ETSI

ETSI TECHNICAL REPORT

ETR 331

December 1996

Source: ETSI TC-STAG

Reference: DTR/NA-002310

ICS: 33.020

Key words: Security

Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Security Techniques Advisory Group (STAG) of the European Telecommunications Standards Institute (ETSI) in view of the growing need of standardization in the area of lawful interception of telecommunications. This ETR describes in general the user requirements regarding to an interception handover interface which, in a later stage, will be translated into the technical design of this interface in the form of an European Telecommunication Standard (ETS).

Blank page

1 Scope

This ETSI Technical Report (ETR) provides guidance for ETSI bodies in the area of co-operation by network operators/service providers with the lawful interception of telecommunications. It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies. Requirements with regard to telecommunications services provided from areas outside national frontiers are not fully developed yet and therefore only some preliminary requirements have been annexed for information.

This ETR describes the requirements from an Law Enforcement Agency's (LEA's) point of view only.

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

These requirements will be used to derive specific network requirements and furthermore to standardize handover interfaces.

2 References

For the purposes of this ETR, the following references apply:

[1] ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislation, recommendations & guidelines governing the provision of security features".

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

3 Abbreviations and Definitions

3.1 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

ATM	Asynchronous Transfer Mode
CAMEL	Customized Applications for Mobile networks Enhanced Logic
DCS 1800	Digital Cellular System - 1 800 MHz
GSM	Global System for Mobile communications
IN	Intelligent Network
IP	Intelligent Peripheral
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
POTS	Plain Ordinary Telephone Service
SMDS	Switched Multimegabit Data Service
STAG	Security Techniques Advisory Group

3.2 Definitions

The following terms might be defined slightly different in other standards or recommendations. For the purposes of this ETR, however, the following definitions apply:

(to) buffer: The temporary storing of information in case the necessary telecommunication connection to transport information to the Law Enforcement Monitoring Facility (LEMF) is temporarily unavailable.

call: Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system.

content of communication: The 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.

identity: A 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.

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

intercept related information: A collection of information or data associated with telecommunication services involving the target identity, 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 (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: In this ETR the term interception is not used to describe the action of observing communications by an LEA (see below).

interception interface: The physical and logical locations within the 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: A technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations.

interception subject: A person or persons, specified in a lawful authorization, whose telecommunications 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 telecommunications 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 telecommunications 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.

network operator: The 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: The 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 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 shall be provided whether or not call activity is taking place.

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

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

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

NOTE: 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, photoelectric or photooptical system.

4 General Introduction

According to rules set by the laws of individual nations as well as decisions of the European Union, there is a need to lawfully intercept telecommunications traffic and intercept related information in modern telecommunications systems. With the aim of harmonizing the interception policy in the member states, the Council of the European Union adopted a set of requirements [2], with the aim of feeding them into national legislation. The LEA requirements have to be taken into account in defining the abstract handover interface (see annex A).

A transformation into technically possible solutions has to take place; this is done in several steps.

Step 1

Step 1 is the definition of user requirements with the LEAs being the users and therefore will be done in close co-operation with the law enforcement and state security agencies. An ETSI STAG ad hoc group on legal interception has produced this ETR being part of step 1.

Step 2

In a further step the network requirements will be derived from the step 1 document. This may be done with assistance from (S)TCs concerned. This step is the Stage 1 description of the lawful interception handover interface(s). The aim is to establish one set of harmonized network requirements.

This step will also be done by STAG, but in close co-operation with (S)TCs concerned. It is planned to publish the results as an ETS.

Step 3

This step encompasses the Stage 2 and Stage 3 descriptions of the interface(s). It will lead to one (or more) concrete models, supporting the abstract model for specific products and services. The number of handover interface(s) should be limited. This work should be carried out by (S)TC Security or Plenary Groups concerned rather than by STAG.

The definition of a handover interface for the delivery of the results of lawful 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;
- as part of business as usual.

5 Architecture

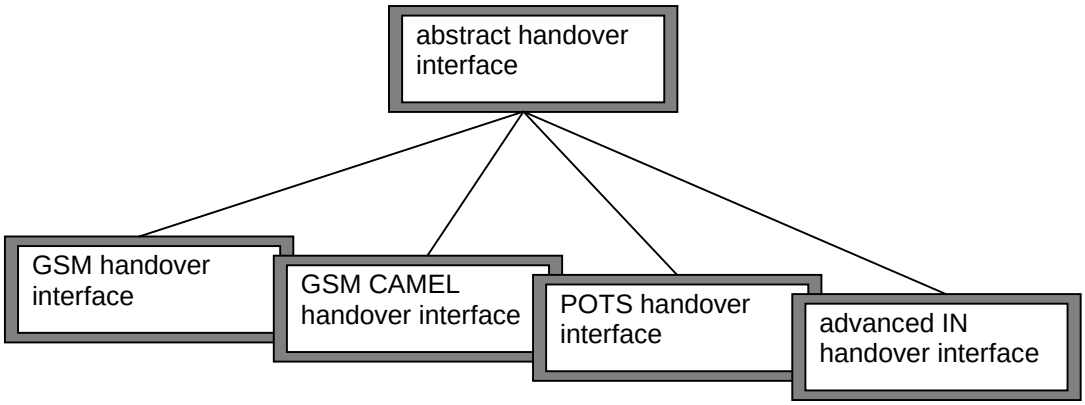
This clause provides some high level explanatory information on possible examples of handover interfaces and their relation to the abstract handover interface (see figure 1).

The interface would take a two layer form:

- an abstract model of the handover and the administration of lawful interception;
- a minimum set of concrete interfaces which support the abstract model for specific products and services, or combinations, such as:

    - 64 kbit digital bearers (speech, digital data, etc.);
    - low bit-rate bearers;
    - Switched Multimegabit Data Service (SMDS) bearers (very high bit-rate);
    - Asynchronous Transfer Mode (ATM) (whole families of bit rates);
    - point-to-point calls;
    - broadcast calls;
    - store-and-forward services;
    - etc.

Such a form allows rapid development of the enhancements required as networks and their associated services grow and evolve. All networks will use the same abstract model, but the concrete interfaces will be enhanced to cope with new networks features, such as the use of Intelligent Network (IN) Intelligent Peripherals (IPs).



CAMEL: Customized Applications for Mobile networks Enhanced Logic
POTS Plain Ordinary Telephone Service

Figure 1: Relationship of possible handover interfaces

6 User (LEA) requirements

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.

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

6.1 General requirements

1) The obligation of the network operator/service provider as to which telecommunications traffic shall be intercepted is subject to national laws.

2) In accordance with the relevant lawful authorization a network operator/service provider shall ensure that:

   a) the entire content of communication associated with a target identity being intercepted can be intercepted during the entire period;
   b) any content of communication associated with a target identity 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 (e.g. a PSTN subscriber).

4) The ability to intercept telecommunications shall be provided relating to all interception subjects operating temporarily within a telecommunications system (e.g. a visiting mobile subscriber).

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

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

6.2 Result of interception

The network operator or service provider 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 (i.e. en clair) and the intercept related information at the instigation of the network operator or service provider.

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

4) Intercept related information shall be provided:

   a) when a call setup 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 this ETR, service should be taken to include so-called supplementary services.

5) Intercept related information shall contain:

   a) the identities that have attempted telecommunications with the target identity, successful or not;
   b) identities used by or associated with the target identity;
   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 target identity participates.

6.3 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 target identity, when telecommunications activity (involving a call or a service) is taking place;

2) the current geographic, physical or logical location of the target identity, 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 a fixed network and an example of a logical location might be a UPT number associated with a physical location.

6.4 Time constraints

1) A network operator/service provider 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 network operator/service provider shall co-operate immediately.

4) After a lawful authorization has been issued, provision of the results of interception of a target identity 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.

6.5 Non disclosure

6.5.1 Network operator/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.

6.5.2 Manufacturers

The network operator/service provider 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.

6.6 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) where switched lines to the LEMF are used, such proof shall be furnished for each call set-up;

10) 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;

11) 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 target identity of the target service or target services concerned;
    b) the beginning and end of the activation or application of the interception measure;
    c) the LEMF to which the result of interception is routed;
    d) an authenticator suitable to identify the operating staff (including date and time of input);
    e) a reference to the lawful authorization.

12) The network operator/service provider shall ensure that the records are tamper-proof and only accessible to specific nominated staff.

6.7 Internal security

The network operator/service provider 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 will be subject to the relevant national security regulations.

6.8 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 of the target service shall not be altered as a result of any interception measure. The quality of service of any telecommunications service other than the target service shall not be altered as a result of any interception measure.

6.9 Technical handover interfaces and format requirements

1) The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure.

2) These handover interfaces need to be implemented in those telecommunication networks for which the interception capability is required by national laws.

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

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

5) The configuration of the handover interface shall be such that that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

6) 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.

7) The correlation between the content of communication and intercept related information shall be unique.

8) LEAs require that the format for transmitting the intercepted telecommunications to the monitoring facility be a generally available format. This format will be defined by the (S)TCs concerned in the specific technical interfaces with national variations where necessary.

9) If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, LEAs require the network operators/service providers to provide intercepted telecommunications en clair.

10) LEAs require network operators/service providers to be able to transmit the intercepted telecommunications to the LEMF via fixed or switched connections.

11) 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.

12) The LEMF will 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.

NOTE: The suitability of the various options depends on various factors which will change with time, and with the development of new services. The technical handover interfaces will be defined by the (S)TCs concerned.

6.10 Independence of the network operator or service provider

1) A network operator 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) A service provider shall ensure that:

a) any network operator whose network is used by the service provider can co-operate in the provision of interception by the service provider, if required;
b) any network operator 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 service provider is involved in the provision of interception facilities, unless that service provider is involved in the co-operative provision of service;
d) any service provider 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.

3) There is a general requirement of LEAs that services provided to their home countries from technical facilities outside those home countries can be intercepted, as if they had been provided from the home country.

NOTE: A draft set of requirements addressing this specific case is given in annex B.

6.11 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 6.4, item 4).

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

6.12 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 network operator/service provider 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.

6.13 Multiple interception measures

1) The network operator/service provider 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 the step 2 document.

2) If multiple interceptions are active, network operators/service providers 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.

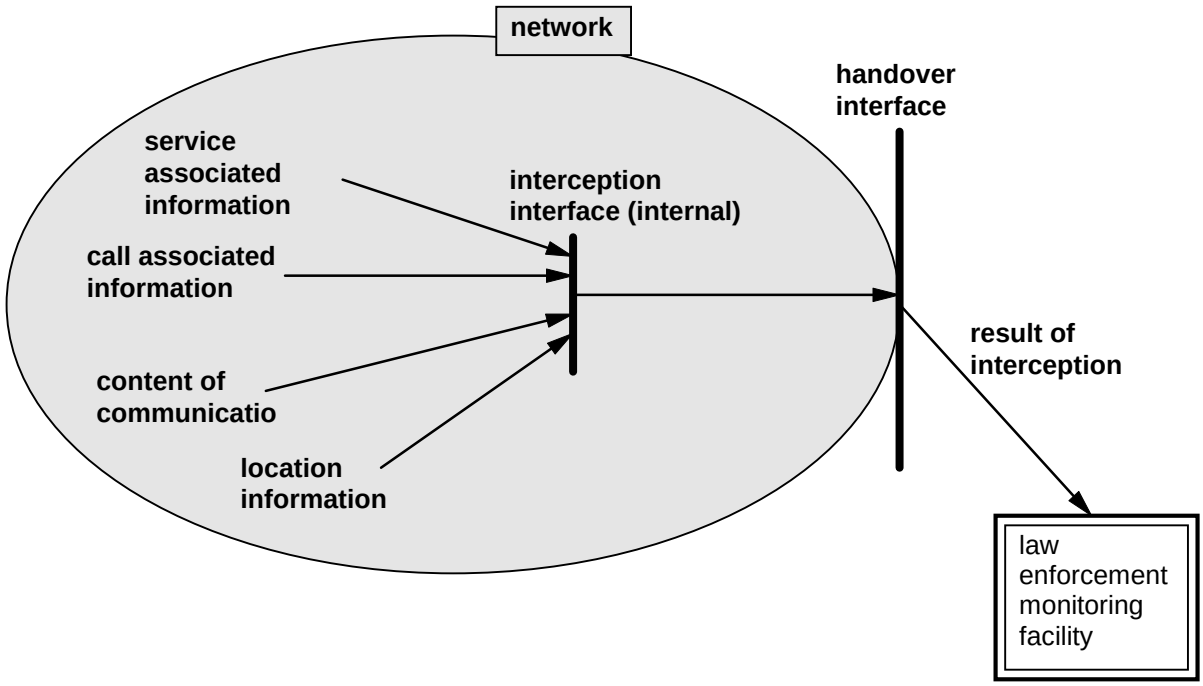
4) The arrangements made in a telecommunication network for the technical implementation of interception measures shall be set up, according to requirements, and configured so as to enable the elimination, without undue delay, of potential bottlenecks in a regional or functional part of that network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

Annex A: Explanatory diagrams

The diagrams provided in this annex are intended to be illustrative of the abstractions employed, and are not intended to limit the scope of the ETR.

A.1 General network arrangements

The general arrangement for a network which is capable of providing interception facilities is as shown in figure A.1.



NOTE: An optional mediation device within the network may be required to convert the information according to national laws.

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 handover interface. From the handover 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.

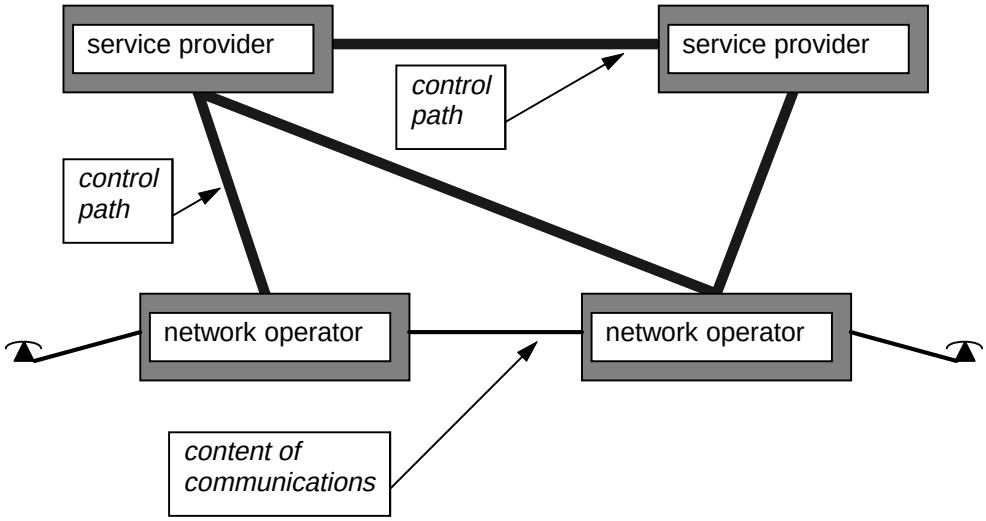


Figure A.2: Service provider relationship to a network operator

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

A.3 Home country service from a foreign territory

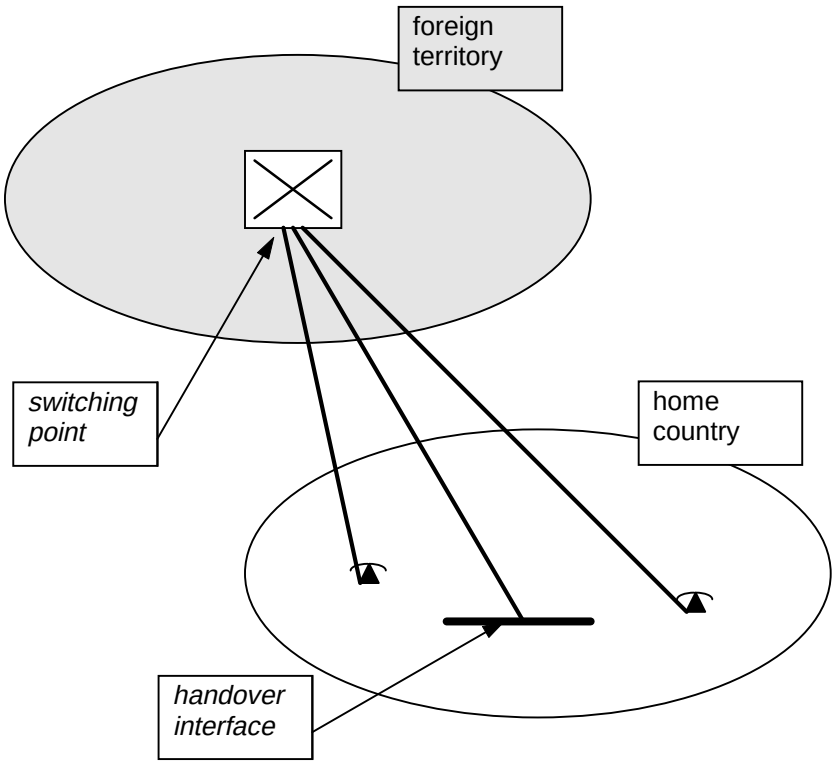


Figure A.3: Home country service, foreign territory switching

There may be a service provider involved, either in the home country or in a foreign territory, which need not be the same foreign territory that the switch point is located in.

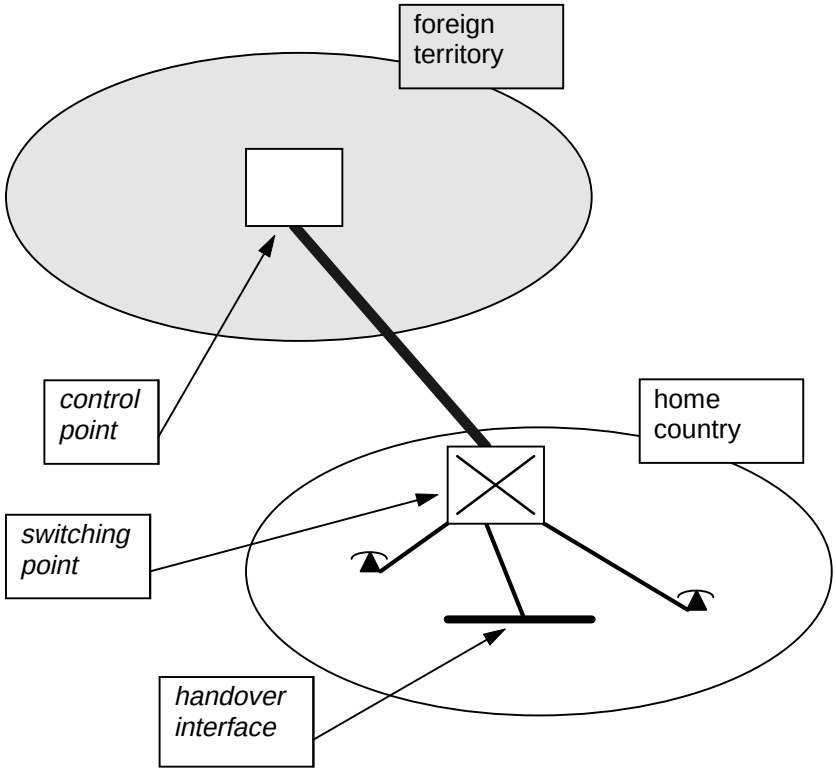


Figure A.4: Home country service, home country switching, foreign territory control

A.4 Identification of a target service

An LEA is concerned with an interception subject as, generally, a specific person or persons. From the viewpoint of the network operator/service provider that interception subject employs one or more target services. Associated with the interception subject's use of each target service is one or more target identities. These relationships are shown in figure A.5.

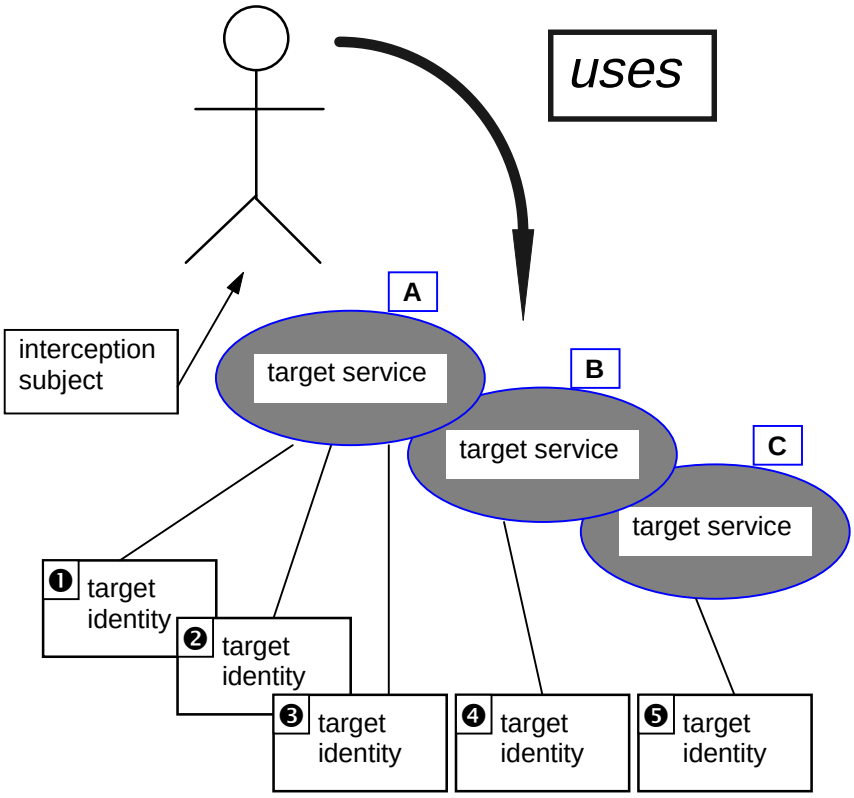


Figure A.5: Target service identification

A single interception subject makes use of three services: A, B and C. When using service A, the interception subject makes use of three identities: ❶❷❸. For service B, the interception subject uses identity ❹. For service C, the interception subject uses identity ❺.

The target identities for target service A could be three different e-mail addresses. Another target identity could be MSISDN, IMSI or IMEI in mobile network (typically Global System for Mobile communications (GSM), DCS 1800).

Annex B: Draft requirements for interception across national frontiers

As the telecommunications market in Europe develops, more services will be provided across national frontiers, using terrestrial or satellite communication links. To address this circumstances further requirements will be necessary. Initial study suggests that at least the following are relevant.

A network operator or service provider providing service to a home country from a foreign territory including international space above earth including satellite operators and those providing service via satellite facilities shall make arrangements such that:

a) interception is possible relating to activity of a target identity within a specific national domain;
b) if the interception interface lies in a foreign territory, then arrangements (both technical and organisational) are made such that interception is possible as if the interception interface were located in the home country;
c) the act of interception is kept discreet;
d) any result of interception is kept confidential, possibly by the use of encryption;
e) any other party involved in the provision of interception facilities is aware of the least detail of operational activities possible;
f) observation of the networks and services involved will not disclose the act of interception;
g) observation of the networks and services involved will not disclose the identities involved in any activity relating to interception;
h) observation of the networks and services involved will not disclose any result of interception;
i) relating to each home country there shall be a legal entity on whom lawful authorizations can be served.

NOTE: The above requirements are subject to further review, particularly with regard to questions of extraterritoriality.

History

Document history	
December 1996	First Edition

ISBN 2-7437-1143-4
Dépôt légal : Décembre 1996