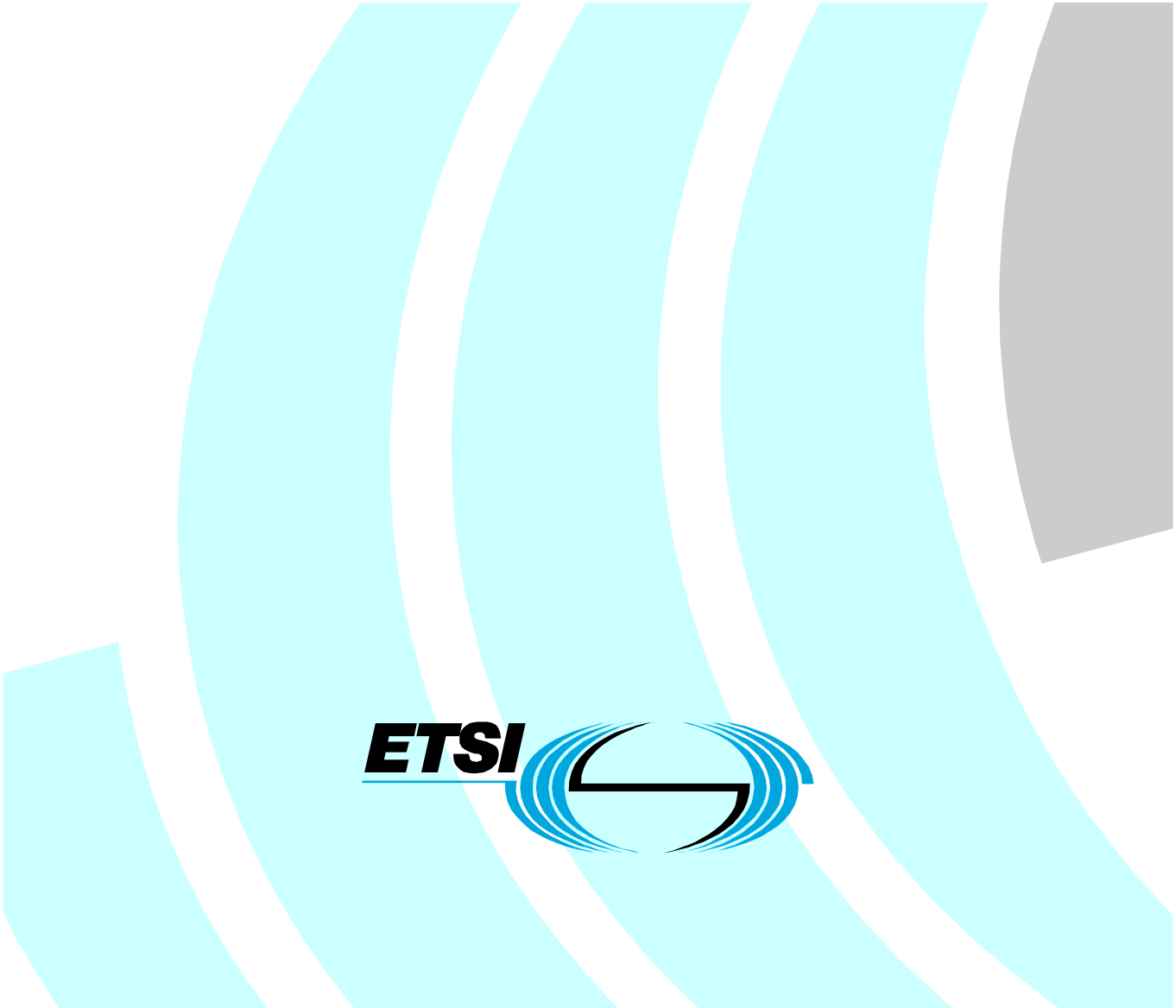
ETSI TR 101 944 V1.1.2 (2001-12)

Technical Report

Telecommunications security;
Lawful Interception (LI);
Issues on IP Interception



Reference
RTR/SEC-003018

Keywords
IP, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

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 ETSI 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://webapp.etsi.org/IPR/home.asp).

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 ETSI 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 Technical Committee Security (SEC).

1 Scope

The present document is intended to raise awareness and to stimulate discussion on the lawful interception of the Internet Protocol Stack (as defined in [4]). It identifies the problem technically. Whilst much of the focus of IP interception is with interception of the single network commonly referred to as "The Internet" and comprising the set of applications that make up the "World Wide Web", the document does not restrict its examination to the single network case but rather concentrates on an investigation of the viability of interception of Internet Protocols and the applications which make use of such protocols.

2 References

For the purposes of this Technical Report (TR) the following references apply:

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

[2] ETSI TS 123 107: "Universal Mobile Telecommunications System (UMTS); QoS Concept and Architecture (3GPP TS 23.107 version 3.5.0 Release 1999)".

[3] RFC 1180: "TCP/IP tutorial".

[4] RFC 791: "Internet Protocol".

[5] RFC 2822: "Internet Message Format".

3 Definitions and abbreviations

3.1 Definitions

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

terminal: some apparatus, of arbitrary complexity, which is connected by the user to the access mechanism

NOTE: The terminal, or elements of the terminal, are under the user's control.

access: mechanism, provided by a party other than the user, which connects the terminal to some point, which provides network connectivity

network connectivity: arrangement of equipment which offers connectivity between one terminal and another

NOTE: The PDU transported is an (IP) datagram.

service: set of functions offered to a user by an organization or a mechanism, which offers functionality to another network component

intercept product: data content which has been intercepted and is delivered to the LEMF

3.2 Abbreviations

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

ADSL	Asymmetric Digital Subscriber Line
BTS/BSC	Base Transceiver Station/Base Station Controller
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GW	GateWay
HI	Handover Interface

IETF	Internet Engineering Task Force
IIF	Internal Interception Function
IP	Internet Protocol
IPSEC	Internet Protocol SECure transmission
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
MSC	Mobile Switching Centre
NAT	Network Address Translation
NW	NetWork
NWO/AP/SvP	NetWork Operator/Access Provider/Service Provider
PABX	Private Automatic Branch eXchange
PDU	Packet Data Unit
PLMN	Public Land Mobile Network
PSTN	Public Switching Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
RSVP	ReSource reserVation Protocol
TCP	Transmission Control Protocol
TE	Terminal Equipment
UDP	User Datagram Protocol
xDSL	any Digital Subscriber Line technology

4 Education on LI for IP Data ("clarity of thinking")

4.1 Searching for clarity

Concepts of applying regulators' Lawful Interception requirements for IP-traffic are drawn extensively from experiences of the Lawful Interception of circuit-switched communications. However the IP-world is a highly structured mixture of communications-transportation and communications-services, with the services being mostly defined so as to be transparent to the communications carrier. Therefore a solution for the requirement for Lawful Interception of IP-traffic is very different from anything experienced to date in the circuit-switched environment.

Furthermore although the convergence of "Telecoms" and "IP-services" seems to promise solutions if not simplicity, the goal continues to be ambitious: Networks, network access points and nodes, services, service areas and regions as well as user-access facilities proliferate - implementing network-based solutions for Lawful Interception is difficult if not impossible in some cases simply because there are limits to what the NWO/AP/SvP can do and what information can be provided. For each of these roles it must be defined what is possible and sensible for its LI participation (Which id can be used? Which information is available? Etc.).

4.2 The core problem: identifying the correct IP packets to intercept

IP addresses are most of the time today assigned on a dynamic basis (e.g. per session), we speak of a "temporary IP address". This implies that IP addresses, when used for purposes of LI, can in general not be used to correctly identify a target and/or its traffic permanently. This restriction does not apply to permanent IP addresses which always correlate to the same user.

4.3 Is there a solution to Lawful Interception of IP-traffic?

Arguably there is. It lies in recognizing that technology convergence is neither a sufficient justification for a common approach to solving an inherently dichotomous problem, nor for extending telecommunications standardization into service domains.

Network access operators can only address regulatory requirements pertaining to the operations and services that they directly control. In places where a communications network only provides network-layered transportation to a service provider, thereby delivering services which are transparent to the access network, the network can only be responsible for intercepting communications at that network layer. LI on that layer does not make much sense, especially for transit nodes, if LI shall be based on application/service information. Access providers can only handle ID-specific LI and service providers LI based on services offered (like email for example). Especially service-based LI is considered to have a substantial impact on performance, it definitely must be backed up by national requirements.

Therefore, regulators should be convinced that Lawful Interception requirements must be addressed separately to Access Provider and Service Provider. It is arguable that the "complete IP-solution" would require considerable interaction and co-operation between these separate entities, but in general it is very likely that such co-operation would be highly contentious on security and privacy grounds, and very probably would be unacceptable to regulators in many countries especially where there existed no organic connection between the two. And where a single corporate entity controlled both Access and Service Provision, the co-operative effort to successfully combine LI efforts in both domains is an organizational issue: the technical dichotomy still applies. Additionally, as in circuit mode, LI across national borders is a juridical problem between the countries involved but no technical issue.

4.4 Are There parallels in support of interception dichotomy?

There is a certain precedent in the case of the use of encryption on a public communications channel, where most regulators implicitly recognize that the access provider is not responsible for removing encryption applied by the user, from LI-targets' (copied) traffic before it is delivered to monitoring centres - the communications channel is in effect regarded as a transparent channel, and the access provider is charged with regulatory responsibility only of those attributes over which it is directly in control.

The IETF recently published an opinion that the IP service-industry had no obligation to design, develop, or deploy IP protocols specifically to meet Lawful Interception requirements. IETF was effectively stating that IP traffic and network layer channels are mutually transparent: Authorities requiring communications interception should look to the communications network for solutions. The implied complement is that authorities requiring interception of tele-services should look to the service providers for solutions - again reaffirming the divide between network layer communications carrying and service provision.

4.5 What then is the role of ETSI TC SEC (WG LI) in regard to monitoring IP traffic?

ETSI exists to establish and publish communications standards - the "T" says no more and no less. ETSI therefore has no responsibility for the delivery of IP-interception standards that are beyond its ability to influence or produce. ETSI TC SEC should preserve the "transparency model" and currently does not explore solutions to Regulators' IP Interception problems beyond the network layer.

5 Basic data model

Network elements are considered along with the format in which content of communication might be retrieved from those elements.

A number of issues are raised by the analysis, which are listed.

NOTE: In accordance with [3] the term TCP/IP in the present document is used in such a high-level sense that it does not necessarily mean only the TCP protocol used over IP but a general variety of TCP or UDP or any other suitable protocol used over IP to transport data.

5.1 The Basic diagram

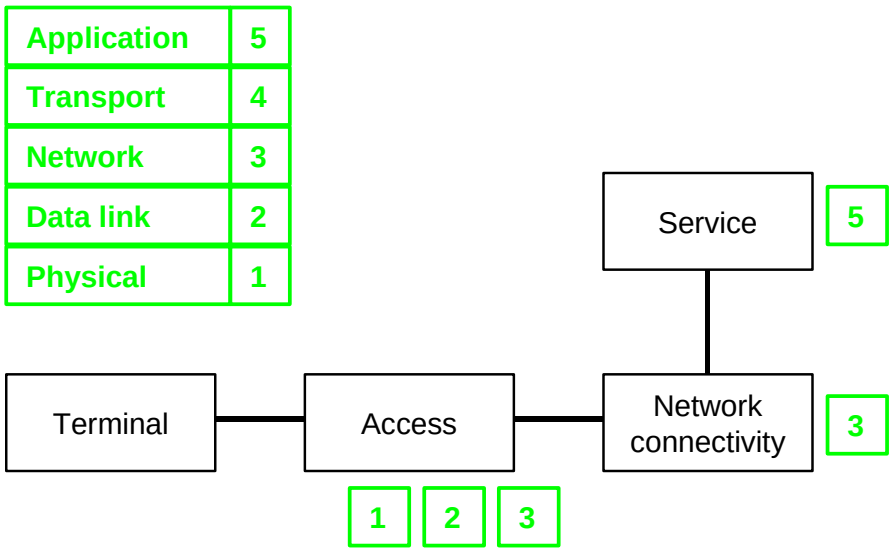


Figure 1: Basic data model for IP intercept

Consider figure 1. The component parts are defined as in table 1, with additions below. The layers column shows which layers in the IP 5 layer model the component is active at.

Table 1: Active components in the 5-Layer model

Component	Definition	Layers
The terminal	Some apparatus, of arbitrary complexity, which is connected by the user to the access mechanism. The terminal, or elements of the terminal, are under the user's control. (The terminal may itself be a network of arbitrary complexity. The terminal possesses one or more **network addressable points**, see figure 8.)	1, 2, 3, 5
The access	A mechanism, provided by a party other than the user, which connects the terminal to some point which provides network connectivity. The access mechanism does not have the functionality to offer connectivity between one terminal and another, other than through the network connectivity mechanism.	1, 2, 3
Network connectivity	An arrangement of equipment which offers connectivity between one terminal and another. The PDU transported is an (IP) datagram.	3
The service	A set of functions offered to a user by an organization or a mechanism which offers functionality to another network component.	5
NOTE: The term access is used in a different sense here as generally used in a PLMN in mobile systems, i.e. it does especially **not** refer to the mobile access system represented by a BTS/BSC or similar construct.		

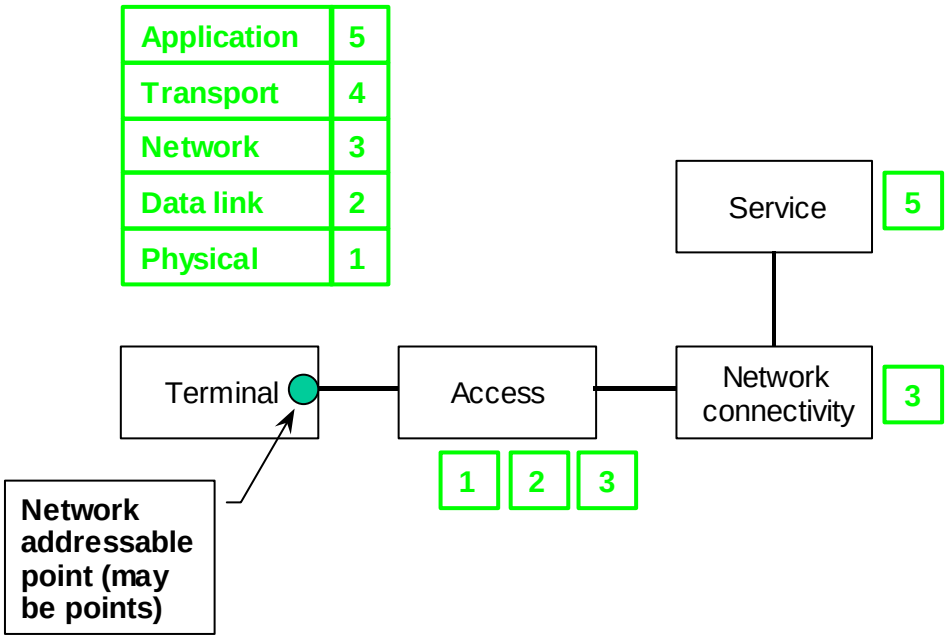


Figure 2: Further clarification of data model

5.2 Who owns which element

Table 2 describes the ownership of the network elements.

Table 2: Network element owners

Element	Owner	Comment
Terminal	User	Usually administered by the owner
Access	Access provider	
Network connectivity	Network connectivity provider	
Service	Service provider	

5.3 Who has what responsibility

In relation to a given terminal there is:

- an access provider, who directly connects to the terminal;
- a network connectivity provider, who offers network connectivity to the terminal;
- one or more service providers who provide services according to a terminal address or a service address.

Each of these players may, in principle, be asked to provide LI facilities. In many circumstances there will be more than one player who could provide LI and there is not yet a clearly understood way of deciding who should be allocated the responsibility. This requires further investigation.

5.4 Network addressable points

It would seem that each network addressable point could be a target for LI. That raises issues as to who allocates these, and what happens if the terminal chooses to use mechanisms such as NAT or RSVP.

5.5 Format of interception

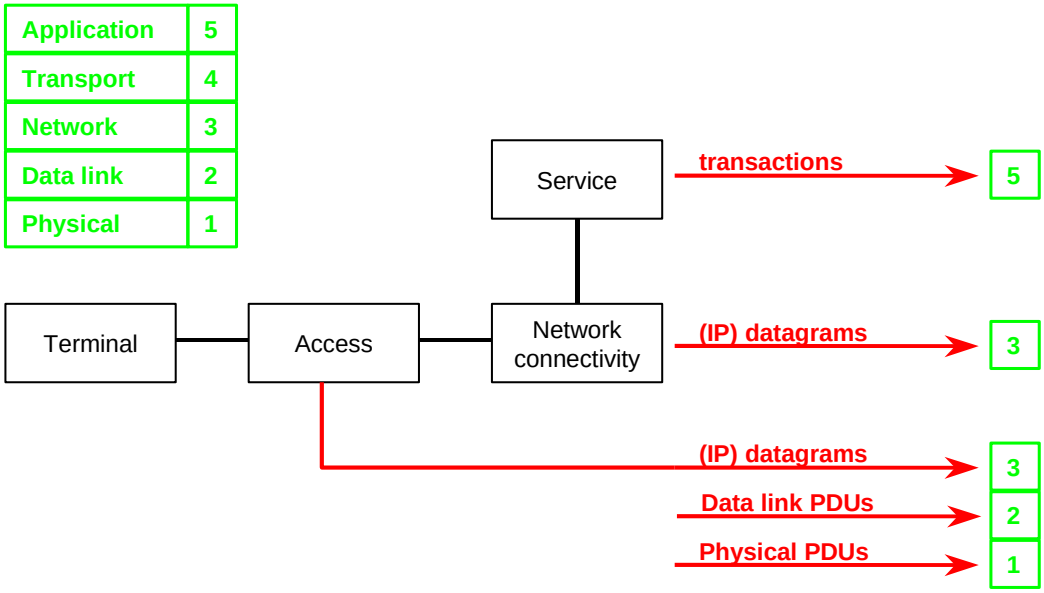


Figure 3: Data model for interception format

Figure 3 shows the layers of the 5 layer model which are available to an interception entity (presumably an IIF).

The access may offer information at the physical, data link or network layers, depending on the technology employed and the configuration. In any particular case then the technology chosen would be that which is most comfortable taking in to account such issues as cost, security and availability in the market place.

The network connectivity only has information available at the network layer, typically IP datagrams.

The service only has data available at the application layer. By way of example, if the service were providing email then the information would be available in formats specified in internet message format standards [5].

5.6 Considerations

It is of the utmost importance to address LI requirements and standards differently to two levels, namely the **network level** on one hand and the **service level** on the other hand. This difference stems from the different tasks offered and the different technologies used. At network level, interception of (IP) datagrams shall be the only appropriate requirement, while other considerations and requirements like interception of certain services, in particular email and similar services such as instant messaging or others still to come, must clearly and absolutely be directed to the service level.

As a consequence, the meaning of HI2 and HI3 interfaces as they are seen and described in [1] needs clearly to be redefined for IP interception on the network level. While the meaning and purpose of HI2 seems to be quite clear for intercepting services ("an email for xyz has just arrived"), this is not quite so easy on the network level. The purposeful use of HI2 messages on the IP network level is not clear. Obviously, giving information in the sense of "party A just sent a datagram to party B" is pretty much useless and would also lead to an uncontrollable flood of HI2 tickets on the interface with practically no information gain. Further investigation is necessary to resolve the problem of what information should be passed in HI2.

6 Implementation architecture for LI of internet communication

6.1 General

The Internet introduces a number of new services related to telecommunications, which are provided over a variety of access technologies, such as for example:

- Telephone connection (PSTN/ISDN);
- Digital Subscriber Line (xDSL);
- Local Area Network (LAN).

These introduce a set of new issues for lawful interception: where to intercept, by whom and when? Traditionally the interception is done at some point in the network, predominantly at a local exchange or in a mobile switch controller. This is based on the assumption that the network operator is also the service provider and thus has access to subscriber identities (phone numbers). In the case of Internet, the service providers have little or no direct relationship with the network operations that are used to convey the services. This also means that the network operators will not have access to the identities that may be targeted for interception: e-mail addresses, web site URLs. Trying to wash out such identities from a stream of high-speed data would be technically challenging, expensive and costly in performance, making the fact that LI is ongoing with that stream difficult to hide. Therefore, this group (TC SEC WG LI) sees no lawful requirements for such action.

The straightforward way of performing an intercept of this kind of traffic is to go for the internet service provision. That would mean that the order to intercept is issued to the ISP and based on the customer-id of the subject with that ISP. When the subject logs into the ISP, interception would be initiated and all traffic copied to the LEA(s) that have requested interception. The kind of software that is needed in the ISP server would be attached to the logon process there and trigger on the customer-id of the subject. When triggering occurs, a separate connection to the LEMF would be set up and all subsequent traffic for the session copied onto that connection.

In the following a more detailed description of some typical implementations will be given. In cases where several interception possibilities are available it is up to mutual agreement between the LEA and the NWO/AP/SvP to select the appropriate location for the interception point.

6.2 Dial up connections

In this case, both the modem telephone connection and the ISP server can be intercepted for the subject. For GSM mobile networks the local exchange would correspond to an MSC.

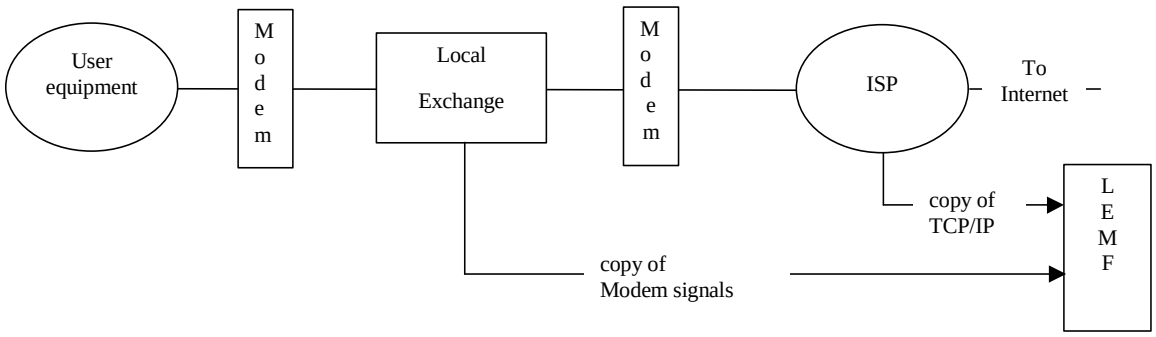


Figure 4: Interception for dial up connection

6.3 Permanent connection models

This covers for example types of connections such as ADSL, LAN or cable modems, etc.

6.3.1 Connection via a dedicated line

This covers scenarios such as ADSL or cable modem access. Here the traffic will bypass the switching equipment and be transmitted directly to the ISP on an IP connection.

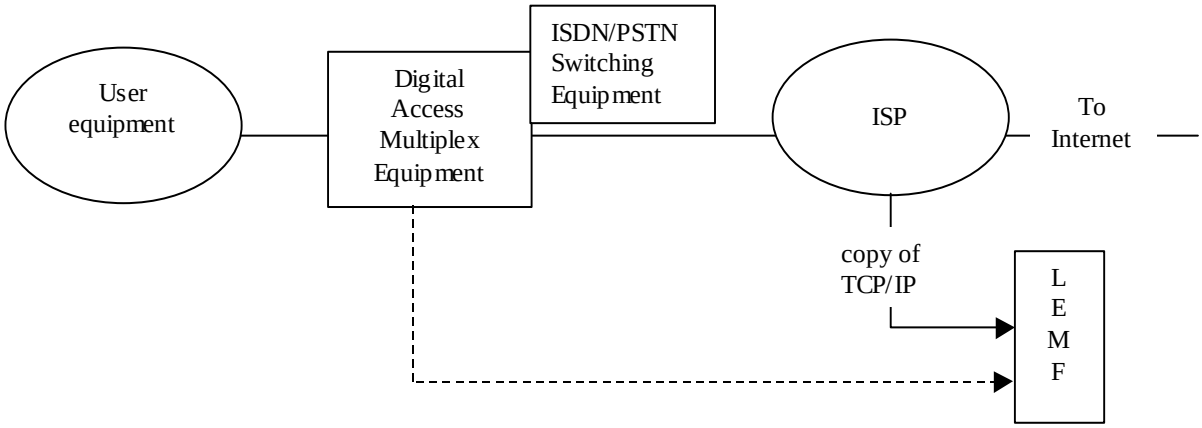


Figure 5: Interception via a dedicated line

Functionally, GPRS internet access (e.g. using RADIUS) would connect the user to the ISP similarly to this configuration. See also ES 201 671 [1].

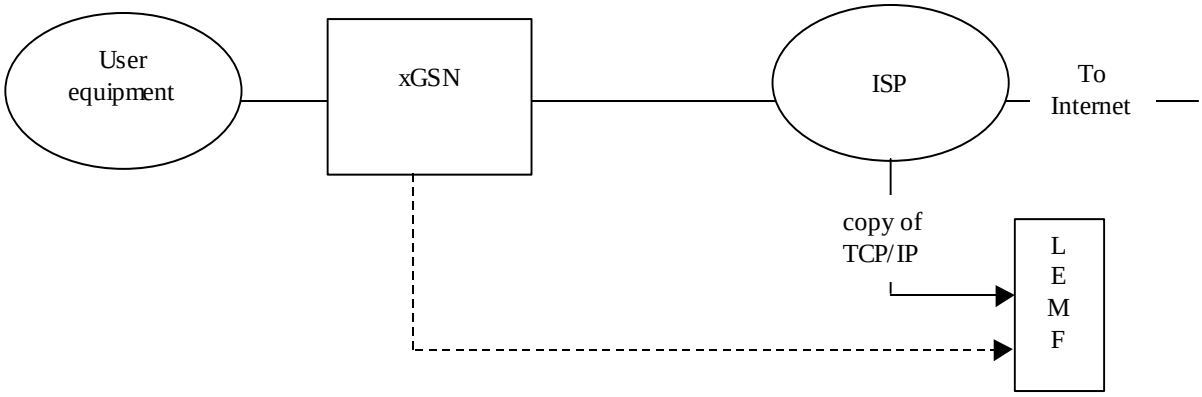


Figure 6: Interception of GPRS user internet connection

6.3.2 Connection via Local Area Network

Connections to Internet via a LAN will in almost all cases be done in a workplace environment, similar to making phone calls via a PABX. The interception of this would have to be arranged for through cooperation with the workplace organization.

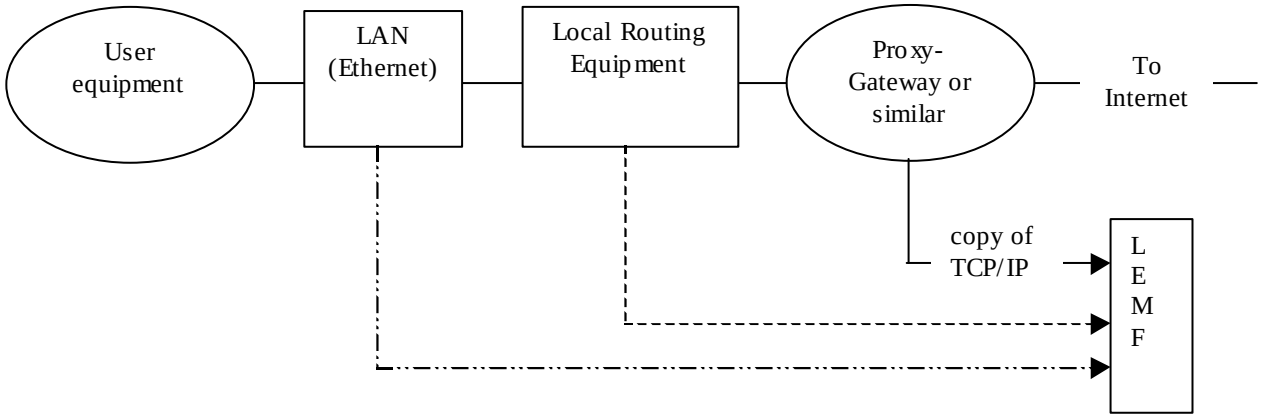


Figure 7: Interception for LAN connection

6.3.3 Permanent IP addresses

Here the user equipment will be permanently defined with its own IP address on the network - a point of presence in its own right rather than with a session-specific temporarily assigned IP address for the session. This can be compared to the situation with for instance PABX interconnect over a virtual private network with semi-permanent connections. Interception can be made in the routing equipment based on the IP address of the subject and using for instance firewall technologies.

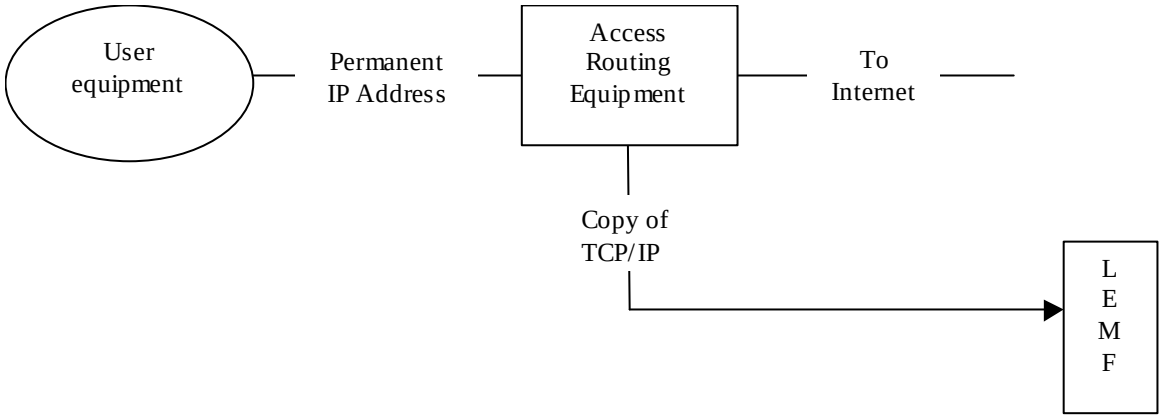


Figure 8: Interception with permanent IP address

6.4 General notes about delivery considerations

There has been much confusion about communication content delivery and this should hopefully bring some clarification. In general, we have to differ between mechanisms which are used to help *to put the information back together* (LI header, see clause 8.3.3) which has been split up for the transport purpose and mechanisms which are used *to transport* the split up information. See also the notes in clause 8.3.

So, when speaking about these things, we actually have to consider two functional blocks:

- information headers. From the point of view of the transport layers these are just part of the information to be transported to the receiver;
- transport mechanisms (or parts thereof) and protocols.

Figures 9 and 10 try to illustrate the interaction for IP HI information, albeit they neglect the transport elements rather generously. But this can be used in a fine way to demonstrate that headers can be seen completely detached from transport protocols. It does not matter at all how the information is transported between the different entities below.

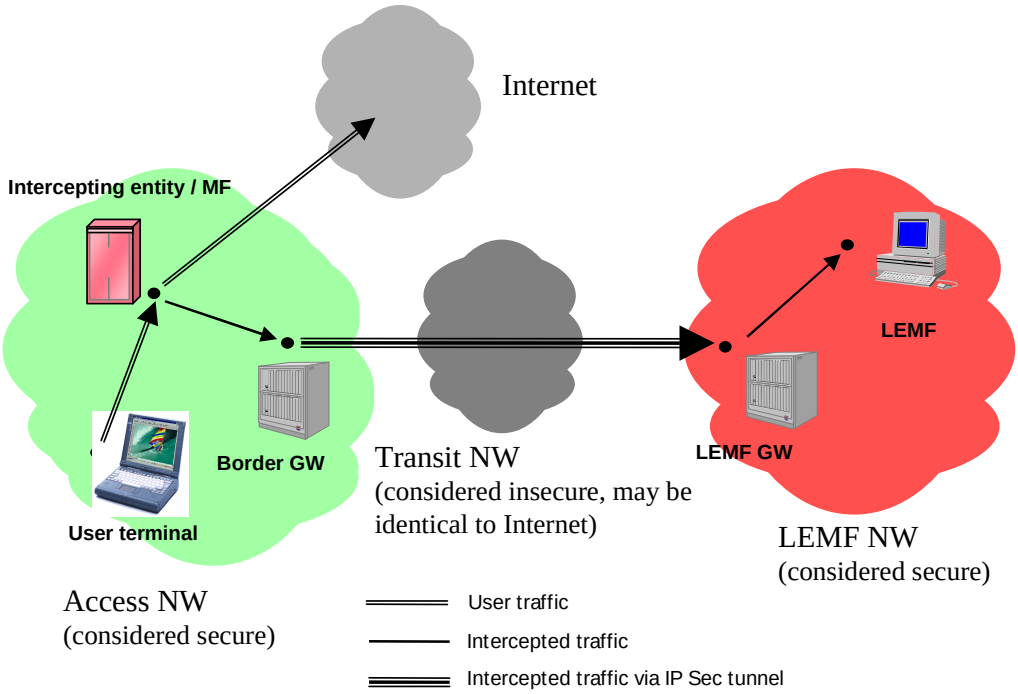


Figure 9: Network scenario example for IP data delivery using IPSEC

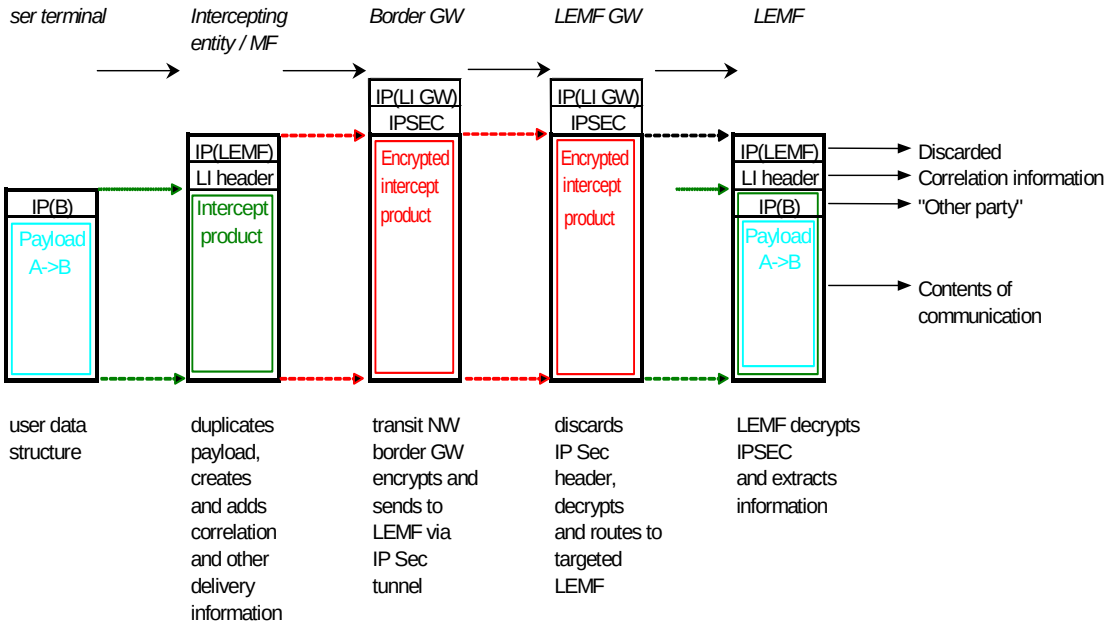


Figure 10: IP data delivery using IPSEC

6.5 3rd Generation mobile technologies

3rd generation systems introduce several new concepts that are significant for Lawful Interception, one of them being Quality of Service (QoS). This aspect needs to be discussed in addition to other data transport aspects. See [2] for further details on QoS.

Network services are considered end-to-end, this means from a Terminal Equipment (TE) to another TE. An end-to-end service may have a certain QoS which is provided for the user of a network service. As it is possible for the two parties of a 3G communication to negotiate a certain QoS for a session (which in the broadest sense can be considered as reserving certain resources and capacities), it is necessary for the interception delivery process to establish an equal or higher QoS with the LEMF in order to guarantee transport of the session content. If the required QoS (i.e. the same one as negotiated between the original parties) cannot be guaranteed by the LEMF, then the session content will not be delivered to the intercepting party. This applies on a session-by-session basis.

7 Security aspects

7.1 Handover

The end-points of the interception link should be capable of being authenticated to each other. This may be achieved using public-key provisions or by symmetric key provisions. The provisions on this link are the primary responsibility of the LEA but have to meet with the acceptance of the service provider.

Data protection responsibilities of a certain layer related to the target are the primary responsibility of the operator of the services responsible for this layer.

7.2 Target information

Any information relating to the target that can be correlated to the warrant should not be available to unauthorized access. This implies a need to provide access control within the service domain on all data relating to targets and potential targets. In case of 3rd party interception the data released should be a minimum required to identify the target.

8 Notes about HI3 for packet oriented content

8.1 Introduction

In the TC SEC WG LI so far four delivery mechanisms have been discussed in or outside the meetings. The logical goal of the WG LI seems to be only one mechanism.

Lining up the mechanisms discussed so far and adding relevant comments could narrow down the number of possibly usable mechanisms. For practical examples of the discussed mechanisms refer to the documents listed in clauses "References" and "Bibliography."

8.2 General requirements for the packet HI3 delivery

Packet data HI3 delivery must be:

- Independent
  The delivery mechanism should be independent of the content or its origin like, for example, independent of the actual packet network, service and/or application.

- Open
  The mechanism must be as open as possible. Preferably the interface may not have aspects that are not fully described in other standards documents (e.g. RFC's).

- Reliable
  Accuracy must be such that it could be used for evidential proof. Omissions must be avoided within feasible limits. If omissions should occur they must be detectable.

- Low cost
  The use of widely available protocols and software is preferred (see also the bullet for "Open").

- Secure
  The confidentiality, integrity, authentication and accountability (CIAA) should be guaranteed. For evidential proof the integrity and authentication must be guaranteed. It must be detected if any attempts are made to change or remove parts of HI3 information. Eavesdropping must not be feasible (in relation to a threat analysis of a specific national implementation).

- As fast as possible
  The mechanism should be effective concerning the transmission delay, overhead, and the processing power required.

8.3 Discussed mechanisms

8.3.1 Observations

There are two types of mechanisms being discussed, data structures and delivery mechanisms, which will both be discussed in the next clauses.

Figure 11 tries to illustrate how the application layer in an LI application could make possible use of different transport mechanisms (TM1, TM2), which of course may be in a certain dependency of each other.

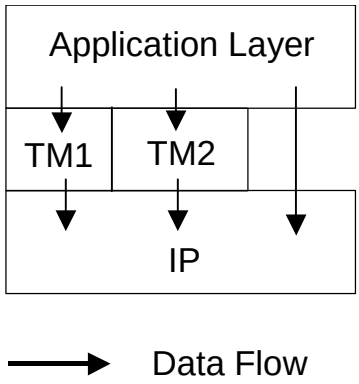


Figure 11: Layer interconnection

8.3.2 Data structures for CC

Data structures describe headers (and possibly trailers) which are added to the payload packets on application or lower levels. They contain additional information describing labels and identifiers needed for LI like correlation information, evidential proof, etc. but also for technical issues like checksum, length of payload, segmentation or fragmentation techniques. Also security mechanisms are an issue to be addressed here, like e.g. encrypting and/or signing the payload. It must be ensured that the information arrives in correct sequence (or can be re-sorted to it upon arrival at the LEMF) and that it arrives completely (no packets are lost).

On designing data structures it is important to keep in mind that they must be flexible but easy and fast to handle, so that passing on the intercepted traffic is only delayed as short as possible. For these reasons only headers should be used, adding trailing data is discouraged for efficiency and ease of handling reasons.

8.3.3 Delivery mechanisms for CC

On designing a new or selecting an already existing delivery mechanism, the following issues should be considered:

- There is the possibility that the LI application calls TCP/IP functionality directly without any additional delivery mechanisms. Can such a solution be used or is there a valid reason for introducing a delivery mechanism at all?

- When should the data be transferred to the LEA? It can be based on the amount of data (send when a certain threshold value is met), event driven (every packet immediately) or based on a timeout specification (e.g. every 20 seconds).

- A delivery structure has to be established (naming conventions for files, etc.). This structure should provide the information necessary for the LEMF to be able to properly recognize the data being delivered.
- If not already provided by the data structure concept, correlation information must be included to ensure sequence and complete transmission of single information elements.
- Security issues must also be addressed here. The delivery mechanism must provide authentication for the communication partners on setting up the connection. It must provide encryption for the payload if not already provided by higher layers.
- Appropriate error and backup mechanics need to be thought of and agreed among all participating parties (communication timeout, retransmission of data not or not properly acknowledged, buffer overflow, alive messages, etc.).

Annex A: Bibliography

- ETSI TR 101 331: "Telecommunications Security Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".
- RFC 959: "File Transfer Protocol".
- RFC 1958: "Architectural Principles of the Internet".
- RFC 2228: "FTP Security Extensions".
- RFC 2401: "Security Architecture for the Internet Protocol".
- ITU-T Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".
- ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".
- ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".
- ETSI TS 133 106: "Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful Interception Requirements (3GPP TS 33.106 version 4.0.0 Release 4)".
- ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful Interception Architecture and Functions (3GPP TS 33.107 version 4.0.0 Release 4)".
- ETSI TS 101 509: "Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage 2 (3GPP TS 03.33 version 8.1.0 Release 1999)".

History

Document history		
V1.1.1	May 2001	Publication
V1.1.2	December 2001	Publication