ETSI TS 133 106 V14.0.0 (2017-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
3G security;
Lawful interception requirements
(3GPP TS 33.106 version 14.0.0 Release 14)

Reference
RTS/TSGS-0333106ve00

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

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

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.

Lawful interception services may include both passive collection of information related to PLMN services provided to a user targeted for interception and active PLMN service invocation in support of lawfully authorized surveillance activities relating to a particular target. This specification considers requirements for both forms of lawful interception. Which PLMN services are subject to lawful interception is defined in national regulations.

The presence of a requirement in this specification does not in itself infer or mandate that a 3GPP operator has an obligation to implement any network service capability, which is not otherwise required to meet LI obligation compliance in relation to specific regulated services, offered by that 3GPP operator. Only those specific requirements and sub-sections of this specification which are applicable to specific network and/or service capabilities implemented in a 3GPP operator's network shall be considered in scope for that operator. In all cases, national regulations define which requirements are applicable to 3GPP operators in each country relative to the services offered by each 3GPP operator.

As such not all requirements in 33.106 will apply in all national jurisdictions or to all 3GPP operator deployments (e.g if an operator does not offer voice services, then voice LI requirement in this specification do not apply unless otherwise mandated in national regulations).

Editor's Note: Scope needs to be enhanced more clearly differentiate between traditional 3GPP service usage reporting and wider LI requirements covered national lawful interception obligations.

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(V3.1.1 May 2007): "Handover Interface for the lawful interception of telecommunications traffic".

[5] - [7] Void.

[8] ANSI J-STD-025-A: (April 2003): "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 Mulimedia subsystem (IMS) based Customized Alerting Tone (CAT)".

[14] 3GPP TS 24.182: "IP Multimedia Subsystem (IMS) Customized Alerting Tones (CAT); Protocol Specificiation".

[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 (V3.11.1 November 2012): "Lawful Interception (LI) Handover Interface for the lawful interception of telecommunications traffic".

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

[20] ETSI TS 102 232-7 (V3.1.1 June 2012): " Service-specific details for Mobile Services"

[21] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[22] OMA OMA-AD-MMS-V1_3-20110913-A.:"Multimedia Messaging Service Architecture".

[23] 3GPP TS 22.071: "Location Services (LCS); Service description; Stage 1".

[24] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[25] 3GPP TS 22 173: "IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1".

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).

Lawful Access Location Services: action (based on the law), performed by a network operator/access provider/service provider, of making available Location Services (LCS) and providing that information to a law enforcement monitoring facility. Depending of legislation this can be part of interception or an additional action.

Lawful Interception (LI): the action (based on the law) for specific target identity(s), by a network operator/access provider/service provider, of accessing and delivering in real-time certain current information to a Law Enforcement Monitoring Facility (LEMF). This information includes Intercept Related Information (IRI) and Content of Communications (CC).

LCS (Location Services): LCS is a service concept in system (e.g. GSM, UMTS, UTRAN or EUTRAN) standardization. LCS specifies all the necessary network elements and entities, their functionalities, interfaces, as well as communication messages, due to implement the positioning functionality in a cellular network. Note that LCS does not specify any location based (value added) services except locating of emergency calls and Lawful Access Services.

LCS Client: Software and/or hardware entity that interacts with a LCS Server for the purpose of obtaining location information for one or more Mobile Stations. LCS Clients subscribe to LCS in order to obtain location information. LCS Clients may or may not interact with human users. The LCS Client is responsible for formatting and presenting data and managing the user interface (dialogue).

LI-LCS Client: describes the instance used by PLMN to provide LEA access to LCS services.

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

Location Information: information relating to the geographic, physical or logical location of a target identity.

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
LALS	Lawful Access Location Services
LDI	Location Dependent Interception
LEA	Law Enforcement Agency

LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MMS	Multimedia Messaging Services
MS	Mobile Station
PS	Packet Switched
QoS	Quality of Service
SIP	Session Initiation Protocol
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].

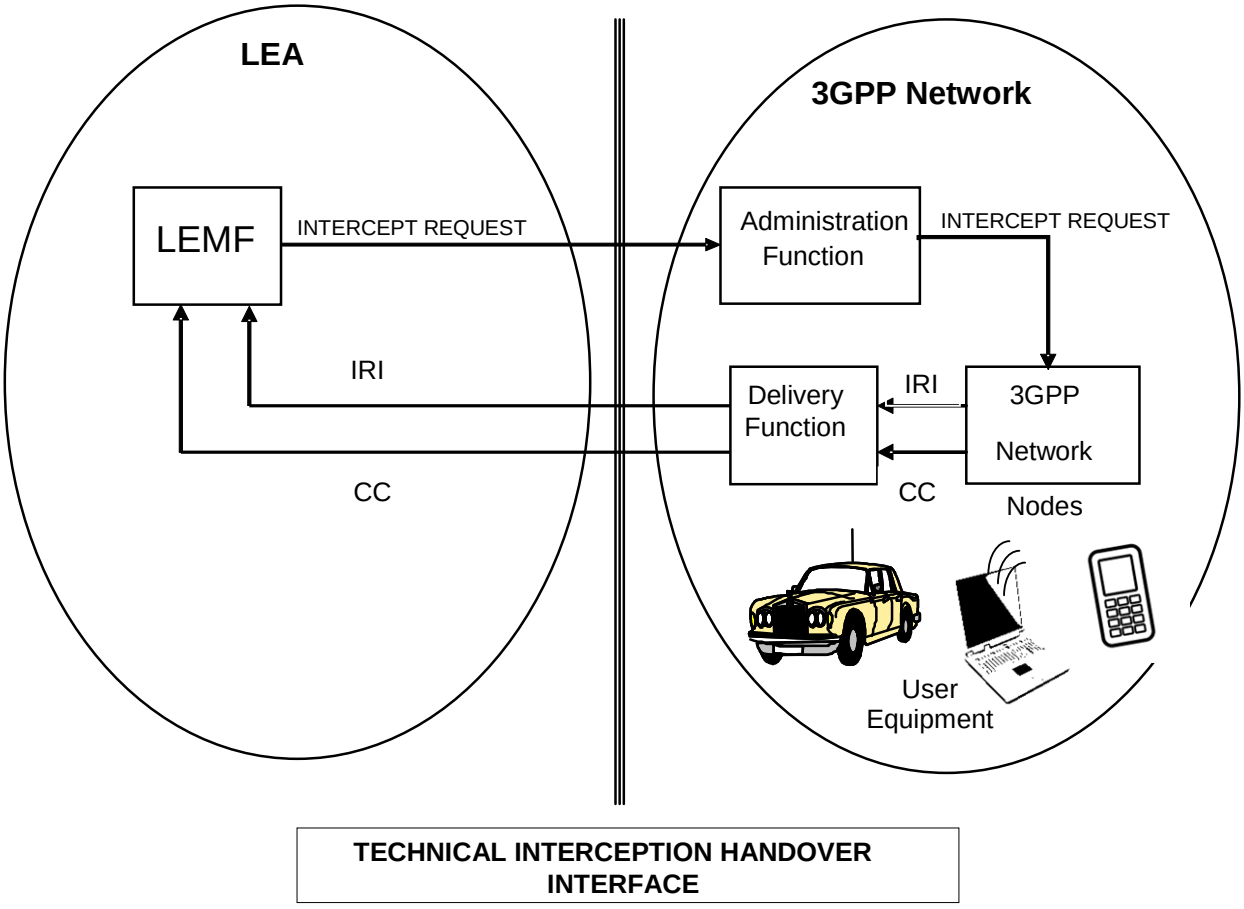

Figure 1: General model for interception

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 target of a given 3GPP network can be a user subscribed to and operating in that 3GPP network, a user equipment operating in that 3GPP network (which is either the HPLMN or a VPLMN), 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.

Interception may be performed in the network access (all or selected APNs) and/or by intercepting a specific service at the application layer (e.g. VoIP). When interception is done on a per-service basis, only the IRI and CC defined for that service shall be delivered to the LEA, if authorized. National regulations will define the service to be intercepted.

For interception, there needs to be a means of identifying the target, correspondent and initiator and related parties of any targeted communication. A means shall exist for the operator to intercept communications based on long term or permanent identifiers associated with a target service or equipment, as identified by the LEA. To achieve interception, the operator may need to translate these into further associated identifiers, in order to identify the data to be intercepted. Target identities used for interception for each domain and service are target service and equipment associated with target use or any derived IDs from such elements that are to be defined in TS 33.107 [9] and TS 33.108 [10]. Examples

of these identities are IMSI, MSISDN, NAI, Tel URI, SIP URI, for the target service and IMEI, MAC for the equipment.

NOTE 1: Identifiers available in 3GPP networks may have different levels of authenticity. For LI purposes, no additional authentication procedures for target identities are required.

In many cases, national regulation will require that LI activity is performed entirely within a particular legal jurisdiction, in line with the requirements in 5.1.2 and 5.1.4.

It is not permitted for a CSP to rely on another CSP or jurisdiction to ensure LI activity can occur. For example, a serving network shall not share LI target identities with a home network in the case of roaming or vice versa (as described in clause 5.1.4).

NOTE 2: LEAs will continue to specify the target of interception using long-term identifiers, such as IMEI or IMSI, even if the network uses other derived or temporary identifiers to identify the correct traffic due to the concealment of long-term identifiers for privacy reasons.

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 enforcement 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 is unknown or unavailable.

National regulations may require that an operator is able to intercept any communication passing through its network based on any visible identity not connected to the operator network. It shall be based on a match between this target identity and identity type (e.g. IMPU) with the detected party fields. This identity is referred as a Non-Local Identity.

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, using the identifiers provided by an LEA as described in section 5.1.2. 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.

National regulations may limit delivery of communications (CC and communications–associated IRI) of an outbound international roaming target by the HPLMN based on roaming specific interception constraints (e.g., roaming outside national border). To support these scenarios, it is a national option for the HPLMN to be able to support a mechanism to apply on a per-warrant/per-intercept to limit the delivery of the communications (CC and communications–associated IRI) to LE of an outbound international roaming target based on roaming specific interception constraints (e.g., roaming outside a national border). The default setting is determined based on a national option. Communications originated by the roaming target are subject to this mechanism. Communications incoming to the target that are answered by the target are subject to this mechanism. Communications incoming to the target that are not answered by the target (e.g., due to call forwarding) are not subject to this mechanism. Non-communications-associated IRI (e.g., serving system event) are not affected by this requirement.

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

NOTE: The requirement of interception by serving network of non 3GPP access and associated services is not defined in this release.

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) ; the service to be intercepted (e.g. 3G PS network access(es) and/ or the services (e.g. VoIP)) that is authorized, the authorized period for interception, and the LEA delivery address(es) for the intercepted information

NOTE: In some situations IRI may contain CC-information. In case of a IRI only intercept the IRI delivery may take place without the CC-information.
In other situations the CC-delivery may provide metadata not sent in the IRI. In case of a IRI only intercept the CC-delivery may take place without the actual content.
It is upon national regulations to implement any of these options.

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 targets.

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.

National regulation may require methods to reduce overloading of the LEMF or LI equipment (e.g. ICEs).

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 voice call request is 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;
- An MMS 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 ;
- Modification and management of the target's IMS supplementary service settings (e.g., multimedia telephony supplementary service settings as defined in TS 22.173 [25]).

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.

If lawful interception is activated during an IMS session (including IMS VoIP), the currently active IMS session is required to be intercepted. However, reporting of call information (e.g., identities of parties) by the CSP depends on its availability. If lawful interception is deactivated during an IMS session, interception should be ceased expeditiously.

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 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 LEMF shall not result in any interruption of the target's on-going telecommunications service.

It is a national option to have buffering of IRI and/or CC to cope with interruptions in the connection to the LEMF.

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 these were not provided by the 3GPP network.

If the target accesses the 3GPP network via another access network 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.

National regulations may require the home network to report:

- subscriber profile change events such as change of identifiers associated with a target (i.e. HLR/HSS target identity change);
- location related events related to the target in the visited network:
  - register location / registration/access control to a new serving network even if such information is coming from a non 3GPP network; or from the previous serving network, happening after the provisioning of the target by the CSP with the received warrant;
  - cancel or purge location;

- location information request or query from other 3GPP networks.

NOTE: Some other national regulations may prohibit the interception when the target is physically outside the jurisdiction of the warrant.

5.5 Charging aspects

The 3GPP network shall be capable of producing charging data related to interception , 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, and, integrity 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.

The LI service's need to provide high availability and high reliability of the near-real-time transport mechanism of the LI data from the CSP to LEMF is subject to bilateral agreement between the relevant authorities and the CSP.

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 (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 requirments, the following additonal 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 (see Note 0) 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 (see Note 0) directly available to the LEMF to support the decryption of communications.

Note 0: Examples of associated encryption information: encryption algorithm, key length, block cipher mode of operation, initialization vector, salt, crypto parameters, padding or roll over counters.

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: If the associated IRI and CC have been delivered to the LEMF, the operator is not required to retain key material or any target related communications after the end of a communication unless national regulations require otherwise.

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 participate in the service as either the calling or the called party. The CSP providing the CAT service, and doing the interception, should report the following:

- When the target activates, modifies (e.g., changes to content, content descriptors, and timing descriptors), and deactivates CAT settings

- When the target invokes the function of copying of another subscriber's CAT

- When the target invokes the up loading or down loading CAT and is not part of CAT delivery to the calling party, the CAT should be delivered to the LEMF.

- The identity whose CAT is played to the target

Additionally when the target is a User, the CSP providing the CAT service, and doing the interception, should report the following:

- The CAT sent to the calling party

- When another subscriber copies the target's CAT

- When available, the access method (e.g., via UE or web) the target used to activate, modify, and deactivate their CAT settings.

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 participate in the service as either the calling or the called party. The CSP providing the CRS service, and doing the interception, should report the following:

- The CRS, when invoked by the target, is sent to the called party

- When the target activates, modifies (e.g., changes to content, content descriptors, and timing descriptors), and deactivates their CRS settings
- When the target invokes the function of copying another subscriber's CRS
- When the target invokes the up loading or down loading CRS, and is not part of CRS delivery to the called party the CRS should be delivered

  The identity whose CRS is played to the target

Additionally for when the target is a User, the CSP providing the CRS service, and doing the interception, should report the following:

- When another subscriber copies the target's CRS
- When available, the access method (e.g., via UE or web) the target used to activate, modify, and deactivate their CRS settings.

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 user or user equipment 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 attached to a H(eNB) is the H(e)NB's location
- 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 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 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.
- 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

5.11.1 General

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;
- for any mobility management event detected in the 3GPP core network which includes a target's location change or update.

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

The location information associated with target communication reported to the LEMF shall be at least location information trusted by the 3GPP network (i.e. the location information is either 3GPP network derived or verified).

National regulation may require that the location information source be provided if known by the CSP.

The 3GPP access network derived or verified location information shall be the location(s) of the access point(s) to which the Target is connected in the access network(s). The location shall be the access network identifier like the radio cell identity.
For non 3GPP access networks, the location information shall be at least the identity of entry point into the 3GPP core network (e.g. fire wall or security gateway). The location information of the non-3GPP access network shall be provided if this information is available to the CSP.

National regulation may require that third party provided location information associated with target communication, that may be available in the 3GPP network, is reported to the LEMF.

If required by national regulation the geographic location and/or civic address information shall be reported to the LEMF. This can include additional radio coverage information.

5.11.2 Location Services

In addition to the 3GPP network derived or verified location information as described in 5.11.1. target location information from Location Services (LCS, as described in 3GPP TS 22.071 [23] and 3GPP TS 23.271 [24]) may be used additionally to provide location information to the LEMF if available. Additional requirements applicable are in Annex B.

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.

If a 3GPP network operator voice service replaces a legacy CS voice service, or is equivalent to a CS voice service, then it shall be considered to be a CS voice service for LI purposes. This also applies to new 3GPP networks without legacy CS voice service.

Subsequently, (at least) the following voice service LI capabilities shall be ensured in IMS VoIP; as they are in CS:

- Location information shall be able to be reported to the LEMF;
- If for a given implementation, the IRI related to the CC is not delivered in near real time (within the time delay allowance defined by national regulation), then the media related information (e.g. SDP) shall be delivered along with the CC to allow the CC content to be decoded or interpreted ,without needing to wait for the IRI;
- If available, activation or modifications of IMS supplementary services shall be reported to LEMF (if authorized).

NOTE 1: void

NOTE 2: void

5.13 Delivery requirements for messaging

The 3GPP network shall be able to support the separate delivery of intercept information (IRI or IRI/CC) for messaging services, to the LEMF from other targeted services. This requirement is applicable for the following messaging services:

- SMS (3GPP TS 23.040 [21]); and
- MMS ([22]).

Message service delivery is independent from network access technology.

5.14 LI requirements for management of IMS supplementary services settings

The IMS network and related service platforms shall be able to support the reporting of IRI for the modification and management of the target's IMS supplementary services settings.

5.15 LI requirements for IMS Video Service

In case of IMS video service, all clause 5.12 requirements shall apply.

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], ETSI TS 102 232-7 [20] 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 (normative): Lawful access usage of Location Services (LCS)

Additional Location information can be reported for various instances; the use of services; the use of network and or radio resources, the loss of a service; requested commercial LCS queries by the user, associates, or other application; and or from network and radio functions providing varying degrees of granularity and accuracy.

Location Service may provide a higher degree of location granularity and accuracy than the existing network based Lawful Interception location capabilities described in clause 5.11.1.

National regulation may impose the following requirements defined in TS 22.071 [23] apply to LCS when invoked as part of LALS (Lawful Access Location Services):

- Any UE (including inbound roamers) served by the PLMNand supported by the serving PLMN LCS (including coverage) shall be targetable by LALS
- If the location positioning for the target UE has failed, the LCS server shall report the reason for failure, if known.
- For LALS Target UEs may be positioned under all circumstances required by national regulatory requirements.

  The target UE user shall not be notified of any LALS location attempt.

  LALS location information provided should be the most recent if requested and available.
- The invocation, use and collection of LALS location should not cause target User service interruptions except for LCS priority described in clauses 4.5 and 7.3 of TS 22.071 [23]. In the case of LCS priority, national regulations may override the definitions in TS 22.071 [23].
- ` Support for LALS Location shall apply for both active and idle UEs.
- LCS shall support LALS requests for the current (updated), or the last known position of an UE.
- The network should be sufficiently flexible to accommodate evolving LCS enabling mechanisms and LALS service requirements.
- Only authorized LALS network functions, resources and LI-LCS Clients shall provide LALS information.
- LALS shall support location of UEs in either circuit switched and packet switched domains.

NOTE: For the purposes of this specification, the portion of LALS dealing with positioning of a target can be considered equivalent to lawful intercept use of LCS described in TS 22.071 [23]. Other aspects such as delivering a target's position to a LEA are beyond the scope of TS 22.071 [23].

National regulations may impose the following requirements in addition to those defined in TS 22.071 [23] to apply to LCS when invoked as part of LALS:

- No LCS subscription is required for any UE within the PLMN for providing LALS location.

The LALS positioning information shall be provided to the collection functions in a secure and reliable manner, such that the location information is neither lost, corrupted, nor made available to any unauthorized third party.

- The LI-LCS Client shall support periodic target UE location reporting to the LEA.
- LALS shall support different location update periods per target for multiple LEAs.

LALS shall support identifying a target UE using any one of the following:

- MSISDN
- Tel URI/SIP URI
- IMPI / IMPU
- IMSI

- IMEI

- Providing LALS location of an UE attached to a 3GPP network, using an IMEI identifier is required by some national regulations. In such case, IMEI may be mapped dynamically by a suitable identity such as IMSI or MSISDN (but is beyond the scope of this standard). Target identities which may be provided by the LI-LCS client to the LCS server are specified by TS 22.071 [23] and TS 23.271 [24].

- LALS shall re-use LCS supported positioning technologies defined in 3GPP, including positioning technology specific limitations, policies, procedures and operations. The specifc positioning technology selected and deployed to support LCS and LALS will vary from operator to operator and even PLMN to PLMN.

- National Regulation may require LALS provide higher accuracy and security than Commercial LCS Services

LALS shall support multiple requests and obtain the location of the same target UE at the same time from different LEAs.

NOTE 1: The Location Services load which may include LALS for specific target UE(s) (e.g. multiple requests, multiple periodic updates, short period updates) may impact network and UE performance (e.g. UE battery performance) and may require establishing operator imposed limits to LALS Location Services requests

Editor's Note: The above list of requirements needs to be checked for concistency and for stage 2 requirements, after completion of stage 2 in 33 107.

NOTE 2: Void.

Editor's Note: For Lawful Access Location Services (where required by national regulatory requirements), the PLMN support of positioning of unauthorized UEs (i.e. including stolen UEs and MEs) where such devices are readily accessible by the LCS in the PLMN is for further study.

Annex C (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-59	11.1.1	0019	SP-130034	12.0.0	Adding ETSI TS102 232 reference
SP-61	12.0.0	0129	SP-130401	12.1.0	Adding version to non 3GPP references
SP-62	12.1.0	0130	SP-130661	12.2.0	Stage 1 enhancements for IMEI targeted LI capabilities
		0131			Addition of Separate Delivery of Messaging
SP-63	12.2.0	0132	SP-140020	12.3.0	Civic Address usages as a new location information
SP-65	12.3.0	0133	SP-140586	12.4.0	Encryption clarification
		0134			Location requirements
		0135			Clarifying Service requirement and editorial alignment of term
SP-66	12.4.0	0136	SP-140821	12.5.0	Adding the interception feature of any modification of target's supplementary services management of 3GPP services
SP-68	12.5.0	0139	SP-150296	12.6.0	Correction to voice and roaming requirement
	12.6.0	0140	SP-150296	13.0.0	Correction to voice and roaming requirement
		0141	SP-150298		Activation and Deactivation of LI for IMS Services
		0142	SP-150298		High Availability and Reliability of the LI Data Delivery Transport Mechanism
SP-69	13.0.0	0143	SP-150470	13.1.0	Removing examples of IWLAN as this is no longer acurate
		0144			Interception of messages to and from HSS/HLR/AAA during interworking or any activities related to the target from any access network
		0145			Location information and interception of message between two nodes that contain the target's id
SP-70	13.1.0	0147	SP-150835	13.2.0	Addition of Location Service

SP-71	13.2.0	0150	SP-160050	13.3.0	Scope Purpose Improvements
SP-71	13.2.0	0151	SP-160050	13.3.0	Text changes required to provide distinction between traditional location in LI and LCS services
SP-71	13.2.0	0152	SP-160050	13.3.0	Text changes to address Note 7, 8 in Annex B
SP-71	13.2.0	0153	SP-160050	13.3.0	Text changes to address Note 4 provided in SP-150835
SP-71	13.2.0	0154	SP-160050	13.3.0	Legal Interception of non local identity
SP-71	13.2.0	0157	SP-160050	13.3.0	Authenticity of identifiers
SP-71	13.2.0	0158	SP-160050	13.3.0	Clarification of "Lawful Interception"

Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2016-06	SA#72	SP-160384	0159	2	C	Cleanup and reorganization of Appendix B (LCS requirements)	13.4.0
2016-06	SA#72	SP-160384	0160	3	B	Requirement to Toggle Interception for an outbound international roaming Target by the HPLMN	13.4.0
2016-06	SA#72	SP-160384	0161	-	C	Stage 1: Clarification on the stage 1 requirement on security of process	13.4.0
2016-06	SA#72	SP-160384	0162	2	F	Per Service Interception Clarification	13.4.0
2017-03	SA#75	SP-170037	0163	1	B	National requirements related to SDP info in HI3	14.0.0
2017-03	SA#75	SP-170037	0164	-	C	Reconfirming LI requirements	14.0.0

History

Document history		
V14.0.0	April 2017	Publication