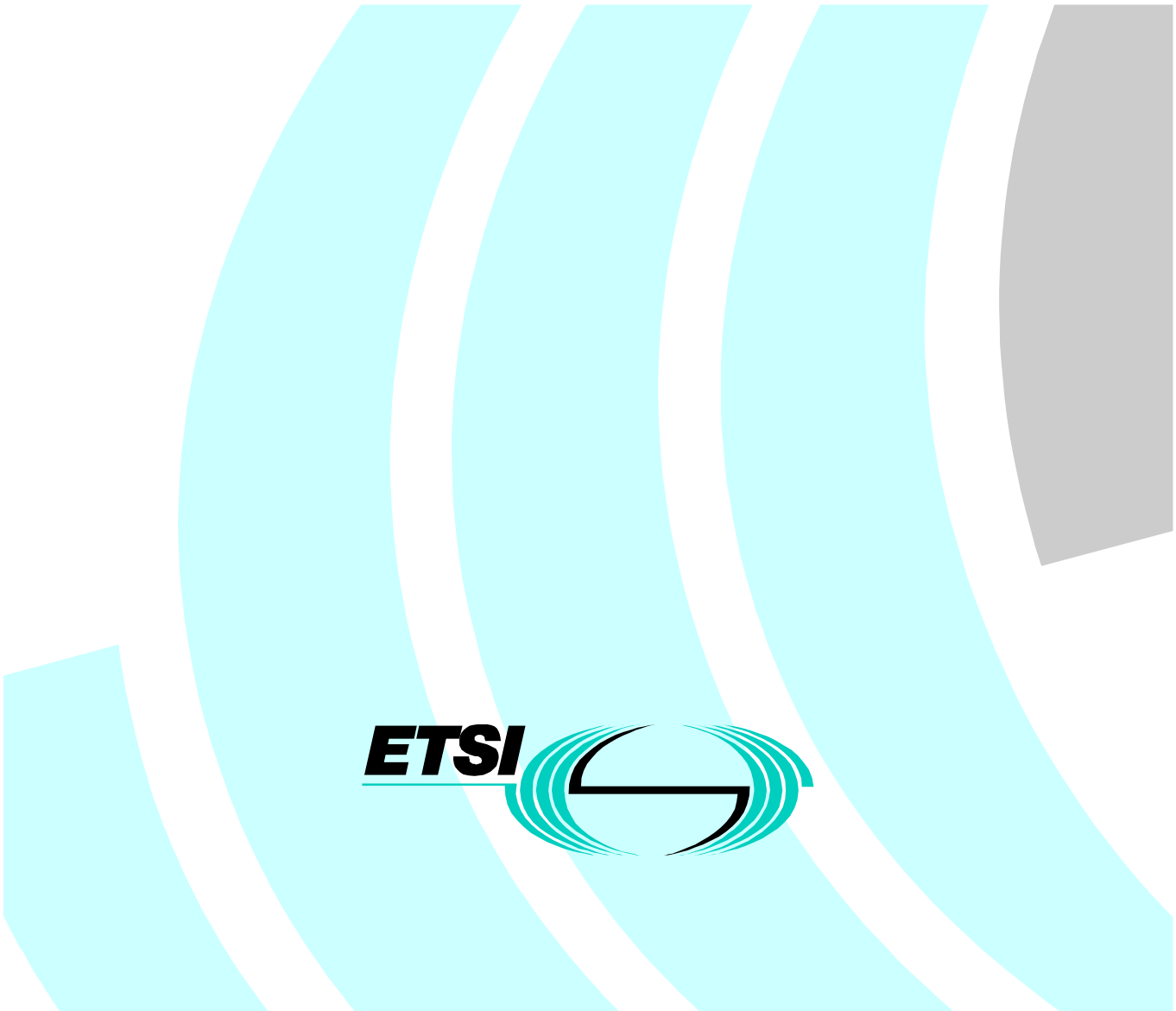
# ETSI TR 101 750 V1.1.1 (1999-11)

*Technical Report*

**Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Security; Studies into the Impact of lawful interception**



Reference
DTR/TIPHON-08001 (g7c00ics.PDF)

Keywords
IP, network, security, VoIP

***ETSI***

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

# Contents

# 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 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://www.etsi.org/ipr).

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 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 Report (TR) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

# Introduction

The present document has been produced by ETSI Project TIPHON of the European Telecommunications Standards Institute (ETSI) in close alliance with the ad-hoc group for TIPHON Security of ETSI Technical Committee Security (TC-SEC) and the Lawful Interception Working Group of TC-SEC.

# 1 Scope

The present document describes the user (Law Enforcement Agencies) requirements for Lawful Interception and the impact in a TIPHON Implementation. It provides an abstract of the requirements [6], [3] and outlines a study on the impact of Lawful Interception for TIPHON compliant systems.

The provision of lawful interception on the SCN part of a TIPHON network is already generally addressed and is not considered in the present document. The present document does consider lawful interception in an IP network.

NOTE: The present document is a pre-study to identify the impact of lawful interception and therefore should lead to a subsequent document which specifies a TIPHON system compliant mechanism to permit the provision of lawful interception according to national law and appropriate standards.

The provision of lawful interception is a requirement of national law, which is usually mandatory. From time to time, a network operator/access provider/service provider shall be required, according to a lawful authorization, to make available results of interception, relating to specific target identities, to a specific Law Enforcement Agency.

# 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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".

[2] ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[3] ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[4] ITU Recommendation H.323: "Packet-based multimedia communications systems".

[5] TR 101 300 (V1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of technical issues".

[6] Official Journal of the European Communities, 99/C329/01: "Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications".

# 3 Definitions and abbreviations

## 3.1 Definitions

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

**access provider:** access provider provides a user of some network with access from the user's terminal to that network.

NOTE 1: This definition applies specifically for the present document. In a particular case, the access provider and network operator may be a common commercial entity.

NOTE 2: The definitions from ETR 331 [3] have been expanded to include reference to an access provider, where appropriate.

**(to) buffer:** temporary storing of information in case the necessary telecommunication connection to transport information to the LEMF is temporarily unavailable.

**call:** any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system. In this context a user may be a person or a machine.

**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.

**Gatekeeper:** Gatekeeper (GK) is an H.323 entity on the network that provides address translation and controls access to the network for H.323 terminals, Gateways and MCUs. The Gatekeeper may also provide other services to the terminals, Gateways and MCU such as bandwidth management and locating Gateways. (See also ITU-T Recommendation H.323 [4]).

**Gateway:** H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 terminals on the packet based network and other ITU terminals on a switched circuit network, or to another H.323 Gateway. Other ITU Terminals include those complying with recommendations H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.234 (GSTN), H.234M (Mobile) and V.70 (DSVD). (See also ITU-T Recommendation H.323 [4]).

**H.323 Terminal:** endpoint on the network which provides for real-time, two-way communications with another H.323 Terminal, Gateway, or Multipoint Control Unit (MCU). This communication consists of control, indications, audio, moving colour video pictures, and/or data between the two terminals. A terminal may provide speech only, speech and data, speech and video, or speech, data and video. (See also ITU-T Recommendation H.323 [4]).

**handover interface:** physical and logical interface across which the results of interception are delivered from a network operator / access provider / service provider to an LEMF.

**identity:** technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis.

**intercept related information:** collection of information or data associated with telecommunication services involving the TI, specifically call associated information or data (e.g. unsuccessful call attempts), service associated information or data (e.g. service profile management by subscriber) and location information.

**interception (or Lawful Interception):** action (based on the law), performed by a network operator / access provider / service provider, of making available certain information and providing that information to an LEMF.

NOTE 3: In this ETSI Standard the term interception is not used to describe the action of observing communications by an LEA (see below).

**interception interface:** physical and logical locations within the access provider's / network operator's / service provider's telecommunications facilities where access to the content of communication and intercept related information is provided. The interception interface is not necessarily a single, fixed point.

**interception measure:** technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations.

**interception subject:** person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted.

**internal intercepting function:** point within a network or network element at which the content of communication is made available.

**internal network interface:** network's internal interface between the Internal Intercepting Function and a mediation device.

**Law Enforcement Agency (LEA):** organization authorized by a lawful authorization based on a national law to receive the results of telecommunications interceptions.

**Law Enforcement Monitoring Facility (LEMF):** law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject.

**lawful authorization:** permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator / access provider / service provider. Typically this refers to a warrant or order issued by a lawfully authorized body.

**location information:** information relating to the geographic, physical or logical location of an identity relating to an interception subject.

**mediation device:** mechanism which passes information between a network operator / access provider / service provider and a handover interface.

**network element:** component of the network structure, such as a local exchange, higher order switch or service control processor.

**network Operator:** operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means.

**quality of Service:** quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

**reliability:** the probability that a system or service performs in a satisfactory manner for a given period of time when used under specific operating conditions.

**result of interception:** information relating to a target service, including the content of communication and intercept related information, which is passed by an access provider or network operator or service provider to an LEA. Intercept related information shall be provided whether or not call activity is taking place.

**service information:** information used by the telecommunications infrastructure in the establishment and operation of a network related service or services. The information may be established by an access provider, network operator, a service provider or a network user.

**service Provider:** natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network. A service provider need not necessarily run his own network.

**target Identity:** identity associated with a target service (see below) used by the interception subject.

**target identification:** identity which relates to a specific lawful authorization as such. This might be a serial number or similar. It is not related to the denoted interception subject or subjects.

**target Service:** telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception.

NOTE 4: There may be more than one target service associated with a single interception subject.

**telecommunications:** any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.

## 3.2 Abbreviations

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

| | |
|---|---|
| AP | Access Provider |
| CC | Content of Communication |
| GK | GateKeeper |
| GSM | Global System for Mobile communications |
| GW | Gateway |
| HI | Handover Interface |
| HI1 | Handover Interface Port 1 (for Administrative Information) |
| HI2 | Handover Interface Port 2 (for Intercept Related Information) |
| HI3 | Handover Interface Port 3 (for Content of Communication) |
| IIF | Internal Intercepting Function |
| INI | Internal network interface |
| IP | Internet Protocol |
| IRI | Intercept Related Information |
| ISDN | Integrated services digital network |
| LEA | Law Enforcement Agency |
| LEMF | Law Enforcement Monitoring Facility |
| LI | Lawful Interception |
| MF | Mediation Function |
| NWO | Network Operator |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| SCN | Switched Circuit Networks |
| SS | Supplementary Service |
| SvP | Service Provider |
| TI | Target Identity |

# 4 General Introduction

According to rules set by the laws and/or regulations of individual nations there is a need lawfully to intercept telecommunications traffic and provide intercept related information in modern telecommunications systems. (Due to the need of mutual legal assistance there is also a need of harmonizing the interception policy between the various nations. This also has an impact on the development of modern telecommunication systems and services).

In a telecommunications network interception usually takes place at a switching function close to the terminal. In the case of a PSTN SCN the interception often takes place at a local switch, to which the Target Identity (TI) is directly connected. Similarly, an IP network which directly supports terminals must make its own arrangements for interception of target identities at some suitable point within that IP network.

Lawful interception in SCNs is already covered by existing specifications and arrangements. The cases where lawful interception is necessary in an IP network shall be considered in step 1 and step 2 of this work. These cases correspond to scenarios 0, 1, 2 and 4 of TR 101 300 [5]. (In scenario 3 the IP network does not support terminals directly.)

The LEA requirements as they apply in Europe [6], ETR 331 [3] have been taken into account in the definition of the abstract handover interface ES 201 158 [1] and ES 201 671 [2]. The transformation into a technically possible solution for TIPHON compliant systems should be done in two steps.

**Step 1**

Step 1 is the content of the present document, being a study of the impact of user requirements on TIPHON compliant systems.

**Step 2**

Step 2 is the specification of an internal interception function for TIPHON compliant systems.

NOTE 1: Identified amendments and requirements shall be reported to ETSI TC Security, Working Group on Lawful Interception for revision of ES 201 158 [1] and ES 201 671 [2].

NOTE 2: Identified amendments and requirements shall be reported to appropriate national and transnational bodies, where such bodies have been identified.

The definition of the internal interception function for the provision of the result of interception should allow the technical facilities to be provided:

- with reliability;
- with accuracy;
- at low cost;
- with minimum disruption;
- most speedily;
- in a secure manner; and
- as part of business as usual.

# 5 User (LEA) requirements for Lawful Interception

This clause presents the user requirements related to the lawful interception of telecommunications with the LEA being the user. The relevant terms are defined in subclause 3.2. These user requirements are subject to national law and international treaties and should be interpreted in accordance with applicable national policies. In many countries the requirements are based on a document similar to [6], which was the starting point for the development of ETR 331 [3].

The following list of requirements is a collection of items, where several requirements might not correspond to the national laws and regulations of individual countries. The internal interception function should be configured in such a way that it can comply with the appropriate national requirements. A lawful authorization should specify a subset of requirements to be delivered on a case-by-case basis.

## 5.1 General requirements

1) The obligation of the NWO/AP/SvP as to which telecommunications traffic shall be intercepted is subject to national laws.

2) In accordance with the relevant lawful authorization a NWO/AP/SvP shall ensure that:

   a) the entire content of communication associated with a TI being intercepted can be intercepted during the entire period;

   b) any content of communication associated with a TI being intercepted which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire period;

   c) if the results of interception can not be delivered immediately to the relevant LEMF, then the content of communication and/or the intercept related information shall be buffered until they can be delivered;

   d) he shall not monitor or permanently record the results of interception.

3) The ability to intercept telecommunications shall be provided relating to all interception subjects operating permanently within a telecommunications system.

4) The ability to intercept telecommunications shall be provided relating to all interception subjects operating temporarily within a telecommunications system.

5) The results of interception relating to a target service shall be provided by the NWO/AP/SvP in such a way that any telecommunications that do not fall within the scope of the lawful authorization shall be excluded by the NWO/AP/SvP.

6) All results of interception provided to the handover interface shall be given a unique identification relating to lawful authorization.

## 5.2 Result of interception

The NWO/AP/SvP shall, in relation to each target service:

1) provide the content of communication, relating to each successful establishment of telecommunication;

2) remove any service coding or encryption which has been applied to the content of communication or the intercept related information at the instigation of the network operator or service provider (provide en clair);

3) provide the LEA with any other decryption keys whose uses include encryption of the content of communication, where such keys are available;

4) Intercept related information shall be provided:

   a) when a call set-up is attempted;

   b) when a call is established;

   c) when no successful call is established;

   d) on change of status;

   e) on change of service or service parameter (e.g. activation of call forwarding);

   f) on change of location.

NOTE: In the present document service should be taken to include so-called Supplementary Services (SSs).

5) Intercept related information shall contain:

   a) the identities that have attempted telecommunications with the TI, successful or not;

   b) identities used by or associated with the TI;

   c) details of services used and their associated parameters;

   d) information relating to status;

   e) time stamps.

6) The conditions mentioned above also apply to multi-party or multi-way telecommunication (e.g. conference calls) if and as long as the TI participates.

## 5.3 Location information

An LEA may request location information relating to locations, in a number of forms:

1) the current geographic, physical or logical location of the TI, when telecommunications activity (involving a call or a service) is taking place;

2) the current geographic, physical or logical location of the TI, irrespective of whether telecommunications activity (involving a call or a service) is taking place or not;

3) the current geographic, physical or logical location of an identity temporarily associated with a target service because of successful telecommunication or an unsuccessful attempt to establish telecommunication;

4) the current geographic, physical or logical location of an identity permanently associated with a target service.

NOTE: This information is expected to be made available from normal network operation. An example of geographic location might be a cell identity in mobile networks, an example of physical location might be a subscriber access number in any network and an example of a logical location might be a UPT number associated with a physical location.

## 5.4 Time Constraints

1) A NWO/AP/SvP shall make the necessary arrangements to fulfil his obligation to enable the interception and delivery of the result of interception from the point in time when the telecommunication installation commences commercial service.

2) The above requirement applies accordingly to the introduction of modifications to the telecommunication installation or to new operational features for existing telecommunications services to the extent of their impact on existing interception capabilities.

3) When a lawful authorization is presented a NWO/AP/SvP must co-operate immediately.

4) After a lawful authorization has been issued, provision of the results of interception of a TI shall proceed on a real-time or near real-time basis. In the case of near real-time the LEA should be able to force real-time (by means of emptying any buffers involved) if necessary.

## 5.5 Non disclosure

1) Network Operator / Access Provider / Service Provider:

   a) information on the manner in which interception measures are implemented in a given telecommunication installation shall not be made available to unauthorized persons;

   b) information relating to target identities and target services to which interception is being applied shall not be made available to unauthorized persons.

2) Manufacturers:

   - the NWO/AP/SvP shall agree confidentiality on the manner in which interception measures are implemented in a given telecommunication installation with the manufacturers of his technical installations for the implementation of interception measures.

## 5.6 Information Transmission and Information Protection Requirements

The technical arrangements required within a telecommunication installation to allow implementation of the interception measures shall be realized with due care exercised in operating telecommunication installations, particularly with respect to:

1) the need to protect information on which and how many target identities are or were subject to interception and the periods during which the interception measures were active;

2) the restriction to a minimum of staff engaged in implementation and operation of the interception measure;

3) to ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, interception and recording shall be carried out in operating rooms accessible only by authorized personnel;

4) the result of interception shall be delivered through a handover interface;

5) no access of any form to the handover interface shall be granted to unauthorized persons;

6) network operators and service providers shall take all necessary measures to protect the handover interface against misuse;

7) the result of interception shall only be transmitted to the LEMF as indicated in the lawful authorization when proof of the authority to receive of the LEMF, and proof of the authority to send of the interface, has been furnished;

8) authentication and proof of authentication shall be implement subject to national laws and regulations;

9) depending on certain interception cases (e.g. satellite interception) LEAs may require confidentiality measures to protect the transmission of the results of such interception. The use of encryption shall be possible;

10) in order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling interception, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input. The records, which are subject to national regulation, shall cover all or some of:

    a) the TI of the target service or target services concerned;

    b) the beginning and end of the activation or application of the interception measure;

    c) a reference to the lawful authorization.

11) the NWO/AP/SvP shall ensure that the records are tamper-proof and only accessible to specific nominated staff.

## 5.7 Internal Security

The NWO/AP/SvP shall configure the technical arrangements in his telecommunication installation so as to enable the interception of classified material within the meaning of applicable national laws. Staff enabling the interception of classified material should be subject to the relevant national security regulations.

## 5.8 Unchanged State of Service, etc.

1) Interception shall be implemented and operated in such manner that no unauthorized person can detect any change from the unintercepted state.

2) Interception shall be implemented and operated in such manner that no telecommunicating parties can detect any change from the unintercepted state.

3) The operating facilities of the target service shall not be altered as a result of any interception measure. The operating facilities of any other service shall not be altered as a result of any interception measure.

4) The Quality of Service (QoS) of the target service shall not be altered as a result of any interception measure. The QoS of any telecommunications service other than the target service shall not be altered as a result of any interception measure.

## 5.9 Technical Interface(s) and Format Requirements

1) The technical interface(s) shall provide the results of interception for the entire duration of the interception measure.

2) The interface(s) need to be implemented in those telecommunication networks for which the interception capability is required by national laws.

3) The configuration of the interface(s) shall ensure that it provides the results of interception.

4) The configuration of the interface(s) shall ensure that the QoS of the telecommunications traffic provided to the handover interface is not inferior to that offered to the target service for each particular call.

5) Each interception target shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.

6) The correlation between the content of communication and intercept related information must be unique.

7) LEAs require that the format for transmitting the intercepted telecommunications to the monitoring facility be a generally available format.

8) If an NWO/AP/SvP initiates encoding, compression or encryption of telecommunications traffic, LEAs require the NWO/AP/SvPs to provide intercepted telecommunications en clair.

9) LEAs require the content of communication to be provided across the handover interface in one of the formats outlined below, to be agreed in each case:

   a) the content of communication relating to two or more communicating parties is placed in a single telecommunications channel;

   b) the content of communications relating to two communicating parties is placed in two separate telecommunications channels;

   c) other configurations appropriate to the target service concerned.

10) The LEMF shall be informed of:

   a) the activation of an intercept measure;

   b) the deactivation of the intercept measure;

   c) any change of the intercept measure and;

   d) the temporary unavailability of the intercept measure.

## 5.10 Independence of the Network Operator/Access Provider/Service Provider

1) An NWO/AP shall ensure that the configuration of the telecommunication installation is such that he can implement and operate each ordered interception measure:

   a) without any involvement of third parties; and

   b) with the minimum of involvement of third parties if a) is not practicable.

2) An SvP shall ensure that:

   a) any NWO whose network is used by the SvP can co-operate in the provision of interception by the SvP, if required;

   b) any NWO involved in the provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorized target services to be intercepted;

   c) no other SvP is involved in the provision of interception facilities, unless that SvP is involved in the co-operative provision of service;

   d) any SvP involved in the co-operative provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorized target services to be intercepted.

## 5.11 Temporary obstacles to transmission

1) When transmission to the LEMF of the content of communication is, in exceptional cases, not possible the remainder of the results of interception (e.g. intercept related information) shall nevertheless be provided to the LEA (see also subclause 5.4 item number 4).

2) Prevention of the interception of the content of communication is not permitted.

## 5.12 Identification of the identity to be intercepted

1) Where the special properties of a given telecommunication service, and the justified requirements of the LEAs, necessitate the use of various identifying characteristics for determination of the telecommunications traffic to be intercepted, the NWO/AP/SvP shall ensure that the telecommunications traffic can be intercepted on the basis of these characteristics.

2) In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear determination of the telecommunications traffic to be intercepted.

## 5.13 Multiple interception measures

1) The NWO/AP/SvP shall ensure that more than one interception measure can be operated concurrently for one and the same identity. Multiple interceptions may be required for a single target service to allow monitoring by more than one LEA. The maximum number of simultaneous interceptions against the same interception subject is network specific and has to be defined in accordance with the handover interface specifications.

2) If multiple interceptions are active, NWO/AP/SvP shall take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.

3) The multiple interception measures may require information according to different lawful authorizations.

4) The arrangements made in a telecommunication network for the technical implementation of interception measures shall be set up, according to requirements, and configured so as to enable the elimination, without undue delay, of potential bottlenecks in a regional or functional part of that network when several interception measures are operated concurrently.

# 6 TIPHON scenarios and role model

## 6.1 TIPHON scenarios

The TIPHON scenarios where the interception takes place on the SCN side of the communication are out of the scope of the present document. Interception in SCNs is already covered by existing specifications.

Only cases where the interception takes place on the IP side of the communication (regardless whether the target is located on the calling or called side) shall be considered in step 1 and step 2 of this work.

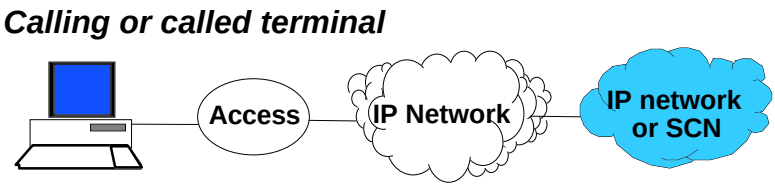



**Figure 1: Simplified model of TIPHON for the scope of the present document**

A target terminal may originate a call, terminate a call or be involved in service configuration. In general an IP terminal may participate in more than one activity at once. In principle, all such activities should be capable of being lawfully intercepted.

## 6.2 Functional block diagram

The following diagram shows the general interception configuration including the interworking between the internal interfaces and the handover interface. However, only the specification of the IIF and INI should be described in the step 2 document (see clause 4).

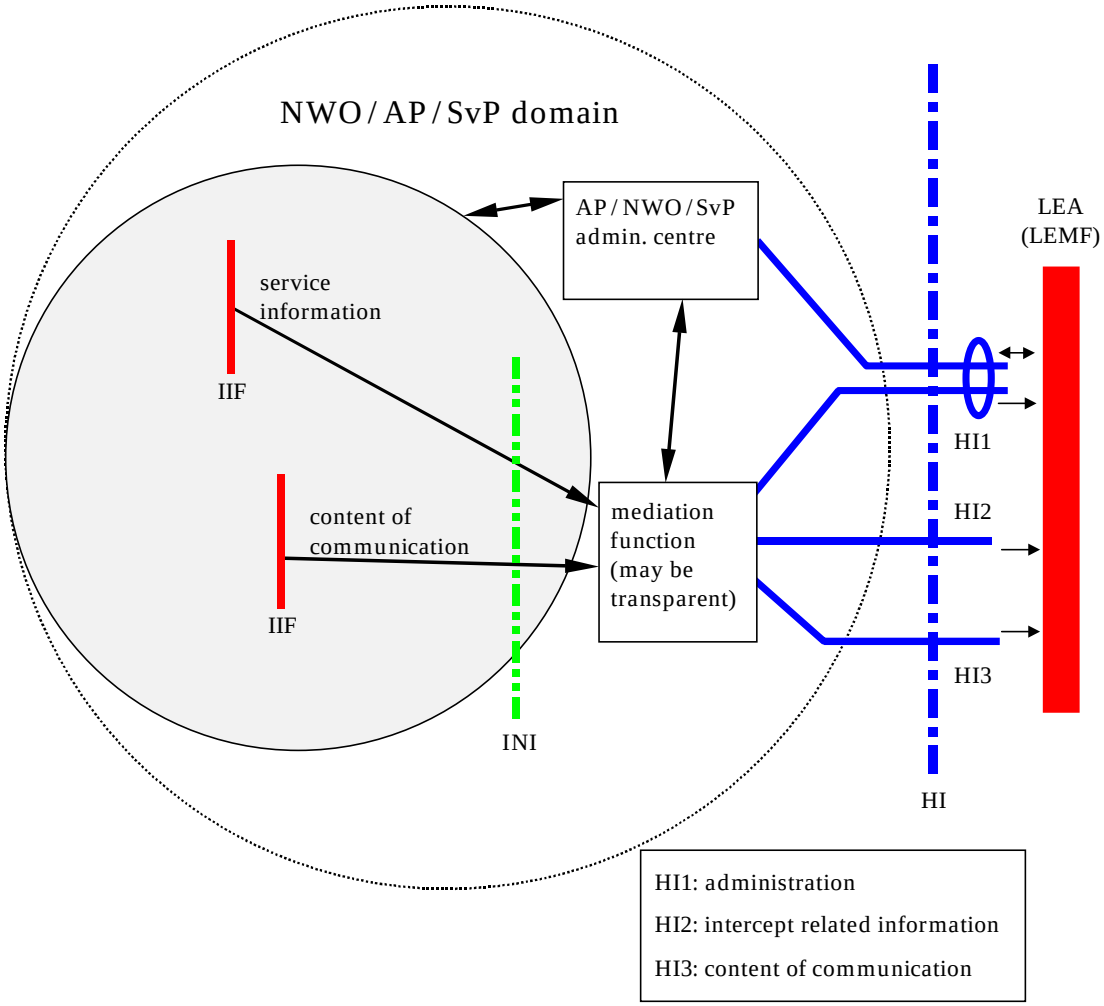



**Figure 2: Functional block diagram of lawful interception**

The functional components, as shown in figure 2, which facilitate the handover interface are shown in table 1.

**Table 1: Functional components of LI for TIPHON**

| Component | Description |
|---|---|
| IIF | An internal intercepting function within the access provider's, network operator's or service provider's domain. There may be more than one IIF involved in the provision of interception. |
| INI | an internal network interface within the access provider's, network operator's or service provider's domain which exists between an IIF and the Mediation Function (MF). |
| AP/NWO/SvP administration centre | the administration centre contacted via the port HI1 (which may be partly electronic, and partly paper based depending on circumstances) is used to set-up the interception action on the LEA request. |
| Mediation function | A function which selects, sequences and transforms information, including content of communication when necessary, between a number of IIFs and the handover interface (HI). Sometimes the MF may be a null function e.g. direct delivery of the content of communication to the LEMF via HI3 with no changes<br>For example, in a GSM network the MF would not transform A law speech as used in a simple call, but would be required to transcode to A law speech when direct coding is employed on a call from one GSM terminal to another |
| Delivery mechanism to LEA/LEMF | a) Intercept requests, status and alarm reports are transmitted between the administration centre and the LEA/LEMF.<br>b) The intercept related information is transmitted through the MF (may be transparent) to the LEMF.<br>c) The content of communication is transmitted through the MF (may be transparent) to the LEMF. |

# 7 Further work

1) Definition of TIPHON specific requirements for LI, to refine those given in [6] and [3].

2) Definition of reference points, where the interception can take place (in relation with the possible GW and GK configuration). Therefore it is necessary to distinguish between the two types of information related to interception:

   - intercept related information (IRI); and

   - content of communication (CC);

   and where these information are available within the TIPHON compliant network configuration.

3) Development of LI specific call scenarios and information flows.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | November 1999 | Publication |
| | | |
| | | |
| | | |
| | | |