ETSI
TECHNICAL
REPORT

ETR 363

January 1997

Source: ETSI TC-SMG

Reference: DTR/SMG-101020Q

ICS: 33.020

Key words: Digital cellular telecommunications system, Global System for Mobile communications (GSM)

GSM®

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Digital cellular telecommunications system;
Lawful Interception requirements for GSM
(GSM 10.20 version 5.0.1)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Special Mobile Group (SMG) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

Blank page

1 Scope

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

2 References

This ETR incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETR only when incorporated in it by the amendment or revision. For undated references, the latest edition of the publication referred to applies.

[1]   GSM 01.04 (ETR 100): "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 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.

X-interface

TECHNICAL INTERCEPTION
INTERFACE
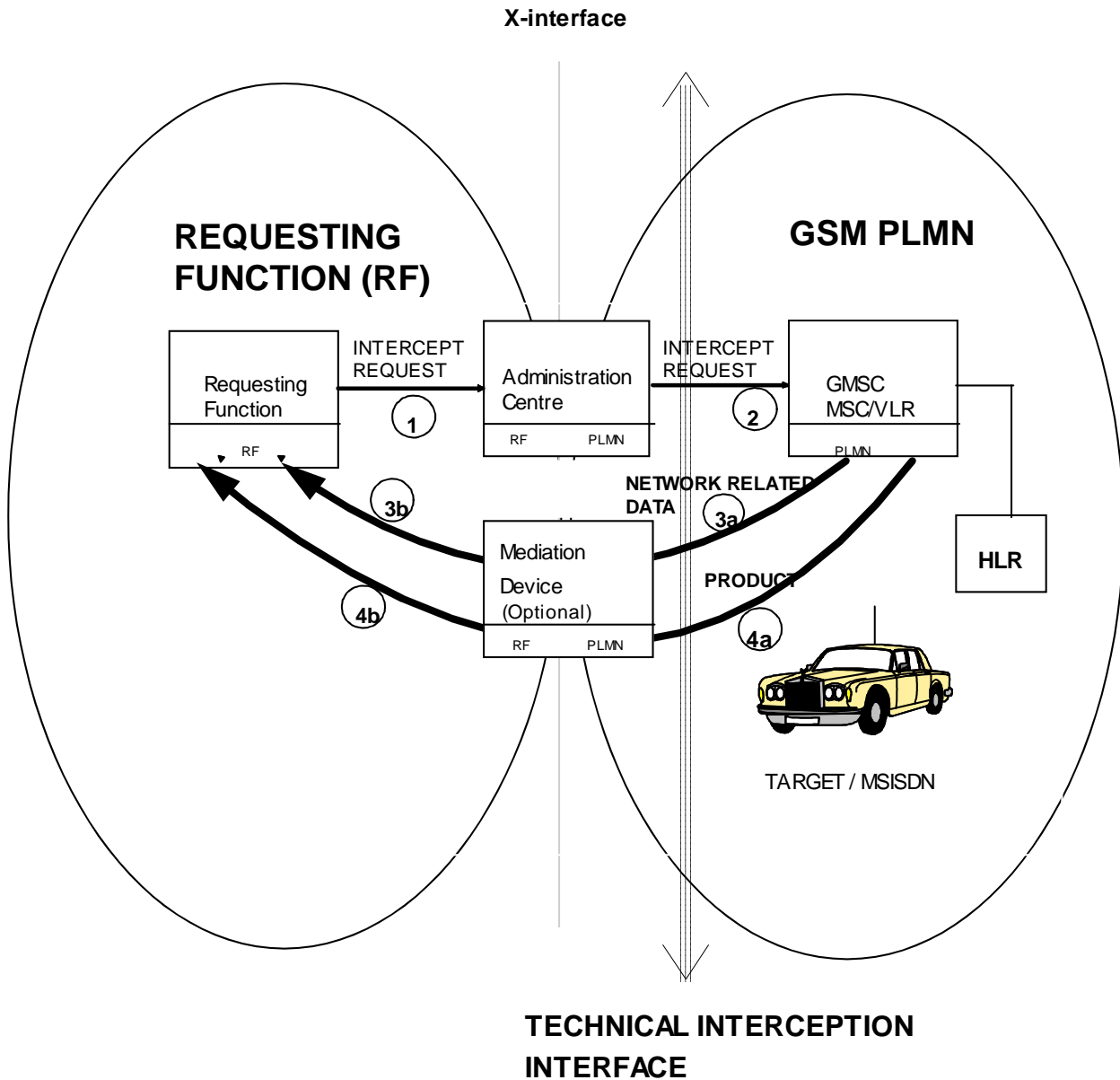
NOTES: 1: Paper or direct request
          2: Electronic request
          3a and 3b: Network related data   }Items 3 & 4 may be
          4a and 4b: Product, such as speech and mobile data   }combined into a common
                                                                 }transport mechanism

          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 network related data of the mobile targets by means of the X-interface. As a minimum requirement the target should be identifiable by Mobile Station International ISDN Number(s) (MSISDN(s)). There should be provision for unambiguous connection of the product and 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 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 (by means of a three party bridge for example) 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 authorized 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 authorized 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 authorized 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 authorized users;

- no indication whatsoever should be given to any PLMN operative (except authorized 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
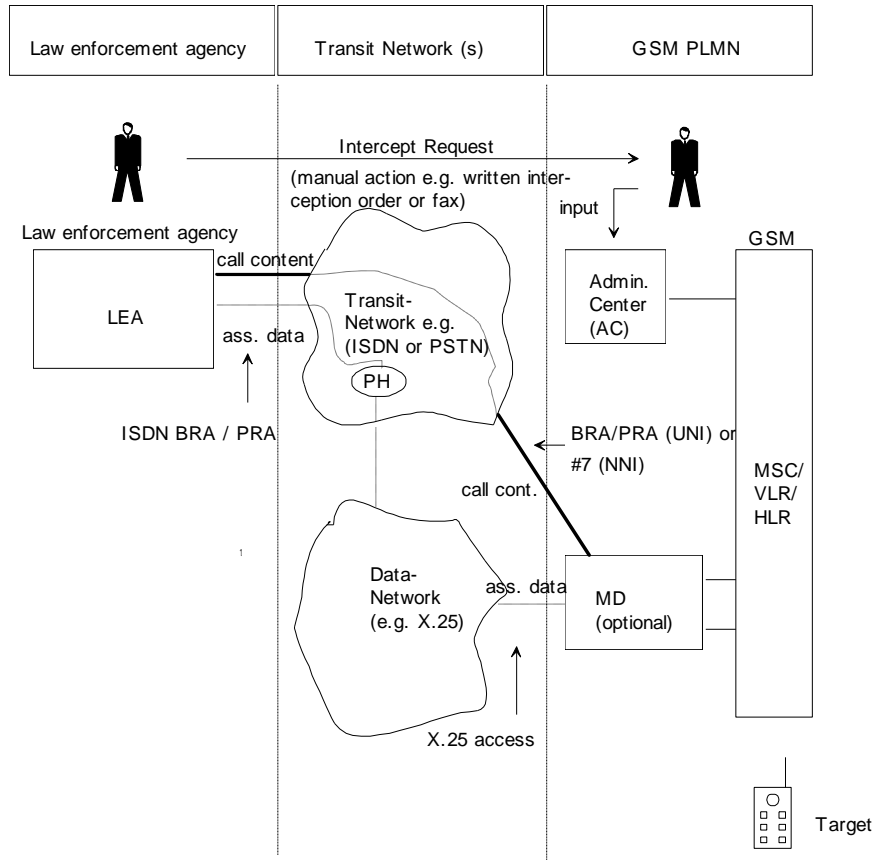
History

Document history	
January 1997	First Edition