Draft EN 301 040 V1.1.1 (1997-06)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface

Reference
DEN/TETRA-06027-1 (9mo00ico.PDF)

Keywords
TETRA, security, voice, data

ETSI Secretariat

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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights 4
Foreword 4
1 Scope 5
2 References 5
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 7
4 User (LEA) requirements - the administrative interface 8
4.1 Non-disclosure 8
4.2 Product of interception 9
4.2.1 Network validity of interception product 9
4.2.2 Identification of interception product 9
4.2.3 Format of interception product 9
4.2.4 Content of interception product 9
4.2.5 Auditing of interception product 10
4.3 Location information 10
4.4 Time constraints 11
4.5 Service transparency 11
4.6 LI interface instances 11
4.7 LI interface events 11
4.8 Identification of the identity to be intercepted 11
5 Stage 1 description of TETRA LI technical interface 12
5.1 Description 12
5.2 Procedures 12
5.2.1 Provision/withdrawal 12
5.2.2 Normal procedures 12
5.2.2.1 Activation/deactivation/registration 12
5.2.2.2 Invocation and operation 12
5.2.2.3 Interrogation 12
5.3 Interaction with TETRA supplementary services 12
5.4 Interaction with other supplementary services 12
5.5 Overall Structured Description Language (SDL) diagrams 13
Annex A (informative): Explanatory diagrams 14
A.1 General network arrangements 14
A.2 Service providers 14
A.3 Service across multiple SwMIs 15
A.4 Service across international borders 16
Annex B (informative): Overview of ITU-T Recommendations I.130 and I.210 18
B.1 Explanation of the terms and content of the items in the service prose definition and description 18
Annex C (informative): Bibliography 21
History 22

Intellectual Property Rights

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA), and is now submitted for the ETSI standards Public Enquiry phase of the ETSI standards Two-step Approval Procedure (TAP).

1 Scope

This European Standard (Telecommunications series) provides the requirements and stage 1 implementation for Terrestrial Trunked Radio (TETRA) systems in the area of Lawful Interception (LI) of communications. It provides a set of requirements relating to LI interfaces for use by Law Enforcement Agencies (LEAs) and state security agencies.

This present document is structured as follows:

- clause 4 outlines the essential requirements of the LEAs;
- clause 5 is an ITU Recommendation I.130 [3] (see annex B) type stage 1 technical description of the LI interface;
- annex A contains explanatory diagrams to assist the reader to understand the requirements;
- annex B summarizes the methods of ITU Recommendations I.130 [3] and I.210 [4];
- annex C contains a bibliography.

Pending national legislation not all requirements may be applicable in one individual nation.

The present document applies to TETRA services where access to the communication of Individual TETRA Subscriber Identities (ITSIs) is available in a network (Switching and Management Infrastructure (SwMI) or Radio Packet Data Infrastructure (RPDI)). Whilst this does not prohibit lawful interception of TETRA Direct Mode Operation (DMO) it removes the liability of network operators and service providers to provide an interception product when communication does not make use of their networks.

The present document does not define the operations or technical requirements of the Law Enforcement Monitoring Facility (LEMF).

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

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

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

[2] ETS 300 392-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice + Data; Part 2: Air Interface (AI)".

[3] ITU-T Recommendation I.130 (1988): "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[4] ITU-T Recommendation I.210 (03/93): "Principles of telecommunication services supported by an ISDN and the means to describe them".

[5] ITU-T Recommendation Z.100 (3/93): "CCITT Specification and description language (SDL)".

[6] ITU-T Recommendation Z.120 (10/96): "Message sequence chart (MSC)".

3 Definitions and abbreviations

3.1 Definitions

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

(to) buffer: The 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 TETRA system.

content of communication: The information exchanged between two or more users of a TETRA service whilst a call is established, excluding intercept related information. This includes information which may, as part of some TETRA service, be stored by one user for subsequent retrieval by another.

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

LI interface : A physical and logical interface across which the results of interception are delivered from a network operator/service provider to a LEMF.

NOTE 1: In ETR 331 [1] this interface is termed the handover interface. The term handover is used in TETRA systems to describe the maintenance of a call when the mobile party moves between cells.

intercept related information: A collection of information or data associated with TETRA services involving the target ITSI, specifically call associated information or data (e.g. user-to-user signalling information), service associated information or data (e.g. service profile management by subscriber) and location information.

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

NOTE 2: In the present document the term "interception" is not used to describe the action of observing communications by an LEA.

interception interface: The physical and logical locations within the network operator's/service provider's TETRA 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: A technical measure which facilitates the interception of TETRA traffic pursuant to the relevant national laws and regulations.

interception product: The sum of all traffic and additional data specified by the interception warrant that is delivered to the LEMF.

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

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

Law Enforcement Monitoring Facility (LEMF): A 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 communication and requiring co-operation from a network operator/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.

Private Mobile Radio (PMR): A radio system designed for a closed user group that is owned and operated by the same organ**iza**tion as its users.

Public Access Mobile Radio (PAMR): A radio system available to members of the general public generally by subscription. The owner and operator is unlikely to be the same as the user.

Public Network Operator (PNO): The operator of a public infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means.

NOTE 3: To avoid confusion the term TETRA Network Operator may be used to distinguish the operator of a TETRA system from the operator of a traditional public network.

Quality of Service (QoS): The quality specification of a TETRA channel, system, virtual channel, computer-TETRA 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 will perform 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 a network operator or service provider to an LEA. Intercept related information may be provided whether or not call activity is taking place.

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

NOTE 4: To avoid confusion the term TETRA service provider may be used to distinguish the operator of a TETRA system from the service provider in traditional public networks.

target Group TETRA Subscriber Identity (GTSI): The identity associated with a target service (see below) used by the interception subject where the interception subject is a group.

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

target service: A communication service associated with an interception subject and usually specified in a lawful author**iza**tion for interception.

NOTE 5: There may be more than one target service associated with a single interception subject.

target Terminal Equipment Identity (TEI): The identity associated with a target service (see above) used by the interception subject where the interception target is an equipment.

telecommunication: 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, photo-electronic or photo-optical system.

3.2 Abbreviations

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

BS	Base Station
DMO	Direct Mode Operation
GTSI	Group TETRA Subscriber Identity
ISDN	Integrated Services Digital Network
ISI	Inter-System Interface
ITSI	Individual TETRA Subscriber Identity
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MM	Mobility Management
MNI	Mobile Network Identity
MS	Mobile Station

PSTN	Public Switched Telephone Network
RPDI	Radio Packet Data Infrastructure
SAP	Service Access Point
SDL	Structured Description Language
SSI	Short Subscriber Identity
SwMI	Switching and Management Infrastructure
TEI	TETRA Equipment Identity
TS	Technical Specification
TETRA	TErrestrial Trunked RAdio

4 User (LEA) requirements - the administrative interface.

This clause presents the user requirements related to the lawful interception of TETRA with the LEA being the user. These user requirements are subject to national law and international treaties and should be interpreted in accordance with applicable national policies.

NOTE: The list of documents given in the Bibliography (annex C) have been referred to during the drafting of this present document but are not explicitly referenced. However these documents should be treated as essential background for the understanding of the context for this present document and may be considered as normative source material particularly in defining the legal and regulatory framework in which this present document is produced.

The network operator/service provider shall use best endeavours at all times to comply with the requirements of the LEA. The specific information to be made available shall be made clear by the LEA. The delivery of information to the LEA (in its designated LEMF) shall be as described in this present document.

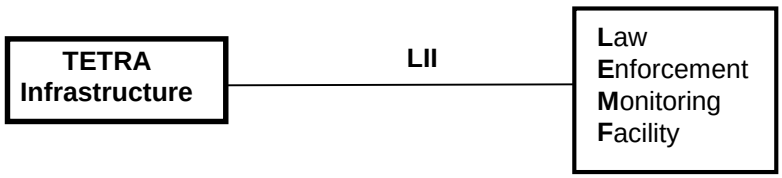

Figure 1: General reference model of lawful interception from user perspective

The general reference model of figure 1 shows that the LI interface lies between the LEMF and the TETRA infrastructure.

4.1 Non-disclosure

Information on the manner in which interception measures are implemented in a given TETRA installation shall not be made available to unauthorized persons.

NOTE: This present document provides the requirements of an implementation and any conformance statements alluding to this present document will be in the public domain and may not be protected. Details of how conformance is achieved should be private and protected.

Information relating to target identities and target services to which interception is being applied at any time in the life of the TETRA installation and as defined thereafter by the LEA shall not be made available to unauthorized persons.

The network operator/service provider shall agree confidentiality on the manner in which interception measures are implemented in a given TETRA installation with the manufacturers of his technical installations for the implementation of interception measures.

4.2 Product of interception

NOTE: The obligation of the network operator/service provider to provide an interception product is subject to national laws and the content of this present document cannot overrule those national laws.

The interception product shall be made available during the period specified by the interception warrant, at the LEMF side of the LI interface and shall contain for those targets and call types as specified in the warrant:

- the content of all calls originated by the target;
- the content of all calls addressed to the target;
- the content of multi-party calls in which to the best knowledge of the network operator/service provider the target is participating;
- the content of broadcast calls to a user population of which to the best knowledge of the network operator/service provider the target is a member.

A network operator shall provide data from the time commencing no earlier than the time at which the warrant is issued plus the time taken to set the interception measures in place which should be as short as possible.

4.2.1 Network validity of interception product

A network operator/service provider shall only provide an interception product for targets operating in their network irrespective of the target belonging to that network. If an interception target migrates to a second TETRA network there shall be no requirement for the home network operator/service provider to provide an interception product from the visited network.

4.2.2 Identification of interception product

The interception product provided at the LEMF side of the LI interface shall be given a unique identification that shall allow identification of the LEA, the target ITSI, network operator/service provider and the warrant reference.

4.2.3 Format of interception product

The network operator/service provider shall, prior to delivery of the interception product:

1) remove any service coding or encryption (i.e. air interface encryption, voice coding and channel coding) applied at the instigation of the network operator or service provider;
2) provide the LEA with decrypted material for applications where relevant keys and algorithms are available.

4.2.4 Content of interception product

The interception product shall contain (subject to national laws):

1) the identities that have attempted communication with the target ITSI, successful or not;
2) the identities that the target ITSI has attempted communication with, successful or not;
3) identities used by or associated with the target ITSI;
4) details of services used and their associated parameters;
5) those signals emitted by the target invoking additional or modified services;

NOTE 1: The above statement ensures that protocol acknowledgements (layer 2) and protocol retries are filtered away from the LI interface.

6) additional time-stamps for identifying the beginning, end and duration of the connection;
7) actual destination and intermediate directory numbers if call has been diverted;

8) the content of the communication from the target ITSI;

9) the content of the communication to the target ITSI;

10) location information;

11) advice of charge for provision of interception product.

The interception product shall apply to all call types if, and as long as, to the best knowledge of the network operator/service provider, the target ITSI is a participant.

For group calls, the GTSI shall be identified as being used by the ITSI where to the best knowledge of the network operator/service provider the target ITSI is a participant in the group. This may be achieved by recording the ATTACH/DETACH GROUP IDENTITY messages that dynamically associate an ITSI to a GTSI, or by defining a group as always attached to an ITSI. If a group requires dynamic attachment and the target ITSI has not explicitly attached then there is no association of ITSI to GTSI for that group.

NOTE 2: For further explanation of this topic see ETS 300 392-2 [2], subclauses 14.5.2 and 16.8.

4.2.5 Auditing of interception product

In order to prevent, and to trace, misuse of the technical functions integrated in the TETRA 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 some or all of the following items:

1) the target ITSI of the target service or target services concerned;

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

3) the LEMF to which the result of interception is routed;

4) an authenticator suitable to identify the operating personnel (including date and time of input);

5) a reference to the lawful authorization.

The network operator/service provider shall ensure that the records are tamper-proof and only accessible by authorized individuals.

4.3 Location information

A network operator shall provide to the best of their knowledge any location information that may be requested by the LEA and addressed within the initiating warrant. Such data should be within the normal operating parameters of the TETRA network and may take one or more of the following forms:

1) the current base station at which the target ITSI is registered;

2) the current line identity associated with a registered target ITSI;

3) the line or service identity to which the target ITSI is currently registered and to which calls are redirected.

The location information should be delivered at one or more of the following times:

1) with registration;

2) with interception product;

3) as specified by the LEMF.

If the TETRA network provides additional location tracking data to which the target ITSI subscribes such information may be provided in addition to the above.

4.4 Time constraints

The instance of the LI interface and communication shall be established to the LEMF as quickly as possible after issue of an interception warrant. Thereafter the interception product shall be delivered to the LI interface on a real-time or near real-time basis.

4.5 Service transparency

The LI interface shall be implemented and operated with due consideration for the following:

1) unauthorized persons should not be able to detect any change from the un-intercepted state;
2) communicating parties should not be able to detect any change from the un-intercepted state;
3) the operating facilities of any network service should not be altered as a result of any interception measure;
4) the quality of service of any network service should not be altered as a result of any interception measure.

4.6 LI interface instances

Each instance of the LI interface shall support the transmission of a single interception product. If an LEA requires a TETRA network to provide multiple interception products to one or more LEMFs these shall be delivered from separate instances of the LI interface. The preceding may be achieved by using separate physical communication channels for each product or by multiplexing many interception products onto a single physical communication channel. The correlation between the content of communication and intercept related information shall be unique.

4.7 LI interface events

The LEMF shall be informed by the TETRA network through the LI interface of the following events:

1) the activation of an intercept measure;
2) the deactivation of the intercept measure;
3) any change of the intercept measure;
4) the temporary unavailability of the intercept measure.

The LI interface shall be active for the period of the warrant. At the expiry of the warrant the LI interface shall remain active until all interception product relating to the target has been delivered. Such data may include an advice of charge from the network operator/service provider indicating the sum of resources used in providing the interception product.

4.8 Identification of the identity to be intercepted

The interception target shall be identified within a TETRA network by means of an ITSI. Groups of which the target is a member shall be identified as those groups to which the target's ITSI has made a group attachment. The groups are identified by GTSI. The attachment that identifies these groups may be requested by the MS with the target's ITSI, enforced by the SwMI or a permanent attachment; and provision shall be made for interception of communications within groups to which the target's ITSI is attached by any of these means. The group communications should cease being intercepted after such time that the SwMI deems the MS to no longer be attached to the group, e.g. by specific detachment, de-registration etc.

In some instances network addresses (ITSIs) may be provided in blocks to user groups (e.g. to fleet operators in which an ITSI is assigned to a vehicle and not a person). The network operator/service provider shall make every effort to identify an unique target identity based upon data present in the original warrant. If the network operator/service provider is unable to map an unique address to the characteristics of the target defined in the interception warrant the LI interface shall not be invoked.

In some instances the target may be a particular equipment identified by its Terminal Equipment Identity (TEI). The network operator/service provider shall in such instances invoke the Mobility Management (MM) service to use the TEI PROVIDE protocol service to identify the ITSI using the target equipment where the use of such a service does not break the rules of service transparency given in subclause 4.5.

5 Stage 1 description of TETRA LI technical interface

5.1 Description

The technical implementation of LI interface shall take its operational requirements from clause 4 of this present document.

5.2 Procedures

5.2.1 Provision/withdrawal

The LI interface service shall always be provided.

5.2.2 Normal procedures

5.2.2.1 Activation/deactivation/registration

The LI interface shall be activated upon issue of a valid interception warrant from an LEA. The LI interface shall be deactivated when the interception warrant expires or as defined by the LEA.

5.2.2.2 Invocation and operation

The LI interface shall be invoked when the target ITSI registers to the network and maintained until the ITSI de-registers from the network.

5.2.2.3 Interrogation

Interrogation shall be possible only from an authorized user.

An authorized user for the purposes of interrogation is one who is allowed by both LEA and the network operator/service provider to administer the LI interface.

5.3 Interaction with TETRA supplementary services

There shall be no interaction.

5.4 Interaction with other supplementary services

There shall be no interaction.

5.5 Overall Structured Description Language (SDL) diagrams

NOTE: In the SDL below, arrows to and from the right indicate data transmitted to the LEA/LEMF and data received from the LEA/LEMF respectively. Arrows to and from the left indicate data transmitted to the SwMI/RPDI and received from the SwMI/RPDI respectively.

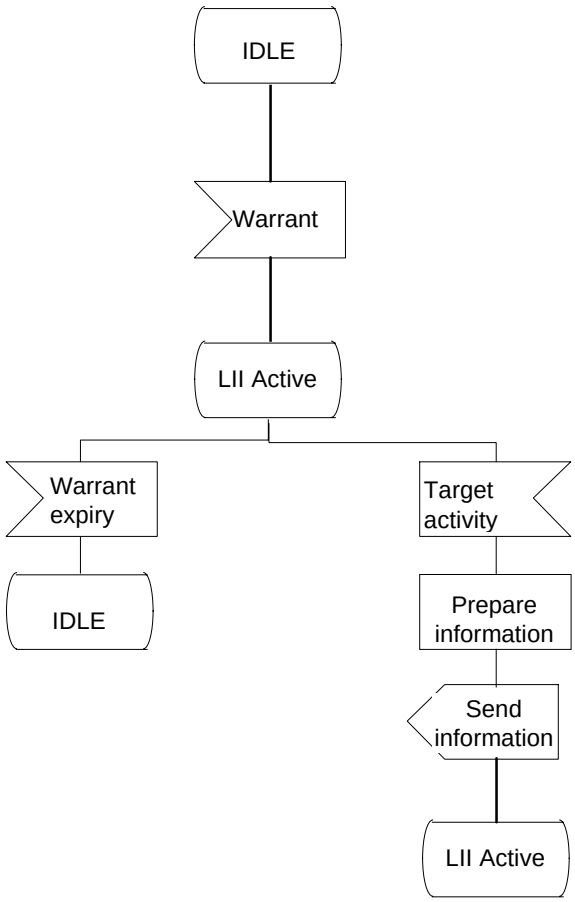

Figure 2: Overall SDL of LI interface

Annex A (informative): Explanatory diagrams

These diagrams are intended to be illustrative of the abstractions employed, and are not intended to limit the scope of this present document.

A.1 General network arrangements

The general arrangement for a network which is capable of providing interception facilities is as shown below:

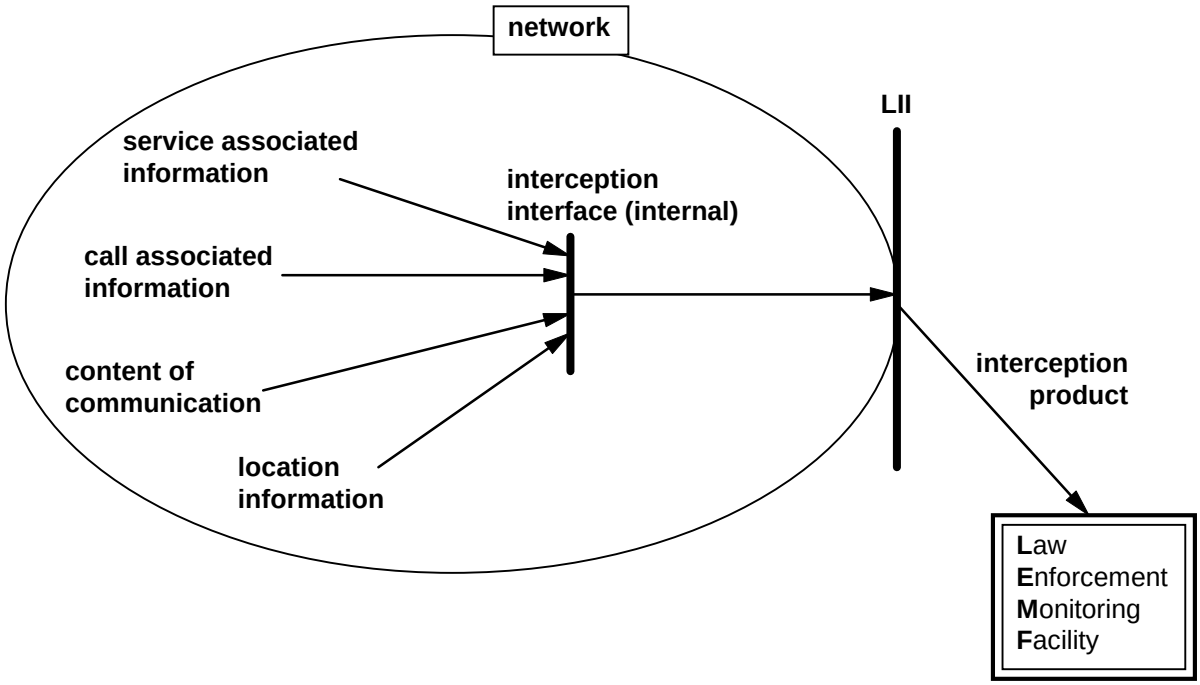

Figure A.1: General network arrangements for interception

Information relating to some target service is collected within the network at an interception interface. This information is then passed to an optional buffer, depending on specific circumstances, and then to a LI interface. From the LI interface information is then passed to the LEMF.

The information collected includes some or all of:

- the content of communication;
- call associated data;
- service associated data;
- location information.

A.2 Service providers

A service provider is an entity which takes advantage of the connectivity offered by a network provider to offer some service which the network's connectivity on its own is otherwise incapable of providing. Depending on circumstance, a service provider may be part of the same organization which operates a network or the service provider may belong to a different organization. The service provider relies on the co-operation of the network operator to deliver their service to their customer. The service provider may also provide some services with the assistance of other service providers.

The services which a service provider may offer are essentially unlimited. Possibilities include:

- voice storage services;
- personal numbers;
- card calling services;
- short data message services;
- data applications;
- dispatching services.

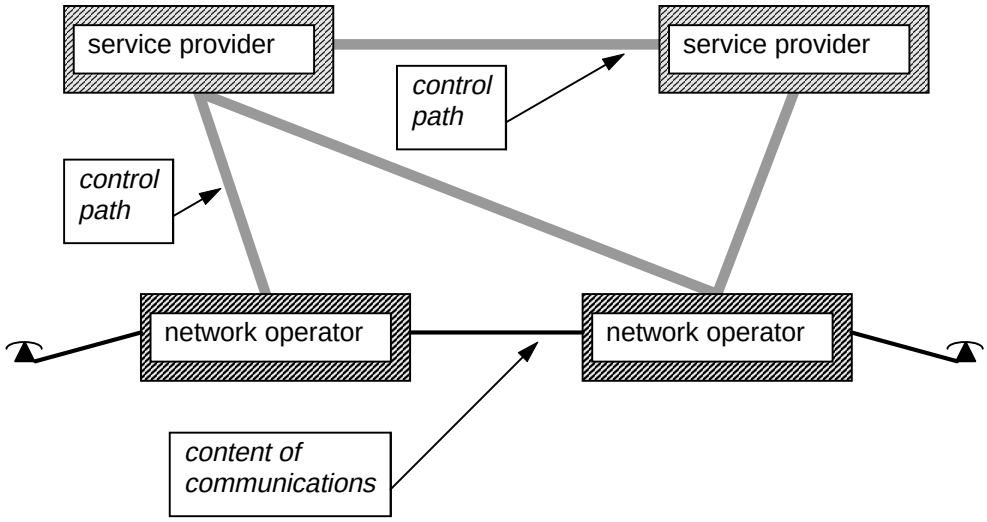

Figure A.2: Service provider relationship to a network operator

Figure A.2 shows that, in general, a service provider has no direct access to the content of communications.

A.3 Service across multiple SwMIs

The following diagram illustrates interception of communication with a Mobile Station (MS) which is registered on its home SwMI:

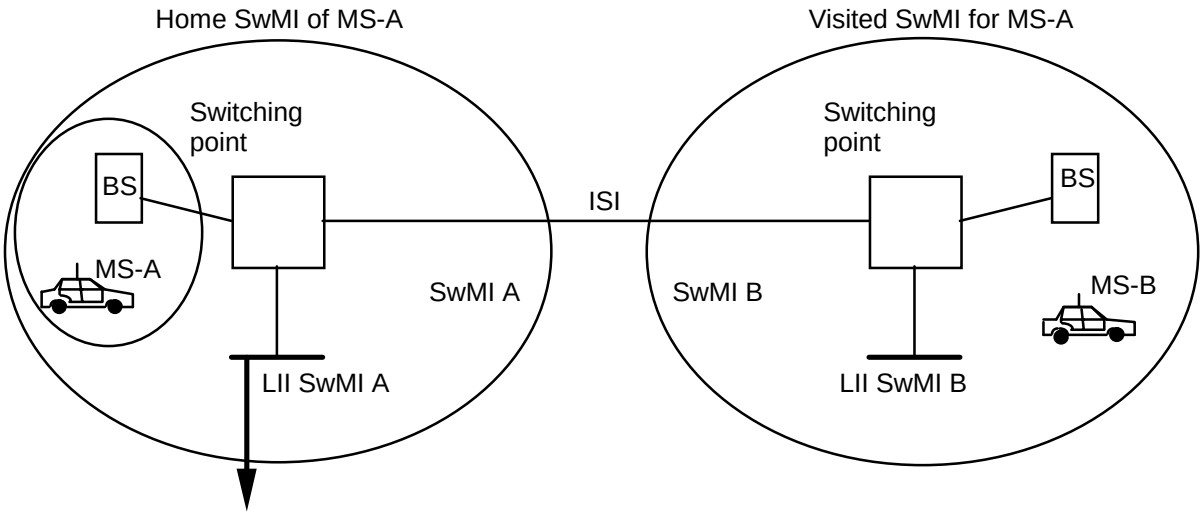

Figure A.3: Service interception with call between 2 SwMIs, target in home SwMI

If the interception target is MS A, the handover interface of SwMI A can provide information on Location Area (LA) A; and that communication is with MS B located in SwMI B; but does not know the LA for MS B. Handover interface of SwMI B is not able to provide interception information as interception target MS A is not registered on SwMI B.

The following diagram illustrates the alternative case, when an MS is registered on a SwMI that is not his home SwMI:

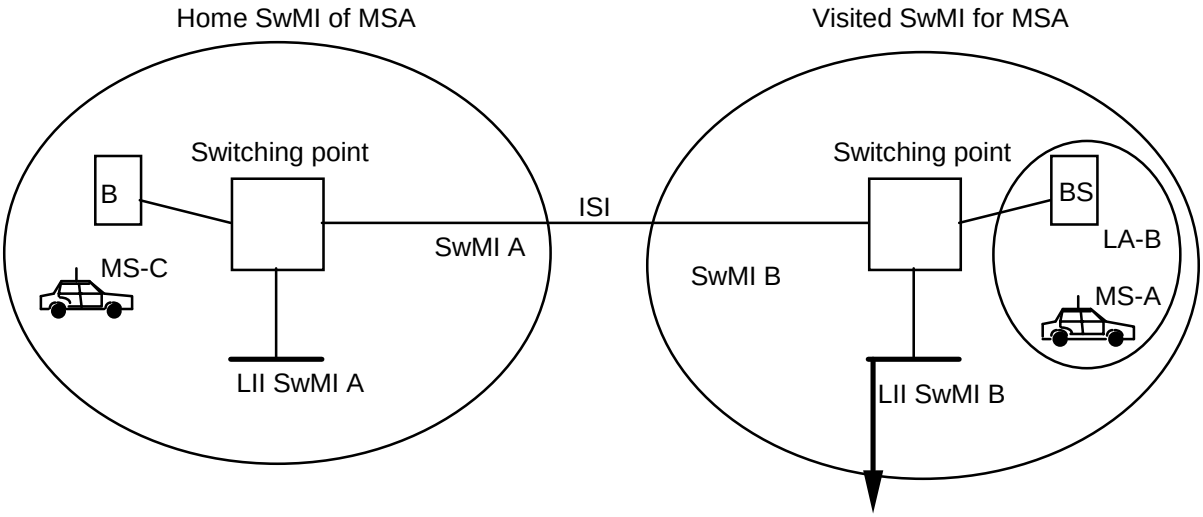

Figure A.4: Service interception with call between 2 SwMIs, target in vSwMI

If the interception target is MS A, now roamed to visited SwMI B, the handover interface of SwMI A can no longer provide information as the MS is out of his home SwMI. The handover interface of SwMI B can provide information on MS A, including the LA B details. If the MS is in communication with MS C, located on MS A's home SwMI, only the interface of SwMI B can provide information concerning MS C, as information can only be associated with the target for interception, MS A.

A.4 Service across international borders

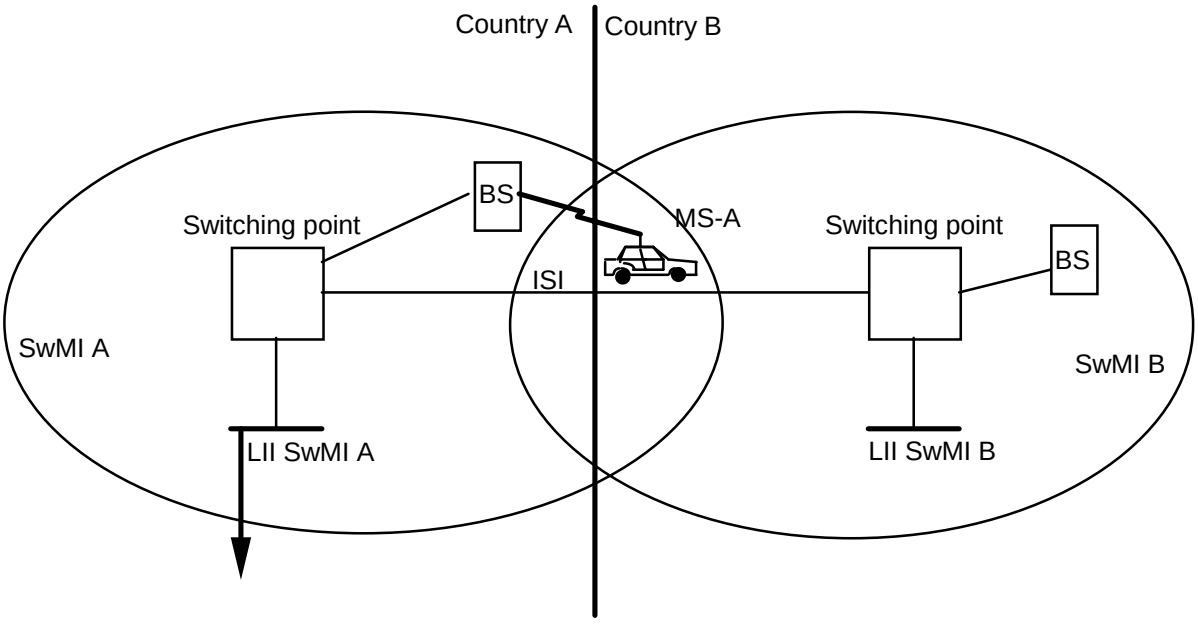

Figure A.5: Service interception in a single SwMI with target on foreign territory

If the interception target MS A is operating from within the borders of country B, but is registered on SwMI A and making use of cross-border coverage, all interception information shall be present at the handover interface of SwMI A, not that of SwMI B.

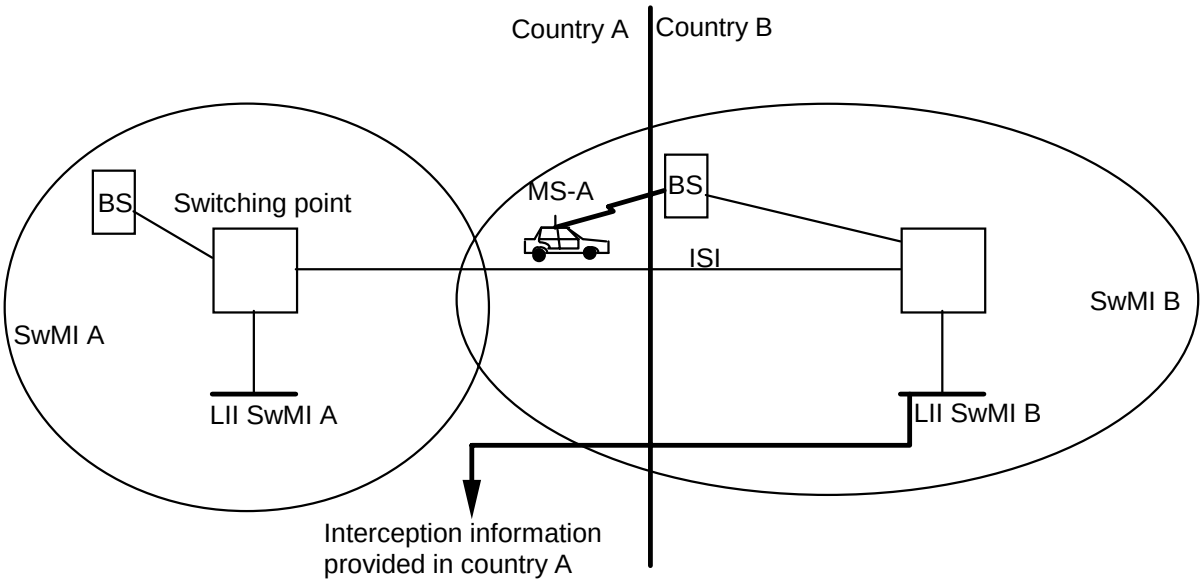

Figure A.6: Service interception in a single SwMI with target and LEMF on foreign territory

If a service provider uses a SwMI based in a foreign country, country B, to provide service across a border into the home country, country A, for geographical coverage or other reasons, he may be required to provide lawful interception information within country A. This shall be achieved by extending the handover interface of the foreign SwMI, SwMI B, into country A.

Annex B (informative): Overview of ITU-T Recommendations I.130 and I.210

The ITU Recommendations provide a means of describing services with a common vocabulary and syntax. When such methods also use SDL (ITU Recommendation Z.100 [5]) and Message Sequence Charts (ITU Recommendation Z.120 [6]) and the attribute method of service description suggested in ITU Recommendation I.210 [4] there is a large common base.

However such methods are not natural in all systems and may require to be supported by means of other formal and semi-formal models and methods of description.

The following text is taken from ITU Recommendation I.210 [4] and summarized where appropriate.

The method used for the characterization of telecommunication services is described in ITU Recommendation I.130 [3]. Within this method the first stage is an overall service description from the user's point of view. In stage 1 there are three steps:

- Step 1.1: Prose service definition and description;
- Step 1.2: Static description of the service using attributes;
- Step 1.3: Dynamic description of the service using graphic means.

Together these three steps define the service characteristics as they apply at a given reference point where the customer accesses the service.

B.1 Explanation of the terms and content of the items in the service prose definition and description

The following text is taken from ITU-T Recommendation I.210 [4], annex A, clause A.2:

"1 Definition

This clause provides a short description of the service in terms of the perceptions of the user receiving the service and any other users involved in the service.

2 Description

This clause expands on the definition and summarizes the operation of the service in a generic form which does not constrain terminal or network design. It is intended to allow an understanding of the service without regard to implementation. It also includes any specific terminology used within the prose definition and description, and any qualifications. For basic services this clause details the applications which could utilize the service whilst for supplementary services this clause details their applicability to particular telecommunication services.

3 Procedures

These procedures relate to all actions between the user(s) and the network during the period that the service is available.

3.1 Provision/withdrawal

This subclause describes the means by which the service is made available by the service provider, e.g. it may be generally available to all customers, or only be available to those customers who have made a prior arrangement.

3.2 Normal procedures

The paragraphs under this subclause describe the normal procedures for activation, deactivation, registration, invocation and operation for the service as appropriate. This subclause describes only the successful outcome of each procedure, and the procedures which are executed as a result of such successful outcomes. The procedures are described in a time-based sequence of events. They describe the interactions of the users involved in the service with the service provider and with each other which lead to, and are elements of, the successful operation of the service.

3.2.1 Activation/deactivation/registration

The procedures for activation, which is the operation of bringing the service into the "ready for invocation" state, and deactivation, which is the complementary action, are described in this subclause. For some services there may be a specific user procedure to allow activation and deactivation as necessary, whilst for others the service is permanently activated on provision and thus no procedure is provided.

3.2.2 Invocation and operation

This subclause describes the procedures for invocation, which is the action and conditions under which the service is brought into operation; in the case of a supplementary service this may only be on a particular call. It should be noted that although a supplementary service may be activated, it may not necessarily be invoked on all calls (invocation takes place either subsequent to or simultaneously with activation).

In the case of basic services this subclause describes the events, perceived at the Service Access Point (SAP), during the establishment, information transfer and clearing phases.

Operation is the procedure which occurs once a service has been invoked. In the case of a supplementary service this is described in terms of the way in which the supplementary service modifies/enhances the network's treatment of a call. This description gives details of the significant actions of the network, treated in principle as a single entity, and the perception of the users involved on the call. It includes details of the information exchanged between the network and relevant users and the indications given to each user, by the network, concerning the states of the call.

3.2.3 Interrogation/editing

Interrogation is the facility which enables a served user to determine, from the service provider, the current status of a particular service. Whether this facility is provided for the service being described, and if so, the procedures that accompany it, are detailed in this subclause.

Editing describes the process whereby any registered information specific to a service may be erased or modified by the served user.

3.3 Exceptional procedures

The paragraphs under this subclause describe the exceptional procedures which result in an unsuccessful outcome of the call. Included within this description are the details for such situations as invalid user action and the handling of certain network and interface conditions. For the case of basic services this includes the handling of such network conditions as congestion.

3.4 Alternative procedures

The subclauses under this subclause describe any alternative procedures, where available, for each of the items shown under subclause 3.2. These either allow an alternative way of activating or invoking the service, or detail a possible alternative treatment of the call by the network.

3.5 Verification

This subclause describes the facilities that are provided by the network to enable the subscriber to verify the operation of the service once it has been activated. Not all services allow provision for verification of the operation of the service.

4 Networking capabilities for charging

This subclause details only those charging aspects specific to the service in question and includes, where necessary, both static (subscription) and dynamic (call related) aspects.

5 Inter-working requirements

This subclause describes special aspects of the individual service, if the service is used in a connection which exists partly inside and partly outside a given ISDN, or which, for certain operational aspects, routes through more than one ISDN."

Annex C (informative): Bibliography

- Official Journal of the European Communities, 99/C329/01: "Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications".
- ETR 363: "Digital cellular telecommunications system; Lawful Interception requirements for GSM (GSM 10.20 version 5.0.1)".
- ETS 300 393-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 1: General network design".
- ETS 300 393-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 2: Air Interface (AI)".
- ETR 086-3: "Radio Equipment and Systems (RES); Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".
- ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic reference model - Part 2: Security Architecture".
- ETS 300 392-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice + Data; Part 7: Security".
- ETS 300 392-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice + Data; Part 1: General network design".
- prETS 300 393-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security".
- prETS 300 396-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 1: General network design".
- prETS 300 396-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 2: Radio Aspects".
- prETS 300 396-3: "Radio Equipment and Systems (RES); Trans European Trunked Radio (TETRA) systems; Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol".
- prETS 300 396-6: "Radio Equipment and Systems (RES); Trans European Trunked Radio (TETRA) systems; Direct Mode Operation (DMO); Part 6: Security".
- ETR 330: "Security Techniques Advisory Group (STAG); A guide to the legislative and regulatory environment".
- CM(95)101: "Council of Europe Recommendation on Problems of Criminal Procedural Law connected with Information Technology", Strasbourg, 31 July 1995, (adopted 7-8 September 1995).

History

Document history				
V1.1.1	June 1997	Public Enquiry	PE 9744:	1997-06-06 to 1997-10-31