

ETSI TS 133 106 V11.2.0 (2015-07)



**Universal Mobile Telecommunications System (UMTS);
LTE;
3G security;
Lawful interception requirements
(3GPP TS 33.106 version 11.2.0 Release 11)**



Reference

RTS/TSGS-0333106vb20

Keywords

LTE,SECURITY,UMTS

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 noticeThe 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 2015.
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 (<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 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.....	4
Introduction	4
1 Scope	5
2 References	5
3 Definitions and abbreviations.....	6
3.1 Definitions	6
3.2 Void.....	6
3.3 Abbreviations	6
4 Relationship to Regional Requirements	7
5 Requirements.....	7
5.1 Description of requirements	7
5.1.1 General technical requirements.....	8
5.1.2 General principles.....	8
5.1.3 Applicability to telecommunication services.....	9
5.1.4 Interception within the Home and Visited Networks for roaming scenarios	9
5.2 Normal operation.....	9
5.2.1 Intercept administration requirements	9
5.2.1.1 Activation of LI.....	10
5.2.1.2 Deactivation of LI	10
5.2.1.3 Security of processes.....	10
5.2.2 Intercept invocation	10
5.2.2.0 General	10
5.2.2.1 Invocation events for lawful interception.....	10
5.2.2.2 Invocation and removal of interception regarding services.....	11
5.2.2.3 Correlation of information and product.....	11
5.2.2.4 Timing.....	11
5.3 Exceptional procedures	11
5.4 Interworking considerations	11
5.5 Charging aspects	12
5.6 Minimum service requirements	12
5.7 LI Requirements for Encrypted Services.....	12
5.8 Lawful Interception for Customized Alerting Tone (CAT).....	13
5.9 Lawful Interception for Customized Ringing Signal (CRS)	13
5.10 Lawful Interception for Home Node B and Home enhanced Node B (H(e)NB)	14
5.11 Location Information.....	15
5.12 LI Requirements for IMS VoIP Service	15
6 Handover Interface Requirements	15
Annex A (informative): Bibliography	16
Annex B (informative): Change history	17
History	18

Foreword

This Technical Specification (TS) 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.

Introduction

This Technical Specification has been produced by the 3GPP TSG SA to allow for the standardisation in the area of Lawful Interception (LI) of telecommunications. This document describes in general the requirements for lawful interception.

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.

1 Scope

The present document provides Stage 1 interception requirements within a 3GPP network.

The specification describes the service requirements from a Law Enforcement point of view only. The aim of this document is to define an interception system for 3GPP networks that supports a number of regional interception regulations, but these regulations are not repeated here as they vary. Regional interception requirements shall rely on this specification to derive such information as they require.

These interception requirements shall be used to derive specific network requirements.

For details see:

Stage 2: 3GPP TS 33.107 [9];
Stage 3: 3GPP TS 33.108 [10].

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] - [3] Void.
- [4] ETSI ES 201 671: "Handover Interface for the lawful interception of telecommunications traffic".
- [5] - [7] Void.
- [8] J-STD-025-A: "Lawfully Authorized Electronic Surveillance".
- [9] 3GPP TS 33.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions".
- [10] 3GPP TS 33.108: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover interface for Lawful Interception".
- [11] 3GPP TS 22.220: "Service Requirements for Home NodeBs and Home eNodeBs".
- [12] 3GPP TS 22.182: "Customized Alerting Tones (CAT) Requirements; Stage 1".
- [13] 3GPP TR 23.872: "Study on Architecture of IP Multimedia subsystem (IMS) based Customized Alerting Tone (CAT)".
- [14] 3GPP TS 24.182: "IP Multimedia Subsystem (IMS) Customized Alerting Tones (CAT); Protocol Specification".
- [15] 3GPP TR 29.882: "Customized Alerting Tone (CAT) in 3G CS Domain".
- [16] 3GPP TS 22.183: "Customized Ringing Signal (CRS) Requirements; Stage 1".
- [17] 3GPP TS 24.183: "IP Multimedia Subsystem (IMS) customized Ringing Signal (CRS); Protocol Specification".
- [18] ETSI TS 101 671: "Lawful Interception (LI) Handover Interface for the lawful interception of telecommunications traffic".

NOTE: Periodically, TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[19] 3GPP TR 21.905: '3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications'.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [19] and the following terms apply.

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.

Customized Alerting Tone: An indication that is customized by the called party or the calling subscriber that is played to the calling party during call establishment or during an established call session indicating that the called party is being alerted, the progress of a communication request, or any alerting event during a call session. A Customized Alerting Tone may be a piece of recorded or composed music, greeting words, voice, advertisement or video.

Customized Ringing Signal: An indication to the called party as an incoming communication indication during the establishment of a communication that is customized by the calling party or the called party. A Customized Ringing Signal (CRS) may e.g. be a picture, a piece of recorded or composed music, greeting words, voice, advertisement or video.

Intercept Related Information: 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, and location information.

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

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

Subject Based Interception: Interception that is invoked using a specific Target Identity

Target Identity: A technical identity that uniquely identifies a target of interception. One target may have one or several identities.

3.2 Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [19] and the following apply:

CAT	Customized Alerting Tone
CC	Content of Communication
CRS	Customized Ringing Signal
CS	Circuit Switched
CSG	Closed Subscriber Group
CSP	Communications Service Provider
HeNB	Home eNodeB
H(e)NB	HNB and HeNB
HNB	Home NodeB
IA	Interception Area
IP	Internet Protocol

IRI	Intercept Related Information
LDI	Location Dependent Interception
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MS	Mobile Station
PS	Packet Switched
QoS	Quality of Service
SIP	Session Initiation Protocol
UE	User Equipment
UTC	Coordinated Universal Time
WLAN	Wireless Local Area Network

4 Relationship to Regional Requirements

Interception requirements are subject to national law and international treaties and should be interpreted in accordance with applicable national policies.

Requirements universally called out in regional interception regulatory requirements are supported by the system defined in this document. Requirements unique to a specific region are not addressed (some examples are given in Section 2 as references).

The intercept system defined here provides subject based interception. Other techniques are outside the scope of this specification.

5 Requirements

5.1 Description of requirements

The present subclause gives the general description of lawful interception requirements.

5.1.1 General technical requirements

Figure 1 shows the general system for interception. Technical interception is implemented within a 3GPP network by special functionality on network elements shown in the figure. Specific lawful interception architecture and functions are found in TS 33.107 [9].

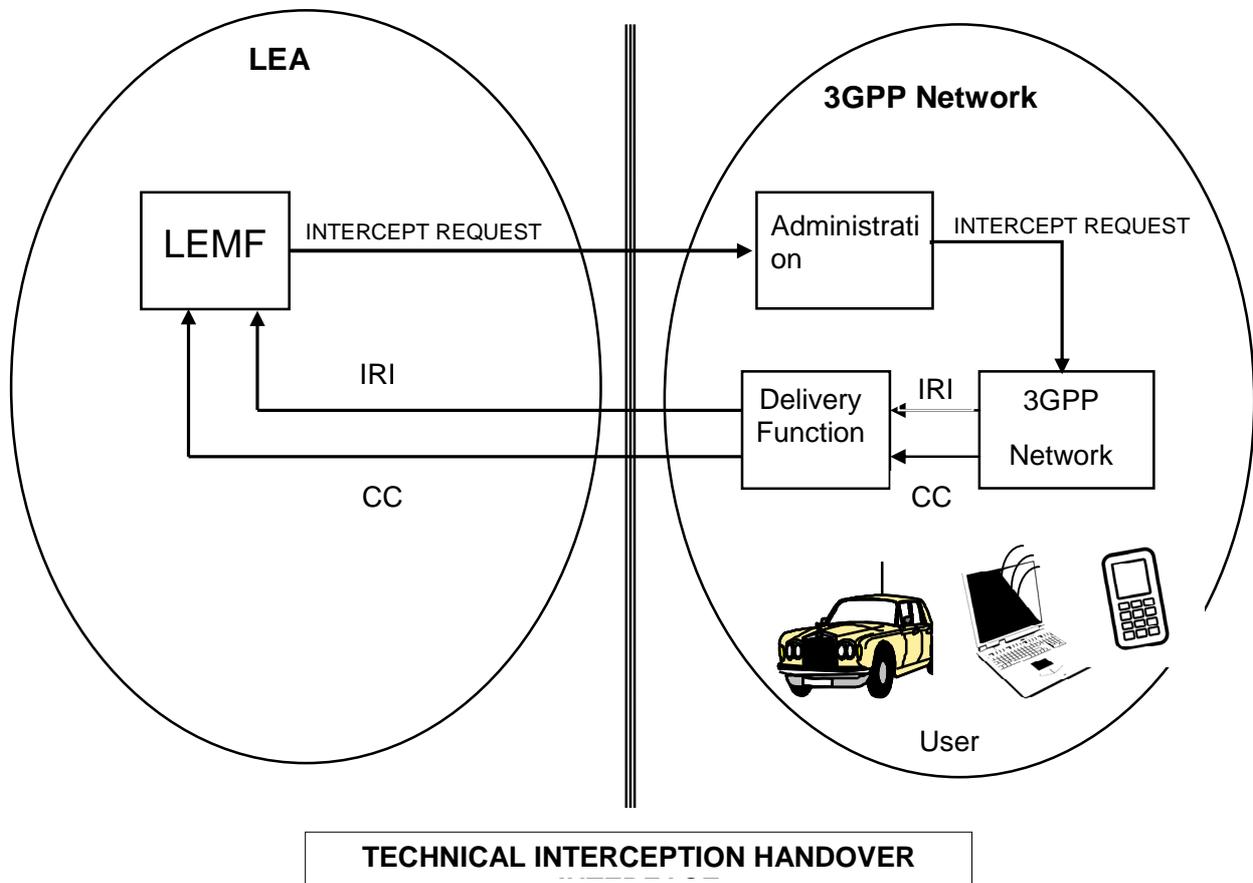


Figure 1: General model for interception

5.1.2 General principles

A 3GPP network shall provide access to the intercepted Content of Communications (CC) and the Intercept Related Information (IRI) of the mobile target and services related to the target (e.g. Call Forwarding) on behalf of Law Enforcement Agencies (LEAs).

A mobile target in a given 3GPP network can be a subscriber of that 3GPP network, or a user roaming from another 3GPP network or from any other network capable of using that 3GPP network. The intercepted CC and the IRI can only be delivered for activities on that given 3GPP network.

For interception, there needs to be a means of identifying the target, correspondent and initiator of the communication. Target identities used for interception for each domain and service are found in TS 33.107 [9] and TS 33.108 [10].

When encryption is provided and managed by the network, it shall be a national option as to whether the network provides the intercepted communication to the LEA decrypted, or encrypted with keys and additional information to make decryption possible. End-to-end encryption implemented in the user equipment based on encryption features provided by the operator is considered to be a network-managed encryption and is subject to the same requirements. See subclause 5.7 for additional requirements.

Encryption not provided or managed by the network, e.g. user provided end-to-end encryption, cannot be removed by the network. In the case that the Communication Service Provider (CSP) provides encryption keys to the subscriber or customer but does not provide the encryption itself, the CSP shall provide the keys to the LEA if required by national regulations.

When compression is provided and managed by the network, it shall be a national option as to whether the network provides the intercepted communication to the LEA decompressed, or compressed with information to make decompression possible.

When encoding is provided and managed by the network, it shall be a national option as to whether the network provides the intercepted communication to the LEA decoded, or encoded with capability (e.g., codec information) to make decoding possible.

Location Dependent Interception, (LDI) allows a 3GPP network to service multiple interception jurisdictions within its service area. Multiple law agencies with their own interception areas can be served by the 3GPP network. All the information or rules given for interception within a 3GPP network apply to interception within an Interception Area (IA) when LDI is invoked. A target may be marked in one or more different IAs within the same 3GPP network. Interception is neither required nor prohibited by this standard when LDI is active and the location of the target subscriber is unknown or unavailable.

5.1.3 Applicability to telecommunication services

The requirement for lawful interception is that all telecommunications services in the 3GPP network standards should be capable of meeting the requirements within this document.

It is a national option that LI, as delivered to the LEMF, may be restricted to specific target subscribed services offered by the CSP or third party providers with a service level agreement with the CSP.

5.1.4 Interception within the Home and Visited Networks for roaming scenarios

The requirements in this clause are additional to the requirements described elsewhere in this specification which apply to the home network in a roaming scenario.

National regulations cover the definition of services and the definition of service provider categories which are subject to LI obligations. This can include how and which IMS services are considered to be covered. For the purpose of roaming, IMS VoIP Service or other 3GPP operator services (CS voice replacement) shall be considered equivalent to a CS voice service and therefore all requirements applicable to legacy CS voice (e.g. interception of voice in isolation from other services) shall be applicable to IMS VoIP Service or other equivalent services.

It shall be possible to intercept all basic voice, data and messaging services provided to a target by a network. The visited network shall be able to support the interception of all services without home network assistance or visibility. However, the visited network is not required to be able to intercept supplementary services (e.g. voicemail, home network based call forwarding) or 3rd party services not directly provided by the visited network. However, national regulation may specify minimum LI capabilities, if such services are in the visited network then they shall be considered in scope for interception (subject to an applicable lawful authorisation). National regulations may require interception to take place in the home network for outbound roamers, where the user session is routed via the home network. There is no requirement to force traffic to the home network for this purpose.

All these requirements are based on conditions and definitions contained in national regulations..

5.2 Normal operation

This section gives the expected operation for lawful interception.

5.2.1 Intercept administration requirements

As depicted in Figure 1, the Law Enforcement Agency (LEA) provides the intercept request (e.g., lawful authorization or warrant) to the CSP. The intercept request identifies, at a minimum, the target, the type of intercept (i.e., IRI-only, or IRI and CC) that is authorized, the authorized period for interception, and the LEA delivery address(es) for the intercepted information

The CSP shall securely administer the intercept (e.g., to activate, deactivate, show, or list targets) within the 3GPP network as quickly as possible. The CSP's administration function shall use appropriate authentication and audit

procedures. When LDI is used, the administration function shall allow specific IAs to be associated with target subscribers.

5.2.1.1 Activation of LI

For the specified target and based on the warrant, the 3GPP network shall activate the delivery of either IRI, or both the IRI and the CC to the designated LEA destination addresses.

5.2.1.2 Deactivation of LI

As a result of deactivation, the 3GPP network shall to stop all, or a part of, interception activities for the specified target.

5.2.1.3 Security of processes

The intercept function shall only be accessible by authorised personnel.

Only authorised personnel can be aware that an intercept function has been activated on a target. No indication shall be given to any person except authorised personnel that the intercept function has been activated on a target. To be effective, interception must take place without the knowledge of any party to the communication.

Authentication, encryption, log files and other mechanisms may be used to maintain security in the system.

CSPs shall ensure that its equipment, facilities, or services that provide a subscriber with the ability to originate, terminate, or direct communications are capable of facilitating authorized communications interceptions and access to intercept related information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects:

- the privacy and security of communications (both signalling and content of communication) not authorized to be intercepted; and
- information regarding the LEA's interception of communications.

Audit procedures, performed by the CSP, should have access to accurate logs of administration commands and accesses to functions and interception information. Log files shall only be accessible by authorised personnel.

5.2.2 Intercept invocation

5.2.2.0 General

The 3GPP network shall provide the means to allow correlation of different phases (e.g., changes in domains or radio access) of a target's intercepted communication.

5.2.2.1 Invocation events for lawful interception

In general, Lawful interception should be invoked when the transmission of information or an event takes place that involves the target. Examples of when Lawful interception could be invoked are when:

- A circuit switched (CS) call is requested originated from, terminated to, or redirected by the target;
- Location information related to the target facility is modified by the subscriber attaching or detaching from the network, or if there is a change in location;
- An SMS transfer is requested - either originated from or terminated to the target;
- A data packet is transmitted to or from a target;
- A Conference Call is targeted.

5.2.2.2 Invocation and removal of interception regarding services

The invocation of lawful interception shall not alter the operation of a target's services or provide indication to any party involved in a target's communication or to any others (e.g., non-authorized personnel). Lawful interception shall not alter the services available for the subscribers.

If lawful interception is activated during a CS service, the currently active CS service is not required to be intercepted. If lawful interception is deactivated during a CS service, all ongoing intercepted activities may continue until they are completed.

If lawful interception is activated when a packet switched (PS) service is already in use, the next packets transmitted shall be intercepted. If lawful interception is deactivated during a PS service, the next packets shall not be transmitted to the LEMF.

5.2.2.3 Correlation of information and product

When only IRI is delivered, an unambiguous correlation shall be established between associated IRI within the single domain for the same communication or session (for example, different legs in CS).

When both IRI and CC are delivered, an unambiguous correlation shall be established between associated IRI, IRI and CC, and associated CC within the single domain (for example different legs in CS or different packets in PS).

Correlation shall be provided to the target's intercepted communications that undergo a radio access technology change or a domain change with Service Continuity.

5.2.2.4 Timing

The IRI and CC shall be delivered in as near real time as possible.

NOTE: There may be regional or national requirements on the timing requirements for delivery of IRI and CC. This includes the requirement for the CSP to timestamp IRI and CC delivery with a time zone indication (e.g., UTC offset) as part of the timestamp.

5.3 Exceptional procedures

A failure with the establishment of the connection towards the LEA shall not result in any interruption of the target's ongoing telecommunications service.

It is a national option to have buffering of IRI in the 3GPP network to cope with interruptions in the connection of the LI delivery.

5.4 Interworking considerations

The 3GPP network, home or visited, shall not be responsible to interpret the protocol used by the target, or to remove user level compression or encryption.

If the target accesses the 3GPP network via another access network (e.g., an Interworking Wireless Local Area Network (I-WLAN)), the 3GPP network shall provide the LEA with the identity of the access network (as known by the 3GPP operator). When the target's communications or signalling information is no longer available to the 3GPP network due to redirection or handover to another network operator, it is a national option that the 3GPP network shall provide, when available, the LEA with the identity of the network operator that has access to the target's communications or signalling information.

5.5 Charging aspects

The 3GPP network shall be capable of producing charging data related to intercept, including the following mechanisms.

- Use of network resources;
- Activation and deactivation of the target;
- Every intercept invocation,
- Flat rate charging.

It shall be possible to produce this data in such a way that access by non-authorised personnel or the target is precluded.

5.6 Minimum service requirements

Quality of service (QoS), capacity, integrity and reliability of the delivered IRI and CC are the subject of bilateral agreement between the relevant authorities and the CSP. Security is an attribute of the negotiated delivery mechanism between the CSP and the LEA. The QoS towards the delivery function provided by the network must be at a minimum, the same QoS as what the network provides to the target.

5.7 LI Requirements for Encrypted Services

Clause 5.1.2 provides a general description of requirements relating to network applied encryption. The additional requirements in this section do not apply where encryption is provided by the network between any network nodes or user equipment (UE) (e.g., hop by hop IMS signaling security or End to Access Edge radio bearer encryption), where this encryption does not affect the ability of the core network to perform interception according to the requirements provided by this specification. In addition to the general requirements, the following additional LI requirements shall apply to network provided and/or network administered end to end or end to middle encryption, where this encryption prevents en-clair capture of communications required to be intercepted.

1. When an encryption service is provided by the PLMN, lawful interception shall take place as for an unencrypted communications.
 - a. In addition, encrypted communications shall be decrypted, or the decryption keys and any required associated information (e.g. roll over counters) shall be provided to the LEMF.
 - b. For the specific case where a key server based solution is used, it is a national option for the operator to make keys and any associated information (e.g. roll over counters) directly available to the LEMF for the decryption of communications.
2. Interception shall be performed in such a manner as to avoid detectability by the Target or others. In particular:
 - a. There shall be no significant difference in latency during call setup or during communications compared to a non-intercepted communications.
 - b. Interception of a Target shall not prevent the use of key exchange applications which provide a user key confirmation mechanism.

NOTE 1: Key confirmation mechanisms such as an authentication string to be exchanged verbally are commonly used to provide additional assurance of authentication.

- c. Should interception fail during a call (or during call setup), the call shall be unaffected.
3. Where the CSP provides decryption of the communication, it is the operator's choice where in the network this decryption is performed. However, following decryption, all IRI and CC shall be provided to the LEMF using handover mechanisms as per an unencrypted communication.
4. An encryption solution shall not prohibit commencement of Interception and decryption of an existing communication.

5. If key material and any associated information are available, it shall be possible to retrospectively decrypt encrypted communications.

NOTE 2: Unless national regulations require otherwise the operator is not required to retain key material or any communications after the end of a communication.

For requirements in the present clause and clause 5.1.2, the CSP is not obligated to comply with the requirements for any encryption which a Target may use which is outside the control of the CSP (e.g. 3rd party end to end VOIP software).

5.8 Lawful Interception for Customized Alerting Tone (CAT)

CAT is a service defined in TS 22.182 [12], TR 23.872 [13], TS 24.182 [14], and TR 29.882 [15]. The target may be either the calling or the called party. The CSP providing the CAT service, and doing the interception, should report the following:

- The CAT sent to the calling party
- When the target activates, modifies (e.g., changes to content, content descriptors, and timing descriptors), and deactivates their CAT
- When the target copies another subscriber's CAT
- When another subscriber copies the target's CAT
- When the target up loads or down loads CAT, the CAT should be delivered
- When available, the access method (e.g., via MS/UE or web) the target used to activate, modify, and deactivate their CAT settings
- The identity whose CAT is played.

Intercepted CAT may, depending on national regulations, be:

- "played" as part of the CC, during a call set up or,
- Delivered as a file in the IRI Record.

NOTE: Depending on national regulations, intercepted CAT media may be considered content or a signalling.

5.9 Lawful Interception for Customized Ringing Signal (CRS)

CRS is a service defined in TS 22.183 [16] and TS 24.183 [17]. The target may be either the calling or the called party. The CSP providing the CRS service, and doing the interception, should report the following:

- The CRS sent to the called party
- When the target activates, modifies (e.g., changes to content, content descriptors, and timing descriptors), and deactivates their CRS
- When the target copies another subscriber's CRS
- When another subscriber copies the target's CRS
- When the target up loads or down loads CRS, the CRS should be delivered
- When available, the access method (e.g., via MS/UE or web) the target used to activate, modify, and deactivate their CRS settings
- The identity whose CRS is played.

Intercepted CRS may, depending on national regulations, be:

- "played" as part of the CC, during a call set up or,

- Delivered as a file in the IRI Record.

NOTE: Depending on national regulations, intercepted CRS media may be considered content or a signalling.

5.10 Lawful Interception for Home Node B and Home enhanced Node B (H(e)NB)

HNB and HeNB are jointly referred to as H(e)NB, as defined in TS 22.220 [11]. The location of the H(e)NB is the location information used by the operator to verify the location for H(e)NB activation.

For the purpose of LI, a target may be a subscriber attached to a H(e)NB, a Closed Subscriber Group (CSG), or it is a national option to allow targeting a H(e)NB itself.

The LI requirements for H(e)NB local routing, selected IP traffic offload (SIPTO) or local IP access (LIPA) are FFS.

Interception should be done in such a manner to avoid detectability by the target or others.

When a target receives service from the PLMN via a H(e)NB, the following applies:

- the interception capabilities shall take place as for normal PLMN use
- H(e)NB information (e.g., location and identification) shall also be provided to the LEMF
- If available, the location reported for the target is the H(e)NB location where the target's MS is attached
- Target attachment to the H(e)NB and handovers to/from the H(e)NB shall be reported to the LEMF
- There may be national requirements to identify specific information that is required to be reported

When the target is the CSG, the CSP shall report the following:

- modifications (e.g., additions, deletions, changes in time limits for temporary CSG Members) of the CSG list for the H(e)NB
- When available, the access method (e.g., via MS/UE or web) the H(e)NB Hosting Party used to modify the CSG list, if multiple access methods are allowed
- CSG member's handovers to/from the H(e)NB
- CSG members attachments to the H(e)NB
- CSG members communications via the H(e)NB
- It is a national option whether interception on CSG members' communications continues after handover occurs from the H(e)NB

NOTE 1: The requirements for the CSG are FFS.

When the target is the H(e)NB, then the CSP shall report the following:

- activation and deactivation of the targeted H(e)NB
- IP address information regarding the secure tunnel endpoints between the H(e)NB and the Femto Security Gateway in the home network
- modifications (e.g., additions, deletions, changes in time limits for temporary CSG Members) of the CSG list for the H(e)NB
- When available, the access method (e.g., via MS/UE or web) the target used for the modification of the CSG list, if multiple access methods are allowed
- handovers to/from the H(e)NB.
- MS/UE registrations on the H(e)NB
- communications via the H(e)NB

- It is a national option whether interception on H(e)NB communications continues after handover occurs from the H(e)NB

NOTE 2: The requirements for the CSG are FFS.

5.11 Location Information

Depending on national requirements, the CSP may be required to report the location of the Target at the beginning and end of CS calls and PS and IMS sessions on a per warrant or per intercept basis. It may also be a national requirement for the CSP to report the location of the Target during on-going communications.

NOTE 1: Currently, in some cases, the location of the Target might not be available.

The location information reported to the LEA shall be trusted location information (i.e., the location information is either network derived or network verified).

NOTE 2: IMS trusted location information is under study in SA2 and reporting for LI is FFS.

5.12 LI Requirements for IMS VoIP Service

The 3GPP network shall be able to support the delivery of IMS VoIP, and the IMS VoIP supplementary services (e.g., call forwarding), to the LEMF via one of the following two methods:

- Intercepted IMS VoIP communications (e.g., IRI or IRI/CC) are delivered separately from other IMS services,
- Intercepted IMS VoIP communications are delivered as part of all other services.

It is a national option as to which of the two options is applicable.

NOTE: If a 3GPP network operator voice service replaces a legacy CS voice service, or is equivalent to a CS voice service, then it is considered to be a CS voice service for LI purposes.

6 Handover Interface Requirements

Handover interface requirements are defined in TS 33.108 [10]. There may be national or regional specifications (e.g., see ETSI ES 201 671 [4], ETSI TS 101 671 [18], and J-STD-025-A [8]).

Annex A (informative): Bibliography

The documents listed below are not explicitly cited in this specification but are provided for background and for historical information.

3GPP TR 41.033: "Lawful Interception requirements for GSM".

3GPP TS 42.033: "Lawful Interception - stage 1".

3GPP TS 43.033: "Lawful Interception; stage 2".

European Union Council Resolution on the Lawful Interception of Telecommunications (17 January 1995).

ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

ETSI ES 201 158: "Lawful Interception; Requirements for network functions".

Annex B (informative): Change history

Change history					
TSG SA #	Version	CR	Tdoc SA	New Version	Subject/Comment
SA#04	1.0.0			3.0.0	Approved at SA#4 and placed under TSG SA Change Control
SA#06	3.0.0	0001		3.1.0	
SP-11	3.1.0	0002	SP-010135	4.0.0	Update of TS 33.106 for Release 4
SP-11	3.1.0	0003	SP-010136	5.0.0	Release 5 updates
SP-17	5.0.0	0004	SP-020510	5.1.0	Changes to 33.106 to clarify interception capabilities
SP-22	5.1.0	0006	SP-030589	6.0.0	Correction to lawful interception references (Rel-6)
SP-24	6.0.0	0007	SP-040396	6.1.0	Clarification on delivery of IRI and CC
SP-29	6.1.0	0008	SP-050569	7.0.0	Correlation for IMS interception
	7.0.0			7.0.1	2006-01: Editorial to show correct version on cover
SP-38	7.0.1	0009	SP-070788	8.0.0	Clarification of requirements
SP-39	8.0.0	0010	SP-080171	8.1.0	Alignment of CC encryption statement in ETSI TS 101 671
2009-12	8.1.0	-		9.0.0	Update to Rel-9 version (MCC)
SP-48	9.0.0	0011	SP-100253	10.0.0	Encryption Requirements
SP-48	9.0.0	0012	SP-100253	10.0.0	CAT LI Support
SP-48	9.0.0	0013	SP-100253	10.0.0	CRS LI Support
SP-48	9.0.0	0014	SP-100440	10.0.0	H(e)NB LI Support
SP-52	10.0.0	0016	SP-110425	11.0.0	Update
SP-53	11.0.0	0017	SP-110511	11.1.0	Requirement for Specific Service Delivery
SP-53	11.0.0	0018	SP-110511	11.1.0	IMS VoIP LI Requirement and Correlation for domain and radio access changes for Service Continuity
--	11.1.0	--	--	11.1.1	Editorial corrections
SP-68	11.1.1	0138	SP-150296	11.2.0	Correction to voice and roaming requirement

History

Document history		
V11.1.1	August 2014	Publication
V11.2.0	July 2015	Publication