

ETSI TS 142 033 V13.0.0 (2016-01)



**Digital cellular telecommunications system (Phase 2+);
Lawful Interception;
Stage 1
(3GPP TS 42.033 version 13.0.0 Release 13)**



Reference

RTS/TSGS-0342033vd00

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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 (<https://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 Specification (TS) 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**", "**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

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	5
1 Scope	6
2 References	6
3 Definitions and abbreviations.....	6
3.1 Definitions	6
3.2 Abbreviations	7
4 Description	7
4.1 General principle	7
4.2 Applicability to telecommunications services	7
4.2.1 Tele and bearer services (TS/BS)	7
4.2.2 Supplementary services (SS)	7
4.2.2.1 General	7
4.2.2.2 Impact	7
4.2.2.3 Intercept of forwarding calls - option.....	8
4.2.2.4 Intercept of calls placed on HOLD (call waiting and multi party services) - option.....	8
4.2.2.5 Network operator specific services	8
4.2.3 Other activities.....	8
5 Normal Operation.....	8
5.1 Intercept administration.....	8
5.1.1 Activation	8
5.1.2 Deactivation.....	8
5.1.3 Security	8
5.1.3.1 Password rules.....	9
5.1.3.2 Log files	9
5.2 Intercept invocation	9
5.2.1 General.....	9
5.2.1.1 Invocation events for lawful interception.....	9
5.2.1.2 Invocation of interception regarding normal GSM service	9
5.2.1.3 Correlation of information and product.....	10
5.2.2 Intercept related information.....	10
5.2.2.1 Intercept related information events.....	10
5.2.2.2 Intercept related information provided to the LEA	10
5.2.2.3 Delivery of intercept related information	11
5.2.3 Intercept product.....	11
5.2.3.1 Speech and single channel circuit switched data/fax.....	11
5.2.3.2 Delivery of intercept product	11
5.2.3.3 SMS.....	11
5.2.4 Correlation between intercept product and intercept related information.....	11
5.2.5 Security related to intercept invocation	11
5.2.6 Warrant Reference Number	11
6 Exceptional procedures	12
7 Interworking considerations	12
8 Charging aspects	12
8.1 Charging principles	12
8.2 Charging characteristics	12
8.2.1 Activation of the target	12
8.2.2 Deactivation of the target.....	13

8.2.3	Intercept invocation	13
9	Minimum Service Requirements.....	13
Annex A (Normative):	GPRS and Lawful Interception	14
A.1	Introduction	14
A.2	Intercept Invocation.....	14
A.2.1	Intercept related information events	14
A.2.2	Intercept related information provided to the LEA.....	14
A.2.3	GPRS intercept product	15
A.3	Interworking considerations.....	15
Annex B (informative):	Change History	16
History		17

Foreword

This Technical Specification 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 Specification provides the stage 1 description for a lawful interception function to be implemented in a given GSM PLMN in order for a network operator to be able to fulfil national lawful requirements. It shall be noted that national variation may exist but it is not the intention for this specification to encompass all of them. The purpose of this specification is to cover the options which may be selectable according to national regulations or as required by the GSM PLMN operator in co-operation with their suppliers.

In the preparation of this specification general reference was made to the European Union Council Resolution, January 1995: "International Requirements for the Lawful Interception of Telecommunications".

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] The European Union Council Resolution reference: 'International Requirements for The Lawful Interception of Telecommunications' (January 1995), (JAI_24_Rev 2, 8197/2/95)
- [3] CCITT Recommendation G.711: "Pulse Code Modulation (PCM) of voice frequencies".

3 Definitions and abbreviations

3.1 Definitions

Target: is the subject of an interception. Different identities might be used (i.e. Mobile Station International ISDN number (MSISDN), optionally International Mobile Subscriber Identity (IMSI) or International Mobile Equipment Identity (IMEI)).

Interception Area: is a subset of the Public Land Mobile Network (PLMN) service area comprised of a set of cells which define a geographical zone.

Intercept product: data sent or received by the target, such as speech, fax or data generated by the users of the telecommunication services.

Intercept related information: collection of information associated to telecommunication services involving the target.

Law enforcement agency: a body authorized by law to carry out telecommunication interceptions.

Location Dependent Interception: is interception within a PLMN service area that is restricted to one or several Interception Areas (IA).

Warrant reference number: is a reference number that links a specific intercept activity to an agency's lawful Interception request.

3.2 Abbreviations

In addition to those below abbreviations used in the specification are listed in GSM 01.04.

LEA:	Law Enforcement Agency
IA:	Interception Area

4 Description

4.1 General principle

GSM Public Lands Mobile Network (PLMN) shall provide access to the intercept product and the intercept related information of the mobile target on behalf of Law Enforcement Agencies (LEAs).

A mobile target in a given PLMN can be a subscriber of that PLMN, or a subscriber of another PLMN. The intercept product and the related information can only be delivered for activities on that given PLMN.

An unambiguous correlation shall be established between the intercept related information and the intercept product. The intercept related information and the intercept product shall be delivered in as near real time as possible.

Location Dependent Interception allows a PLMN to service multiple interception jurisdictions within its service area. Multiple law agencies with their own interception areas can be served by the PLMN. All the information or rules given for interception within a PLMN apply to interception within an IA when Location Dependent Interception is invoked. A target may be marked in one or more different IAs within the same PLMN. Interception is not required nor prohibited by this standard when Location Dependent Interception is active and the location of the target subscriber is not known or available.

Additional GPRS interception requirements are contained in annex A.

4.2 Applicability to telecommunications services

4.2.1 Tele and bearer services (TS/BS)

All teleservices and bearer services are subject to interception of the target.

Interception is applicable to Short Message Service (SMS) point-to-point, but not SMS Cell Broadcast (SMSCB).

Impact of application to the Voice Group Call Service (VGCS) and the Voice Broadcast Service (VBS) is for further study (FFS).

4.2.2 Supplementary services (SS)

4.2.2.1 General

It shall be possible to report any activities regarding supplementary services to the LEA. It may be a national or operator/supplier option to implement this function.

4.2.2.2 Impact

The application of the following supplementary services has no impact on the interception function: Calling Line Identity Presentation/Calling Line Identity Restriction (CLIP/CLIR), Connected Line Identity Presentation/Connected Line Identity Restriction (COLP/COLR), Call Barring (CB) services, Advice of Charge (AoC) services, Closed User Group (CUG), Completion of Calls to Busy Subscriber (CCBS).

4.2.2.3 Intercept of forwarding calls - option

Activation by the target of any Call Forwarding (CF) service, Call Deflection (CD), or Explicit Call Transfer (ECT) shall result in the capability to intercept the forwarded, diverted or transferred product.

It may be a national or operator/supplier option which of these are implemented.

4.2.2.4 Intercept of calls placed on HOLD (call waiting and multi party services) - option

In some countries it is a national requirement that when the target puts other parties on HOLD (call waiting (CW) and multi party services (MPTY) the other parties product will be interrupted. When the other parties rejoin the call, the intercept product shall be reconnected.

4.2.2.5 Network operator specific services

Impact on a network operator's specific services is not covered in this specification.

4.2.3 Other activities

Location information in the format of cell global identity (CGI) should be available with call related activities. Conversion to other formats of location information (e.g. latitude/longitude) is not covered by this specification. It is a matter of national or operator/supplier option whether location information shall be provided in connection with non call related activities, e.g. location update.

5 Normal Operation

5.1 Intercept administration

A secure means of administrating the service by the PLMN operator and/or intercept requesting entity is necessary. This mechanism shall provide means to activate, deactivate, show, or list targets in the GSM PLMN as quick as technically possible. The function shall be policed by appropriate authentication and audit procedures.

The administration function shall allow specific IAs to be associated with target subscribers when Location Dependent Interception is being used.

5.1.1 Activation

As a result of the activation it shall be possible to request for the specified target either the intercept product, the intercept related information or both, and the LEA destination addresses for the delivery of the intercept product and intercept related information if required. These shall be selectable on a PLMN basis according to national options.

5.1.2 Deactivation

As a result of deactivation it shall be possible to stop all interception activities for the specified target.

5.1.3 Security

The intercept function shall only be accessible by authorised personnel.

No indication shall be given to any PLMN staff except authorised personnel that the intercept function has been activated on a target.

5.1.3.1 Password rules

Password rules are specially defined for local and remote administrative and maintenance access. More specifically:

- The minimum length of a password shall be eight characters;
- The password shall be valid for a limited number of days. e. g. 30 days;
- The system shall support password history, i.e. the last e.g. 20 passwords are not allowed.

5.1.3.2 Log files

An audit log of the use of the intercept function (successful or failed) shall be maintained, accessible only to authorised users.

It shall be configurable to maintain a log file for all Lawful Interception commands or intercept relevant events on all network elements. The following events shall be logged with both time and date stamp and if available User-ID, Target-ID etc.:

- activation, deactivation and interrogation of lawful interception;
- attempt of unauthorised access of lawful interception;
- communication failures at network element interfaces;
- interception system failures;
- maintenance work.

The log file shall be password protected.

The log file shall be maintainable separately from other non intercept operations (read, delete, download).

The log file shall be cyclic deleted. The policy of how the log file is deleted is a matter of national option.

The log file shall be divided from regular operation of the network elements. Lawful Interception commands shall not be logged at any other file.

5.2 Intercept invocation

5.2.1 General

5.2.1.1 Invocation events for lawful interception

Lawful interception is invoked when:

- a voice call is requested - either originated from or terminated to the target;
- a circuit switched data call is requested - either originated from or terminated to the target;
- location information related to the subscriber is modified by the subscriber attaching or detaching from the network, or if there is a change in location, (see subclause 4.2.3);
- an SMS transfer is requested - either originated from or terminated to the target.

5.2.1.2 Invocation of interception regarding normal GSM service

The invocation of lawful interception shall not alter the operation of a target's services or provide indication to any party involved in communication with the target. Lawful interception shall not alter the standard function of GSM network elements. If lawful interception is activated during a call, the call shall not be intercepted. If lawful interception is deactivated all ongoing intercept activities shall continue till they are completed.

5.2.1.3 Correlation of information and product

When lawful interception is invoked, intercept related information and/or intercept product shall be sent to the LEA. Where both intercept related information and intercept product are sent to the LEA, then these two types of information shall be able to be correlated by the LEA, and they should be sent to the LEA in as near real time as possible.

5.2.2 Intercept related information

This subclause describes the service requirements for the provision of intercept related information when the target is using the following basic services:

5.2.2.1 Intercept related information events

Intercept related information concerning call progress may be provided to the LEA when the target is using the following basic services:

- telephony - teleservice 11;
- alternate speech and facsimile - teleservice 61;
- automatic facsimile group 3 - teleservice 62;
- data services - bearer services 2x, 3x;
- alternate speech and data - bearer service 61;
- speech followed by data - bearer service 81.

The following intercept related information events concerning call progress may, if applicable to the Tele Service/Bearer Service (TS/BS) and available, be provided to the LEA:

- the call establishment attempt;
- the answer of the call;
- the disconnecting of the call;
- changes of location of the target.

For the case of an SMS transaction the intercept related information is provided in conjunction with the SMS intercepted product to the LEA (see subclause 5.2.3.3).

5.2.2.2 Intercept related information provided to the LEA

The specific information provided by the intercept related information events will vary depending upon: the specific event, and the availability of information in a particular scenario (for example when interworking with network of different capabilities - i.e. non-ISDN networks).

A list of the type of information that may be provided to the LEA by intercept related information events, includes:

- an activation reference identity;
- the target identity which has been intercepted (e.g. MSISDN, IMSI, IMEI if applicable);
- called number;
- calling number;
- numbers related to forwarding and multi party calls;
- type of service used;
- location information of target (Cell Global Identity);
- time of event;

- call release reason.

5.2.2.3 Delivery of intercept related information

Intercept related information shall be delivered to the LEA using the specific address information that has been provided as part of the activation of the service.

5.2.3 Intercept product

5.2.3.1 Speech and single channel circuit switched data/fax

This subclause describes the service requirements for the provision of intercept product when the target is using the following basic services:

- telephony - teleservice 11;
- alternate speech and facsimile - teleservice 61;
- automatic facsimile group 3 - teleservice 62;
- data services - bearer services 2x, 3x;
- alternate speech and data - bearer service 61;
- speech followed by data - bearer service 81.

Intercept product should be in "clear" form - no GSM radio interface or PLMN generated radio interface encoding or encryption should be present, (the PLMN can not remove subscriber encryption). Intercept product shall be maintained during handover.

5.2.3.2 Delivery of intercept product

Intercept product shall be delivered to the LEA using the specific address information provided as part of the lawful intercept activation.

Any additional delay in setting up the call caused by the invocation of lawful interception should not be noticeable to the target or other users on the call.

5.2.3.3 SMS

Intercept product for SMS is sent to the LEA along with the intercept related information for both SMS mobile originated and SMS mobile terminated.

5.2.4 Correlation between intercept product and intercept related information

Intercept product and intercept related information shall be presented to the LEA in a way that allows for accurate correlation between these two components.

5.2.5 Security related to intercept invocation

There shall be arrangements between the GSM PLMN and the LEA to ensure uncorrupted and confidential delivery of information and product related to lawful interception.

5.2.6 Warrant Reference Number

The Warrant Reference Number may be used by an LEA for an indirect identification of a specific intercept activity.

6 Exceptional procedures

When a failure occurs while establishing the connection towards the LEA to transfer the intercept product this shall not result in any interruption of the ongoing telecommunications service. No further specific requirements apply for the intercept product in the GSM PLMN.

When failure occurs while trying to provide the interception related information it shall be temporarily stored in the GSM PLMN and some further attempts shall be made to deliver it if available.

7 Interworking considerations

While it is recognised that speech encoding in CCITT G.711 format presently does not raise any problem, the transmission of GSM encoded speech in the future - speech transmission for mobile to mobile calls without transcoding - will create difficulties to provide the product in the correct format to the LEA. It shall be noted that forcing transcoding for the intercepted calls will result in a noticeable and perceived systematic degradation in the speech quality for the mobile parties.

8 Charging aspects

8.1 Charging principles

The PLMN may require to raise charges for lawful interception. Charging may be based on one or more of the following:

- use of network resources;
- activation and deactivation of the target; or
- every intercept invocation.

The PLMN shall be capable of producing intercept charging data. It shall be possible to produce this data in such a way that access by non authorised personnel or the target is precluded.

8.2 Charging characteristics

Some of parameters listed below might not be applicable in specific GSM PLMNs:

8.2.1 Activation of the target

- Activation reference;
- Mobile target identity;
- Date of activation;
- Time of activation;
- Destination address;
- Specified output(s);
- Network identity.

8.2.2 Deactivation of the target

- Activation reference;
- Mobile target identity;
- Date of deactivation;
- Time of deactivation;
- Network identity.

8.2.3 Intercept invocation

- Activation reference;
- Mobile target identity;
- Date of activity;
- Start time of activity;
- Stop time or duration of the activity;
- Service type, Speech, data, SMS.

9 Minimum Service Requirements

Quality of service, capacity and reliability are the subject of bilateral agreement between the Regulation (Licensing) authorities and the GSM PLMN operator.

Annex A (Normative): GPRS and Lawful Interception

A.1 Introduction

In GPRS interception is applicable to Point-To-Point (PTP) services, Point-To-Multipoint Group call (PTM-G) and Short Message Service (SMS). Interception is not applicable to Point-To-Multipoint Multicast (PTM-M).

A.2 Intercept Invocation

Lawful interception is invoked when a GPRS PDP mobile is attached. If lawful interception is activated when a PDP context is already activated, the next packet transmitted shall be intercepted. If lawful interception is deactivated, the next packets transmitted shall not be intercepted.

A.2.1 Intercept related information events

Intercept related information concerning call progress may be provided to the LEA when the target is using the GPRS service. The following intercept related information events may be provided to the LEA:

- GPRS attach;
- GPRS detach;
- the PDP context activation (GPRS);
- the start of interception with PDP context active;
- the PDP context deactivation (GPRS);
- Cell and/or RA update;
- SMS.

For the case of an SMS transaction the intercept related information is provided in conjunction with the SMS intercepted product to the LEA.

A.2.2 Intercept related information provided to the LEA

The specific information provided by the intercept related information events will vary depending upon: the specific event, and the availability of information in a particular scenario.

For GPRS, a list of the type of information that may be provided to the LEA by intercept related information events, includes:

- an activation reference identity;
- the target identity which has been intercepted (e.g., MSISDN, IMSI, IMEI if applicable);
- type of protocol activated (e.g. Internet Protocol or X.25);
- PDP address used by the target;
- location information of target (Cell Global Identity);
- time of event;
- Access Point Name.

A.2.3 GPRS intercept product

GPRS is capable of carrying many different protocols at the application level. The intercept product shall be the packet as sent by the application without interpretation or modification except for possible reframing, segmentation, or enveloping required to transport the packet to the LEA. No PLMN encryption, compression or encoding shall be present in the intercepted product. The intercepted product should be delivered to the LEA using a standard or widely used protocol.

A.3 Interworking considerations

For GPRS, the PLMN, visited or roaming, shall not be responsible to interpret the protocol used by the target, or to remove user level compression or encryption.

Annex B (informative): Change History

Change history						
SMG#	Spec	Version	CR	<Phase>	New Version	Subject/Comment
						No Phase 1 version
SMG#19	02.33				1.0.0	To SMG#19 for information
SMG#20	02.33			R96	2.0.0	To SMG#20 for approval
SMG#20	02.33	2.0.0		R96	5.0.0	TS approved by SMG#20
	02.33	5.0.0	A001r2	R98	7.0.0	CR 02.33-A001r2 (GPRS) approved by SMG#25 The specification was converted to version 7.0.0 because the work item is related to Release 98 version 5.0.0 was withdrawn.
SMG#27	02.33	7.0.0	A002r2	R98	7.1.0	CR 02.33-A002r2 (LI) - approved by SMG#27
SMG#27	02.33	7.0.0	A003r2	R98	7.1.0	CR 02.33-A003r2 (LI) - approved by SMG#27
SMG#28	02.33	7.1.0	A004	R98	7.2.0	CR 02.33-A004 (category F) (LI Release 98) approved by SMG#28
SMG#29	02.33	7.2.0	A005	R98	7.3.0	CR 02.33-A005 (category B) (additions and corrections for LI for GPRS) approved by SMG#29
04-2000	02.33	7.3.0	-	R99	8.0.0	Release 99 version
Change history						
TSG SA#	Spec	Version	CR	<Phase>	New Version	Subject/Comment
SP-11	02.33	8.0.0	-	Rel-4	42.033 v 4.0.0	Upgrade to Release 4 (3GPP numbering)
SP-16	42.033	4.0.0	-	Rel-5	5.0.0	Upgrade to Release 5
SP-26	42.033	5.0.0	-	Rel-6	6.0.0	Upgrade to Release 6
SP-36	42.033	6.0.0	-	Rel-7	7.0.0	Upgrade to Release 7
SP-42	42.033	7.0.0	-	Rel-8	8.0.0	Upgrade to Release 8
SP-46	42.033	8.0.0	-	Rel-9	9.0.0	Upgrade to Release 9
2011-03	42.033	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)
2016-01	-	-	-		13.0.0	Update to Rel-13 version (MCC)

History

Document history		
V13.0.0	January 2016	Publication