ETSI TR 141 033 V12.0.0 (2014-10)

Digital cellular telecommunications system (Phase 2+);
Lawful Interception requirements for GSM
(3GPP TR 41.033 version 12.0.0 Release 12)

Reference
RTR/TSGS-0341033vc00

Keywords
GSM, SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This Technical Report describes the interface requirements of a mechanism which will deliver intercept from GSM mobile stations, including both speech and data product.

The stage 1 description of Lawful Interception will be specified in 3GPP TS 42.033.

The stage 2 description of Lawful Interception will be specified in 3GPP TS 43.033.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM MoU Association document SG09, June 1995

[3] The European Union Council Resolution reference: 'International Requirements for The Lawful Interception of Telecommunications' (January 1995), (JAI_24_Rev 2, 8197/2/95)

[4] ITU-T Recommendation G.711: "Pulse Code Modulation (PCM) of voice frequencies".

3 Definitions and abbreviations

3.1 Definitions

A-party: The originating party number.

B-Party: The called party number.

C-Party: A diverted-to party number.

Network related data: Data associated with a call, excluding the actual product such as speech or data.

Product: Data sent or received by a mobile user such as speech or fax or data.

RF: Requesting Function; mechanism owned by an interception authority to set-up and receive the interception product.

Target: An MSISDN (or sometimes IMSI) which is to be made the subject of an interception.

WAN: Wide Area Network, or interconnected LANs providing a computer data network between PLMN elements.

3.2 Abbreviations

In addition to those mentioned below, abbreviations used in this report are listed in GSM 01.04.

CGI	Cell Global Identity
FTAM	File Transfer Access and Management
GSM	Global System for Mobile communications
HLR	Home Location Register
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
LEA	Law Enforcement Agency
MoU	Memorandum of Understanding
MoU-SG	The MoU Security Group
MS	Mobile Station
MSC	Mobile-services Switching Centre
MSISDN	Mobile Station International ISDN Number
PLMN	Public Lands Mobile Network
PSTN	Public Switched Telephone Network
RF	Requesting Function
SMG	Special Mobile Group
SMG-SG	The ETSI TC SMG Security Group
SMS	Short Message Service
SS	Supplementary Service
SS7	Signalling System No. 7
UDI	Unrestricted Digital Interface (64 kbit/s ISDN data)
WAN	Wide Area Network

4 Telecom interception requirements

4.1 Background

Previous MoU-SG specification SG09 has defined the interception of GSM in general terms. This report will define the X-interface to the Public Lands Mobile Network (PLMN) to support interception.

4.2 Background technical requirements

This report describes the interface to the PLMN, defined as the X-interface. The interface is illustrated in figure 1.

The X-interface is between the Requesting Function (RF) and the PLMN. It is divided into three logical parts:

1) The X1-interface is used to present commands to the PLMN, from an administration centre. This interface is part of the switch management capability, usually over an X.25 interface or Wide Area Network (WAN).

2) The X2-interface receives "Network related data" from the Mobile-services Switching Centre (MSC), in switch management or file output format, probably over an X.25 network or WAN. Alternatively, it may be sent in combination with the ISDN product in the X3-interface described below.

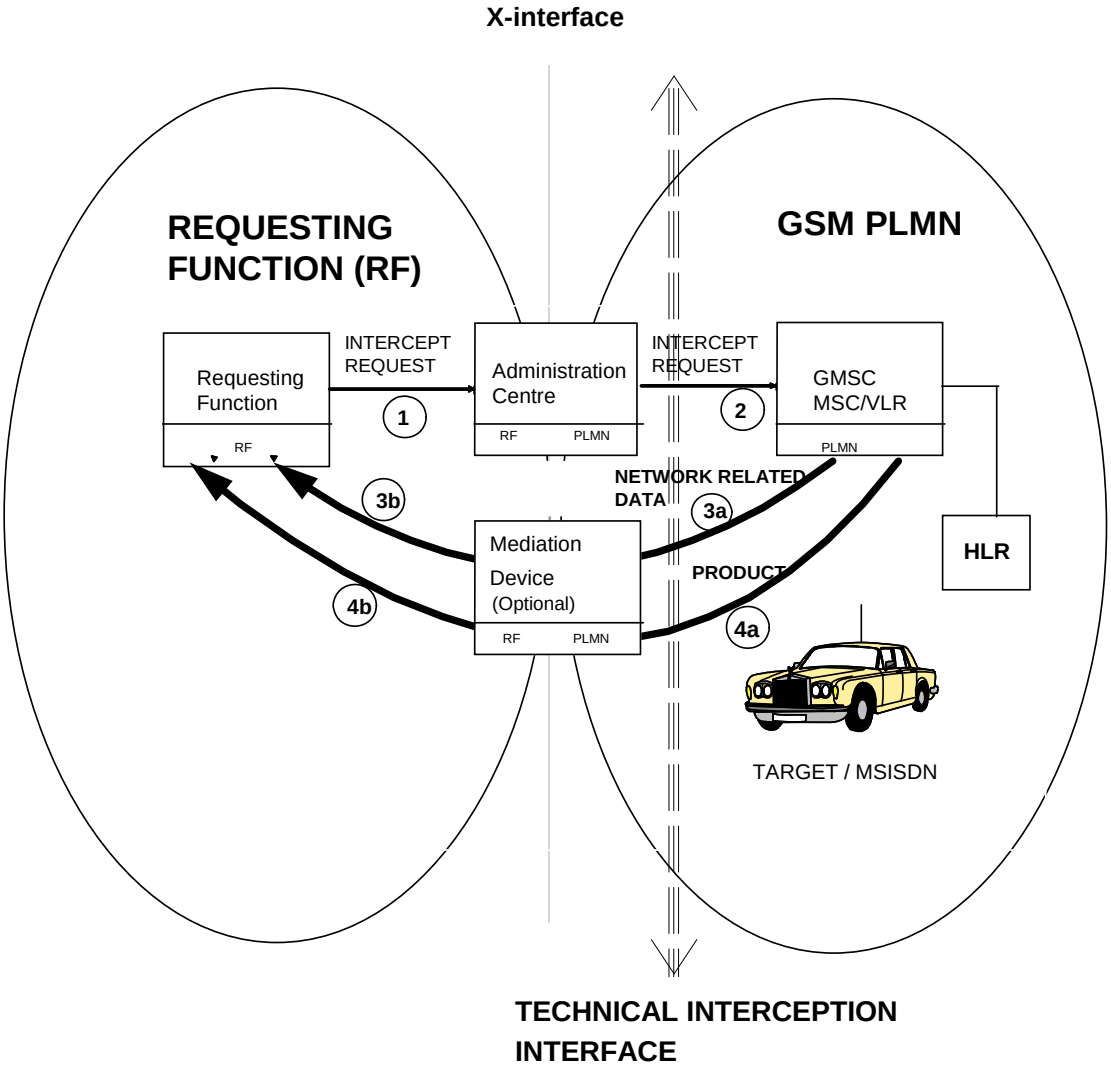
3) The X3-interface receives "Product" (mobile user's speech and data) from the MSC. It is contained within one or more 64 kbit/s channels.

The objective of the X-interface is to allow a standard to be created so that a PLMN consisting of MSCs from different manufacturers may be combined. Although the X1-interface commands may be slightly different for each manufacturer, it should be possible to create a single intelligent system to manage the interface at a low cost, capable of managing all different manufacturers implementations.

Similarly, the outputs defined in the X2 and X3 parts of the X-interface should be capable of processing by the same "Requesting Function".

5 General technical requirements for legal interception in GSM/PCN networks

Figure 1 shows the general system for interception. Technical interception is implemented within a PLMN by special functionality on network elements; primarily the MSCs/VLRs and Home Location Registers (HLRs). Use of the function and delivery of the "Product" from the target is defined by the X-interface.



NOTES: 1: Paper or direct request
2: Electronic request
3a and 3b:"Network related data" } Items 3 & 4 may be combined into
4a and 4b:"Product", such as speech and mobile data } a common transport mechanism
X1 = Interface 2
X2 = Interface 3a
X3 = Interface 4a

Figure 1: General specification for interception

5.1 General principles

The PLMN network should provide access to the "Product" and the "Network related data" of the mobile targets by means of the X-interface. As a minimum requirement the target should be identifiable by the Mobile Station International ISDN Number(s) (MSISDN(s)). There should be provision for unambiguous connection of the "Product" and the "Network related data" to the remote Requesting Functions (RFs). A secure means of administration of the service should be available to the PLMN operator and/or appropriate requesting functions in accordance with national laws.

5.2 Capability

The following minimum capabilities are required:

- it will be possible to support as "Product": speech, user data, fax and SMS, from the interception function;
- roamers from other PLMNs may also be targets;
- mobile originating, mobile terminating, and diversion or multiparty calls will be capable of interception;
- location information.

5.3 Operation

The interception function shall not alter the operation of a target's service or provide indication to any party involved in the call. Output product should be in "clear" form - no GSM radio interface or PLMN generated radio interface encoding or encryption is present (the PLMN cannot remove subscriber encryption). The service should not alter the standard functions of GSM network elements. The "Product" and the "Network related data" shall be delivered as near as possible to the time the call is made.

6 Summary of information passed over the X-interface

6.1 Intercept request, set-up details for target (X1)

Data to be stored for target mobile station:

- MSISDN, or optionally the International Mobile Subscriber Identity (IMSI);
- Connection address for the Requesting Function (RF);
- Type of output:
  - "Product" or "Network related data" or both.

6.2 Output (from PLMN to RF)

6.2.1 X2, "Network related data"

- unique reference number for MSC call event;
- MSISDN, (and optionally IMSI, International Mobile station Equipment Identity (IMEI));
- type of call (i.e. originating or terminating);
- A-party number, B-party number;
- C-party (diversion or multiparty numbers);
- start time of call;

- finish time of call (or call duration);
- location information (Cell Global Identity (CGI));
- teleservice or bearer service used, Supplementary Service (SS) used;
- call completion message (giving call release reason).

NOTE 1: The above list is a guide to the information which may be provided by the MSC, but not all the items will be available for every call type.

NOTE 2: Connected party numbers (A-, B- and C-party) may only be available for calls completely contained within ISDN based networks.

NOTE 3: Appropriate "Network related data" should also be output from the MSC for unsuccessful call attempts.

6.2.2 X3, "Product" (when requested)

- "Product": speech, user data, fax, or Short Message Service (SMS);

NOTE: SMS text may be forwarded to the RF by means of the X2-interface mechanism.

- Unique reference number for MSC call event.

7 Interception mechanisms

7.1 Intercept Request Function (X1)

The following basic target administration functions are to be supported:

ADD

- flag a target by MSISDN, or optionally IMSI;
- X2 delivery address, e.g. X.25 or WAN address;
- X3 "Product" delivery address, E.164 address;
- select "Network related data" alone, or "Network related data" and "Product".

REMOVE

- de-flag a target.

SHOW

- list one or more targeted MSISDNs.

7.2 Interception output, "Product" and "Network related data"

The "Product" of the target and connected parties will be additionally connected to an output port of the MSC (for example by means of a three party bridge) which routes the "Product" to an RF, possibly via an optional mediation device. The mediation device provides interface conversion (if necessary) between the PLMN X2- and X3-interfaces and the RF.

Different RFs may require the same information. The mediation device may simultaneously provide multiple output of "Product" and "Network related data" regarding one MSISDN to more than one RF. No information should be passed to the RF about which other RFs are using the information.

Some types of call may require multiple links to the RF, for example Unrestricted Digital Interface (UDI) data services, and optionally in-band data (3.1 kHz) services.

7.3 Delivery mechanisms

7.3.1 Network related data (see subclause 6.2.1)

There are two mechanisms proposed for delivery of "Network related data"; these are:

- ISDN user to user signalling; or
- MSC/HLR file format output, (via an X.25 network using File Transfer Access and Management (FTAM), or WAN).

7.3.2 Product

The "Product" should be passed in ISDN format: i.e. for voice according to ITU-T Recommendation G.711, A-law encoding in one or more 64 kbit/s channels.

For UDI data the output is transparently transmitted in two 64 kbit/s channels.

"Product" (speech and data) should be routed to the RF by E.164 address.

SMS product, exceptionally, will probably be transported according to the mechanism selected for "Network related data".

7.4 Administration mechanism

A secure means of administrating the service by the PLMN operator and/or requesting function is necessary. This mechanism should provide for the addition and removal of subscribers from the marked list by authorised personnel, and a show marked MSISDNs command. Access should be policed by appropriate authentication and audit procedures.

7.4.1 Security

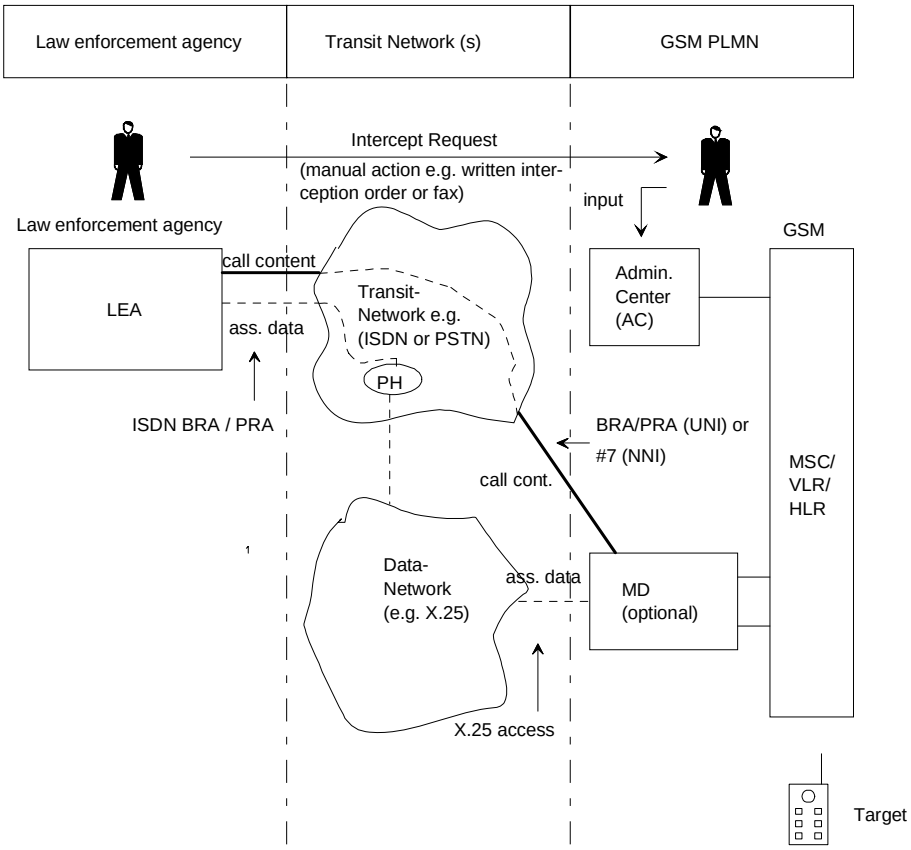
The intercept function must only be capable of being used by authorised personnel. Security functions should provide the following capability (to national requirements):

- security administration to control nominated user access to the function;
- secure data network arrangements between administration centre and MSC/HLR for the intercept function commands;
- security mechanisms to control access to the function should be provided at both the administration centre and MSC/HLR elements;
- secure network arrangements between MSC/HLR and the RF to ensure that "Network related data" and "Product" only reach the appropriate authorities;
- it should not be possible for non authorised personnel to read the target list of MSISDNs;
- an audit log of use of the intercept function (successful or failed should be maintained, accessible only to authorised users;
- no indication whatsoever should be given to any PLMN operative (except authorised personnel) or the target or customer that the intercept function has been invoked on the target.

7.5 Merging and processing of "Product" and "Network related data"

This aspect of the service is not addressed by this report. It is a matter of discussion between relevant authorities and the PLMN operator as to responsibilities for the provision of the mediation device, and the means of handling product at the RF.

Annex A:
Diagram of an example interception technical implementation



Annex B:
GPRS and Lawful Interception

B.1 Introduction

B.1.1 Overview

The general system for lawful interception in GSM PLMN is similar in both circuit and packet switched services. Technical interception is implemented within a PLMN by special functionality on network elements; primarily the MSCs/VLRs, the GPRS Support Nodes (GSNs) and HLRs. The objective of the X-interface is to allow a standard to be created so that a PLMN consisting of different network elements (GSN, MSC/VLR, HLR) from different manufacturers may be combined.

The interception mechanisms are similar in both circuit and packet switched services, but there are few things that require modifications: The GPRS service brings packet data specific requirements to the information passed over the X-interface. Also the definition of target identity is different in the GPRS service.

B.1.2 Scope

The scope of this annex is to introduce GPRS specific X-interface and identification requirements to this lawful interception report.

B.2 Target Identity

A GPRS subscriber identified by an IMSI (or an MSISDN) shall have a network layer address(es) temporarily and/or permanently associated with it that conforms to the standard addressing scheme of the respective network layer service used. GPRS shall provide a means to interwork with external data networks. The GPRS operator provides an appropriate Packet Data Protocol (PDP) address to the external data network for the subscriber as part of the GPRS subscription. That address can be either dynamic (e.g. the user's IP address is allocated from a pool of unused IP addresses every time the subscriber activates the access to an IP network) or static (e.g. a certain IP address is permanently allocated to a particular subscriber).

B.3 Summary of Information Passed over the X-interface

B.3.1 Intercept Request, Set-up Details for Target (X1)

Data to be stored for target GPRS mobile station:

- IMSI, or MSISDN;
- Connection address for the Requesting Function (RF);
- Type of output:
  - "Product" or "Network related data" or both.

B.3.2 Output (from PLMN to Requesting Function)

B.3.2.1 X2, "Network related data"

- unique reference number for PDP context activation;
- IMSI, (and optionally MSISDN, International Mobile station Equipment Identity (IMEI));
- type of packet data transfer (i.e. originating or terminating);
- A-party PDP address, B-party PDP address;
- C-party (diversion or multiparty PDP addresses);
- time of PDP context activation;
- time of PDP context deactivation (or PDP context duration);
- location information (Cell Global Identity (CGI));
- teleservice or bearer service used, Supplementary Service (SS) used;
- PDP used;
- call completion message (giving call release reason);
- timestamp (see subclause B.3.2.2).

The above list is a guide to the information which may be provided by the GPRS service, but not all the items will be available for every call type. Appropriate "Network related data" should also be output from the GPRS service for unsuccessful packet data transfer attempts. For certain protocols like IP, the sender and receiver addresses are always included in the IP packet and do not need to be part of "Network related data".

B.3.2.2 X3, "Product" (when requested)

- "Product": user data or Short Message Service (SMS);
- unique reference number for PDP context activation;
- timestamp on each PDP packet.

At the law enforcement agency the data packets and the "Network related data" can be accurately correlated by copying the timestamp in the data product packet into the timestamp field of the "Network related data" packet. In addition to the timestamp the unique reference number or user identification may be required for correlation. All packet data transmissions to or from the intercept target may be subject to interception regardless of their outcome. For example, when an SMS packet to an MS is intercepted, it is not known whether the packet was actually received by the MS.

Annex C:
Change history

Change history						
SMG#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
						No Phase 1 version
SMG#18	01.33		-		1.0.0	To SMG#18 for information
SMG#19	01.33	2.0.0	-	R96	5.0.0	TC TR approved by SMG#19
01-1997	01.33	5.0.0	-	R96	5.0.1	TC TR converted to ETR 363
03-1998	01.33		A001r1	R98	7.0.0	CR 01.33-A001r1 (GPRS) approved by SMG#25 TR renamed to GSM 01.33 (as agreed by SMG#22) Report converted to version 7.0.0 because work item is related to Release 98
04-2000	01.33	7.0.0	-	R99	8.0.0	Release 99 version
Change history						
TSG SA#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
SP-11	01.33	8.0.0	-	Rel-4	41.033 v 4.0.0	Upgrade to Release 4 (3GPP numbering)
		4.0.0			4.0.1	May 2001: change from TS to TR layout.
SP-16	41.033	4.0.1	-	Rel-5	5.0.0	June 2002: Upgrade to Release 5
SP-26	41.033	5.0.0	-	Rel-6	6.0.0	December 2004: Upgrade to Release 6
SP-36	41.033	6.0.0	-	Rel-7	7.0.0	June 2007: Upgrade to Release 7
SP-42	41.033	7.0.0	-	Rel-8	8.0.0	December 2008: Upgrade to Release 8
SP-46	41.033	8.0.0	-	Rel-9	9.0.0	December 2009: Upgrade to Release 9
2011-03	41.033	9.0.0	-	Rel-10	10.0.0	Update to Rel-10 version (MCC)
2012-09	-	-	-		11.0.0	Update to Rel-11 version (MCC)
2014-09	-	-	-		12.0.0	Update to Rel-12 version (MCC)

History

Document history		
V12.0.0	October 2014	Publication