable by English version of MS Windows ® applications, e.g. 19/02/2002.

Page: 2

[H13] Enter a single letter corresponding to the most appropriate category listed below. For more detailed help on interpreting these categories, see the Technical Report [21.900](#) "TSG working methods".

Page: 2

[H14] Enter a single release code from the list below.

Page: 2

[H15] Enter text which explains why the change is necessary.

Page: 2

[H16] Enter text which describes the most important components of the change. i.e. How the change is made.

Page: 2

[H17] Enter here the consequences if this CR was to be rejected. It is necessary to complete this section only if the CR is of category "F" (i.e. correction).

Page: 2

[H18] Enter the number of each clause which contains changes.

Page: 2

[H19] Tick "yes" box if any other specifications are affected by this change. Else tick "no". You MUST fill in one or the other.

Page: 2

[H20] List here the specifications which are affected or the CRs which are linked.

Page: 2

[H21] Enter any other information which may be needed by the group being requested to approve the CR. This could include special conditions for it's approval which are not listed anywhere else above.

Page: 2

[H22] This is an example of pop-up text.