3G TS 33.106 V3.1.0 (1999-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Lawful Interception Requirements
(3G TS 33.106 version 3.1.0 Release 1999)

Reference
3TS/TSGS-0333106U

Keywords
Security, Architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

3 the first digit:

3 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 specification.

Introduction

This Technical Specification has been produced by the 3GPP TSG SA to allow for the standardisation in the area of lawful interception 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 basic interception requirements within a Third Generation Mobile Communication System (3GMS).

The specification describes the service requirements from a Law Enforcement point of view only. The aim of this document is to define a 3GMS interception system 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.

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.

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

[2] ETR 331: "Definition of User Requirements for Lawful Interception of Telecommunications; Requirements of the Law Enforcement Agencies".

[3] ES 201 158: "Lawful Interception; Requirements for network functions".

[4] ES 201 671: "Handover Interface for the lawful interception of telecommunications traffic".

[5] GSM 01.33: "Lawful Interception requirements for GSM".

[6] GSM 02.33:" Lawful Interception - stage 1".

[7] GSM 03.33: "Lawful Interception - stage 2".

[8] J-STD-25 Interim Standard, "Lawfully Authorised Electronic Surveillance".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

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).

Network Based Interception: Interception that is invoked at a network access point regardless of 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.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CC	Content of Communication
IA	Interception Area
IP	Internet Protocol
IRI	Intercept Related Information
LDI	Location Dependent Interception
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
3GMS	Third Generation Mobile Communications System

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. Network based interception is not included.

5 Requirements

5.1 Description of requirements

This section 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 3GMS by special functionality on network elements shown in the figure.

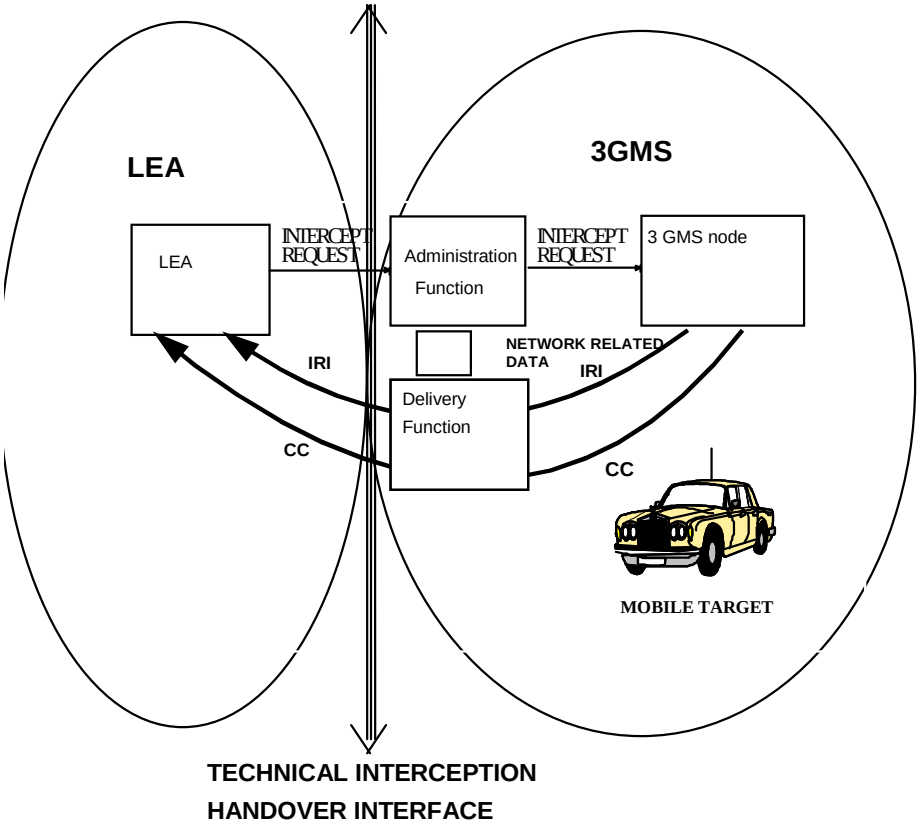

Figure 1: General specification for interception

5.1.2 General principles

3GMS shall provide access to the intercepted Content of Communications (CC) and the Intercept Related Information (IRI) of the mobile target on behalf of Law Enforcement Agencies (LEAs).

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

For interception, there needs to be a means of identifying the target, correspondent and initiator of the communication. Target Identities used for interception shall be MSISDN, IMEI and IMSIWhen network encryption is introduced, it shall be a national option as to whether the network provides the CC to the agency decrypted, or encrypted with a key available to the agency.

Location Dependent Interception, (LDI) allows a 3GMS to service multiple interception jurisdictions within its service area. Multiple law agencies with their own interception areas can be served by the 3GMS. All the information or rules given for interception within a 3GMS apply to interception within an IA when Location Dependent Interception is invoked. A target may be marked in one or more different IAs within the same 3GMS. Interception is not required nor prohibited by this standard when Location Dependent Interception is active and the location of the target subscriber is not known or available.

5.1.3 Applicability to telecommunication services

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

5.2 Normal operation

This section gives the expected operation for lawful interception.

5.2.1 Intercept administration requirements

A secure means of administrating the service by the 3GMS operator and intercept requesting entity is necessary. This mechanism shall provide means to activate, deactivate, show, or list targets in the 3GMS as quickly as possible. The function shall be policed by appropriate authentication and audit procedures. The administration function shall allow specific IAs to be associated with target subscribers when Location Dependent Interception is being used.

5.2.1.1 Activation of LI

As a result of the activation it shall be possible to request for the specified target, either the CC, the IRI or both, and designate the LEA destination addresses for the delivery of the CC and IRI if required. These shall be selectable on a 3GMS basis according to national options.

5.2.1.2 Deactivation of LI

As a result of deactivation it shall be possible 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.

To be effective, interception must take place without the knowledge of either party to the communication. Therefore, decryption must also take place without either party being aware that it is happening.

No indication shall be given to any person except authorised personnel that the intercept function has been activated on a target. Authentication, encryption, audits, log files and other mechanisms may be used to maintain security in the system. Audit procedures should be capable of keeping accurate logs of administration commands.

5.2.2 Intercept invocation

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 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.

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 communication with the target. Lawful interception shall not alter the standard function of 3GMS network elements.

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

If lawful interception is activated when a packet data service is already in use, the next packets transmitted shall be intercepted. If lawful interception is deactivated during a packet data service, the next packets shall not be transmitted.

5.2.2.3 Correlation of information and product

When both IRI and CC are invoked, an unambiguous correlation shall be established between the two. The IRI and CC shall be delivered in as near real time as possible.

5.3 Exceptional procedures

When a failure occurs while establishing the connection towards the LEA to transfer the CC this shall not result in any interruption of the ongoing telecommunications service. No further specific requirements apply for the CC in the 3GMS.

A national option may be that when failure occurs while trying to provide the IRI it shall be temporarily stored in the 3GMS and some further attempts shall be made to deliver it if available.

5.4 Interworking considerations

For 3GMS, the network, homed or visited, shall not be responsible to interpret the protocol used by the target, or to remove user level compression or encryption.

5.5 Charging aspects

The 3GMS may require raising charges for lawful interception. However charging aspects are subject to national laws and regulations. Some charging mechanisms include the following:

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

The 3GMS shall be capable of producing intercept-charging data. It shall be possible to produce this data in such a way that access by non-authorised personnel or the target is precluded.

5.6 Minimum service requirements

Quality of service, capacity and reliability are the subject of bilateral agreement between the relevant authorities and the 3GMS operator.

6 Handover Interface Requirements

Handover interface requirements are defined by national or regional specifications. See references [4] and [8].

Annex A (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	001		3.1.0	