

**Technical Specification Group Services and System Aspects  
Meeting #4, Miami, USA, 21-23 June 1999**

***TSG SA#4(99)294***

TSG SA WG3 #4, London, 16-18 June 1999

S3-99204

**Subject: 3G TS 33.106 V1.0.0**

Source: TSG SA WG3

Document for: Information and Approval

# 3G TS 33.106 V1.0.0 (1999-06)

---

*Technical Specification*

**3rd Generation Partnership Project;  
Technical Specification Group Services and Systems Aspects;  
WG3 Security  
Lawful Interception Requirements  
(3G TS 33.106 version 1.0.0)**

---



The present document has been developed within the 3<sup>rd</sup> Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

---

Reference

---

DTS/TSG<SA 3>-0<WG 3><33.106 v2.0.0> U

Keywords

---

<keyword[Security, Lawful, Legal, Interception]>

**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 .....	4
Introduction .....	4
1 Scope .....	5
2 References .....	5
3 Definitions, symbols and abbreviations .....	5
3.1 Definitions .....	5
3.2 Symbols .....	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 .....	7
5.1.2 General principles .....	8
5.1.3 Applicability to telecommunication services .....	9
5.2 Normal operation .....	9
5.2.1 Intercept administration requirements .....	9
5.2.2 Intercept invocation .....	10
5.3 Exceptional procedures .....	10
5.4 Interworking considerations .....	10
5.5 Charging aspects .....	11
5.6 Minimum service requirements .....	11
6 Handover Interface Requirements .....	11
History .....	12

---

## Foreword

This Technical Specification has been produced by the 3GPP SA WG3.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval.

---

## 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

- [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] **DES/SEC-003003**: 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 Communications Assistance for Law Enforcement Act (CALEA)
- [9] Encryption and law Enforcement, Performance and Innovation Unit, Horse Guards Road, London SW1P, UK. 3AL Published: May 1999 CABI J99-4278/9905/D16

---

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

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

**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.

## 3.2 Symbols

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

## 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
STAG	Security Techniques Advisory Group

---

## 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

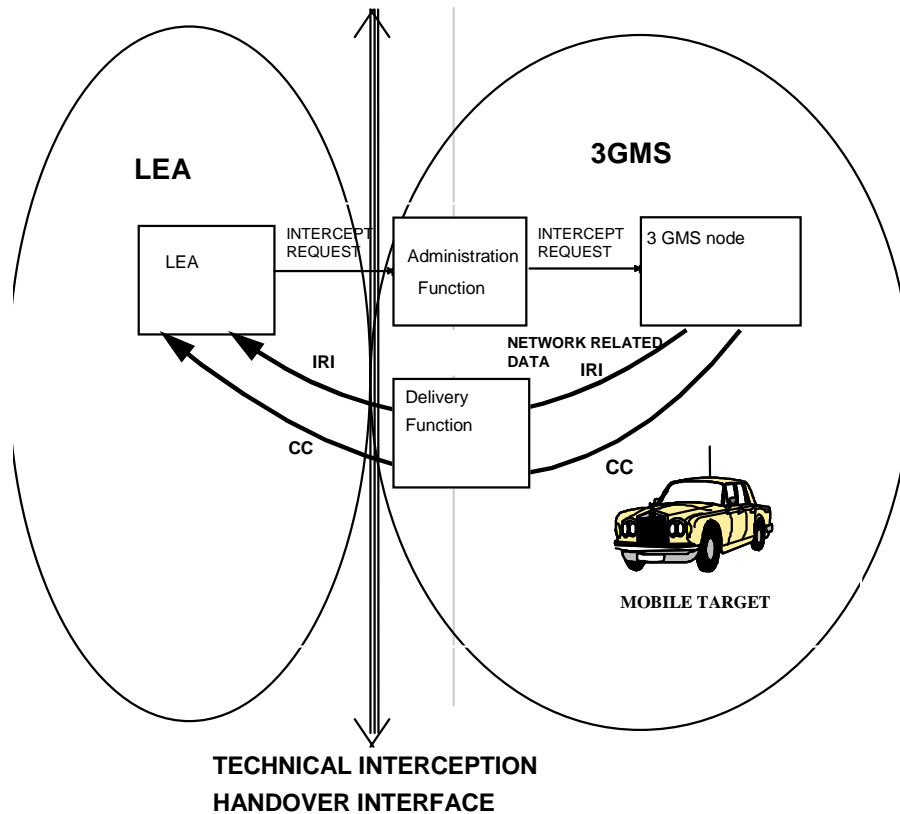
### 5.1 Description of requirements

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 user of that 3GMS, or a user of another 3GMS or any other service 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.

There needs to be a means of identifying the sender and recipient of a message, and the identity of the encryption key holder to allow information to be rendered readable.

An unambiguous correlation shall be established between the IRI and CC. The IRI and CC shall be delivered in as near real time as possible.

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 existing or planned 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. Audit procedures should be capable of keeping accurate logs of administration commands.

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

*[Editor's note: A list of target identities used to trigger interception is for further study after the 3GPP documents are more mature.]*

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

A number of factors applying to stored data and to encrypted stored data must be taken into account in the production of evidence, as follows:

- Stored data must be retrieved in such a way as to ensure that its provenance can be proved in court, and handled in such a way as to maintain the 'chain of evidence'.
- Decryption of stored data must therefore take place in accordance with best practice on computer forensic evidence.

In general, this may require access to the decryption key rather than the plain text (otherwise doubt might be cast in court on the authenticity of the plain text). It may also require access to the stored data, which must be within a legal time limit imposed by the instrument under which it is obtained. It is important that the methods employed for lawful

interception should be provable in a law court, for example the trusted functionality of the process and the inability for records or information to be changed.

## 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,
- A circuit switched data call is requested either originated from or terminated to 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 lawful interception is invoked, IRI and/or CC shall be sent to the LEA. Where both IRI and CC are sent to the LEA, then these two types of information shall be able to be correlated by the LEA, and sent in as near real time as possible. They should be capable of being accurately associated and sequenced, for example with sequential numbers.

## 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

Interworking refers to the interface between the delivery function and the LEA in Figure 1. The delivery function should provide information in a form that is easily capable of being understood by the LEA. Interworking is a matter of national or regional requirements.

## 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 regional specifications.

---

---

## History

<b>Document history</b>		
Edition x	<MMMM yyyy>	Publication as <old doctype> <old docnumber>
0.0.1	25. February 1999	Initial Draft
0.0.2	15. March 1999	First Draft
0.0.3	15. April 1999	First Draft
0.0.4	05 May 1999	First Draft
0.0.5	06 May 1999	First Draft
1.0.0	16 June 1999	Agreed in SA WG3 to be presented to SA#4 for information and approval