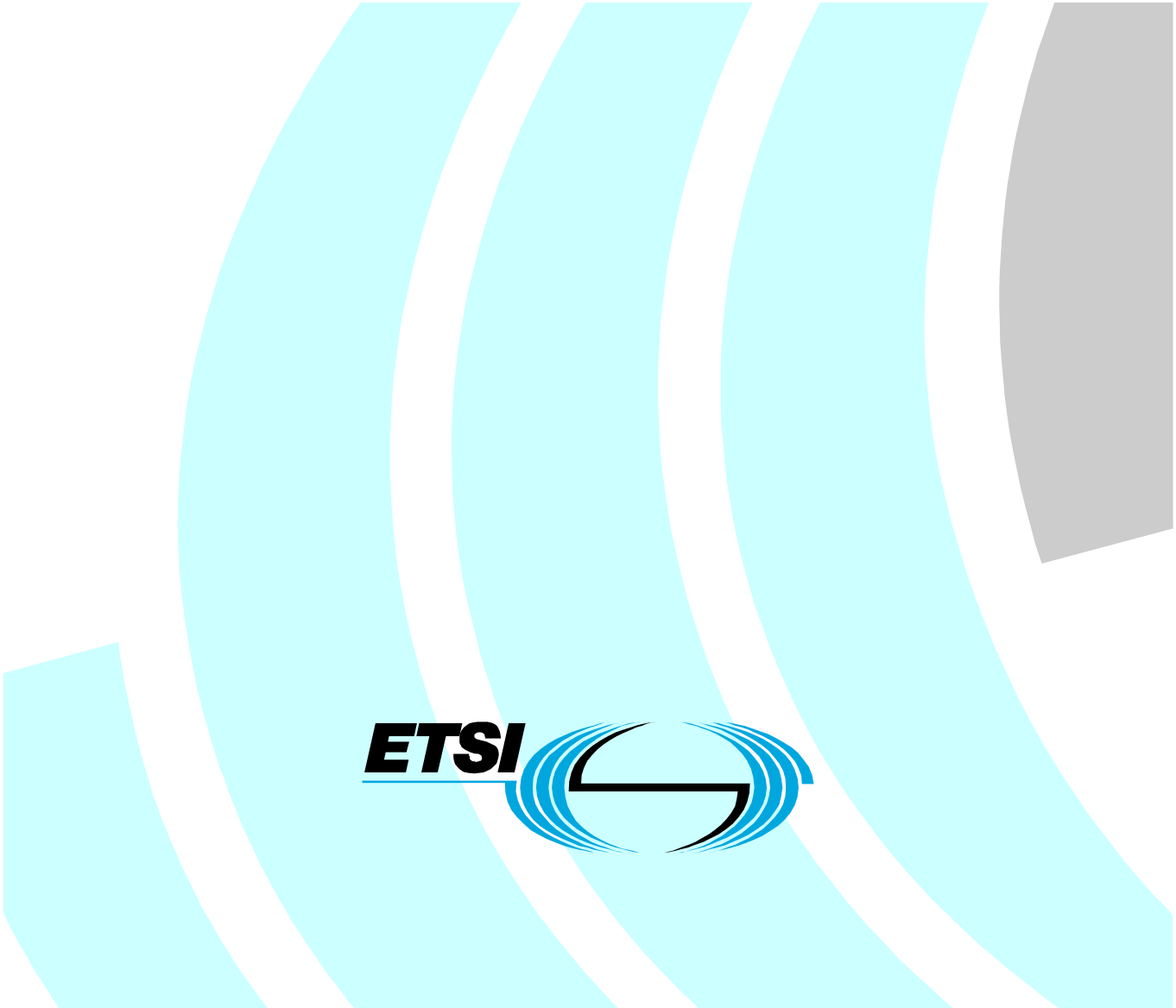
ETSI TR 102 519 V1.1.1 (2006-05)

Technical Report

Lawful Interception (LI);
Lawful Interception of public Wireless LAN Internet Access



Reference
DTR/LI-00014

Keywords
access, internet, IP, lawful interception, security, service

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2006.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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 Lawful Interception (LI).

Introduction

The present document focuses on intercepting IP data in relation to the use of Wireless LAN based Internet Access Services and is to be used in conjunction with the TS 102 234 [1]. In the latter document the interception of various types of Internet Access data is described.

1 Scope

The present document provides an overview of the issues and challenges regarding the Lawful Interception of Public Internet Access by means of Wireless LAN technology as defined in the IEEE 802.11 [2] specification and possible approaches for dealing with these issues, considering different architectures and business models.

The present document is applicable to public Internet access. The private use of Wireless LAN technology is excluded.

2 References

For the purposes of this Technical Report, the following references apply:

[1] ETSI TS 102 234: "Lawful Interception (LI); Service-specific details for internet access services".

[2] IEEE 802.11: "ISO/IEC 8802-11) IEEE Standards for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[3] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[4] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[5] IEEE 802.16: "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems".

[6] Directive 2002/21/EC of the European Parliament and of the Councilof 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[7] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[8] ETSI TS 123 234: "Universal Mobile Telecommunications System (UMTS); 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (3GPP TS 23.234)".

[9] ETSI TS 129 234: "Universal Mobile Telecommunications System (UMTS); 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3 (3GPP TS 29.234)".

[10] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[11] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 234 [1] and the following apply:

access point: technical equipment that offers IEEE 802.11 connectivity to a mobile terminal

federated network: network, possibly spanning one or more countries or territories, in which different networks share connectivity, such that customers of one network may use the resources of another network, or acts as a gateway to other networks, such that connectivity to several networks is provided via a single gateway

hotspot: nominated area where a user can expect to receive Wireless LAN access

3.2 Abbreviations

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

AAA	Authentication, Authorization and Accounting
ADSL	Asynchronous Digital Subscriber Line
AF	Administration Function
AM	Application Manager
AP	Access Point
CC IIF	Content of Communication Internal Interception Function
CC	Content of Communication
CID	Communication IDentifier
CMTS	Cable Modem Termination System
COPS	Common Open Policy Service
ESSID	Extended Service Set IDentifier
GPRS	General Packet Radio Service
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
IAP	Internet Access Provider
IIF	Internal Interception Function
INI	Internal Network Interface
INI1	Internal Network Interface 1 (for Administrative Information)
INI2	Internal Network Interface 2 (for Intercept Related Information)
INI3	Internal Network Interface 3 (for Content of Communication)
IP	Internet Protocol
IRI IIF	Intercept Related Information Internal Interception Function
IRI	Intercept Related Information
ISM	Industrial, Scientific and Medical
ISP	Internet Service Provider
LAN	Local Area Network
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
NAT	Network Address Translation
NWO	Network Operator
PS	Policy Server
SNMP	Simple Network Management Protocol
SvP	Service Provider
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UE	User Equipment
WAP	Wireless Access Point
Wi-Fi	Wireless Fidelity Alliance
WISP	Wireless Internet Service Provider

4 Public Internet access over Wireless LANs

4.1 Technology

4.1.1 IEEE 802.11

Wi-Fi is a registered trademark of the Wi-Fi Alliance (see note 1), and is used to indicate equipment which conforms to an interworking profile for IEEE 802.11a, -b or -g [2]. These standards are available from the IEEE web site (see note 2), though the interested or simply curious reader will need to download their individual copy due to licensing conditions. The profile is the bedrock for the widespread adoption of the radio technology, which is typically being used for home (computer) networks, business computer networks and public access to the Internet. The term "wireless LAN" is used to indicate the Wi-Fi interworking profile throughout the present document.

NOTE 1: http://www.wi-fi.org/.

NOTE 2: http://standards.ieee.org/getieee802/.

This paper is concerned principally with the application of wireless LAN to public access to the Internet, and the issues of lawful interception (LI) which such connection raises. In spite of various criticisms of the various IEEE 802.11 standards, principally in relation to area spectral efficiency and security, IEEE 802.11b and IEEE 802.11g equipment is being fitted to a great deal of new personal computing equipment. Intel's Centrino initiative packages IEEE 802.11a, -b or -g (see note 3) functionality together with a low power consumption mobile processor. This allows attractive portable computing equipment to be manufactured at an affordable price. Naturally, there are many other players in the market-place.

NOTE 3: http://www.intel.com/products/mobiletechnology/.

For the user, IEEE 802.11 technology brings freedom to connect to the Internet with no wires, and frequently with no need for prior arrangement. There is a downside for the user in the sense that frequently IEEE 802.11 access has to be paid for. The business model for offering IEEE 802.11 access is still being developed. One could say that it is a lot easier to manufacture IEEE 802.11 equipment than it is to make money offering Internet access using IEEE 802.11 [2], and a number of business models are being tried.

No-one yet knows which business models will work in the long term, if any at all.

4.1.2 WiMax

WiMax is another interworking profile, but aimed principally at fixed access networks, based on IEEE 802.16 [5] and ETSI HIPERMAN. WiMax will allow for mobile access, but this is unlikely to be an issue until the turn of the decade. It is thus mentioned only to note that it has been explicitly ignored from the present document.

4.1.3 Hotspots and Access Points

The reader will find frequent reference to the terms "hotspots" and "access points". A hotspot is a nominated area where a user can expect to receive Wireless LAN access. A hotspot might be a few metres across if it is serving a small room or perhaps 100 metres across if serving a large open space.

One hotspot will be served by one or more Access Points (AP), typically using a single Extended Service Set Identifier (ESSID). An access point is the technical equipment which offers IEEE 802.11 connectivity to a mobile terminal.

How a user terminal roams between hotspots is an open question, to which there is no standard answer. Possibilities include the use of Mobile IP.

NOTE: See, for instance http://www.computer.org/internet/v2n1/perkins.htm.

4.2 Business models

We start by considering business models, since the impact of these drives the technical infrastructure, and infrastructure arrangements which do not support a viable business model will not survive for very long.

4.2.1 Free access

An access point owner, the service provider, provides free access to the Internet, typically as part of another service. So a hotel might offer wireless LAN coverage to encourage its guests to return, or a coffee bar might offer wireless LAN coverage to encourage its customers to stay longer and eat and drink more, and generally improve its popularity.

In these cases the cost of billing, and dealing with dissatisfied customers, and the potential for customers to be dissatisfied in the first place, is a very strong incentive for offering free service. Thus free wireless LAN service equates to satisfy customers, who will, one way and another, then pay more for a business's principal services.

This model might apply to a single location, or to a number of locations. Note that the free service might be provided by the business owner's own assets, or by assets supplied by another party.

An example from the UK is the provision of wireless LAN access using access points attached to ADSL lines already provided for downloading games to games machines situated in pubs or other entertainment venues.

EXAMPLE: http://www.theregister.co.uk/2003/05/22/hey_you_get_onna/.

4.2.2 Paid access to single operator network

A service provider business establishes their own set of access points (locations), which their customers may use, for a fee of some sort. Some customers will be subscribers, some customers will be pay-as-you-go typically paying over the air for a few hours service using a credit card. The fee for using pay-as-you-go service might be a few Euros an hour. The charging method for subscribers might allow so many hours access or so much data transfer per time period.

Typically, the tariff is set by comparison to the cost of GPRS air-time and what the market will bear. The target customer, today, is a business person or a bright young thing with disposable income. Over time, the tariffs may be expected to reduce with competition.

Generally the equipment is provided and operated by the service provider. However, the service provider can not offer their branded access anywhere where they own no infrastructure, which is unattractive to, for instance, international travellers.

This monopoly model is being superseded by the following, federated, model.

4.2.3 Paid access to federated network

A customer, as above, may be a subscriber or a pay-as-you-go user. The service provider, who may or may not own their own network, contracts with other networks to provide wireless LAN access to the service provider's customers. This allows the service provider to retain their contact, and branding, with their own customer base, but to offer that customer service over a wide set of locations, with no need for capital investment on the part of the service provider.

The area over which their customer base can receive service, and the profitability of the business, depend on the commercial negotiating skills of the service provider.

Typically, when a service provider's customer receives service at a location, that customer will be offered a choice of service providers and must select the one which they wish to use.

This is a rich model, and can be expected to evolve with time.

4.2.4 Federation details

A service provider A may negotiate with service provider B a contract for that service provider to extend the area over which A's customers may receive service. The technical infrastructure which offers service may be provided directly by B, or by third party service providers with whom B has, in turn, a contractual relationship. A third party access provider could be a small domestic user or shopkeeper, for instance, who offers IEEE 802.11 access through a package. Equally, a third party access provider could be a multi-national business (who in their turn may federate, of course).

It is very noticeable that there are players, IEEE 802.11 service franchisers, whose business model is to offer other businesses, who already have locations, the opportunity to install IEEE 802.11 access points as a managed service. So a hotel, for instance, would install one or more access points but the technical details, customer support etc. would be dealt with by the service franchiser. Either party might have the customer relationship and the franchisee is paid commission by the franchiser according to revenue.

4.2.5 International issues

The networks described have no fundamental regulatory limits as far as international frontiers are concerned. This is a consequence of telecommunications market liberalization. In the EU, market regulation should be in accordance with Directive 2002/21/EC [6] which makes clear that regulation is appropriate only when a player has significant market power, and for purposes of constraining that market power. Thus if an operator with a central location in Luxembourg proposes to serve access points in Germany, France, the UK and The Netherlands there are no prescriptive reasons why this arrangement should not be set in place. Should the hypothetical operator then wish to federate with networks in the USA and Australia there are few real barriers, always supposing that financial backing exists.

4.2.6 Service areas

Typically, an access point will serve a large public area, such as a railway station concourse or a hotel lobby. Sometimes a number of physical access points will be connected and operated in such a way as to appear as, logically, a single access point.

A hotel might have an AP in the lobby, but also wish to offer serviced in-room to its clientele. Usually, this will require extra access points whose cost would be paid for from the increase in revenue which extra coverage brings.

4.2.7 Coverage

Today, very few IEEE 802.11 networks offer broad coverage. Rather, the coverage is centred on a number of popular locations with gaps in between.

4.3 Service architectures

4.3.1 Basic structure

Figure 1 identifies the elements involved in arranging an IEEE 802.11 Internet access service, and their interconnection. A **mobile terminal** uses a **radio link** to communicate with an **access point**, using IEEE 802.11 protocols and the Wi-Fi interworking profile. The access point links to Authentication, Authorization and Accounting **(AAA) functions**, which may be local or remote. The access point also offers **Internet connectivity**, which again may be local or remote.

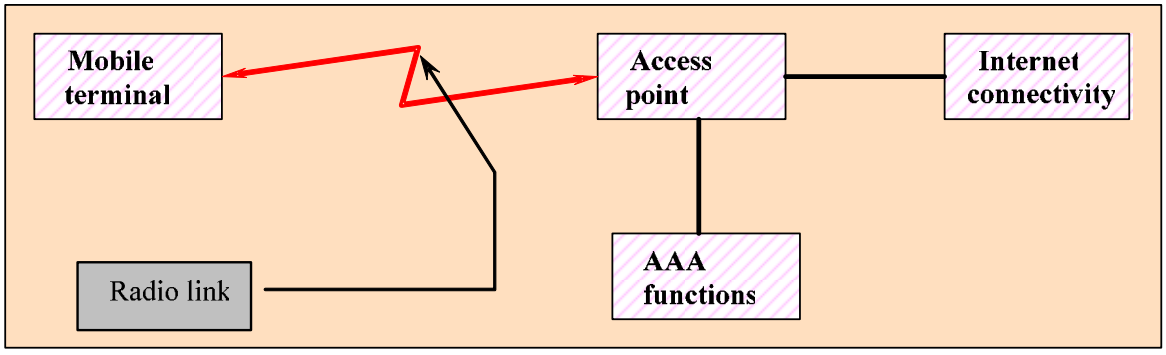


Figure 1: The elements of an IEEE 802.11 Internet access arrangement

4.3.2 Central access control and backhaul to the Internet

Figure 2 shows the typical arrangement of a centrally controlled access service. A **backhaul network** connects a number of geographically dispersed access points to a central location. At that location the AAA functions and Internet connectivity are provided. So that control may be provided over subscriber access, the arrangements do not allow direct access to the Internet from an access point. Instead, traffic is sent through the backhaul via the backhaul network. Such a network typically uses L2TP tunnels established through the (public) Internet, one tunnel set up per active user.

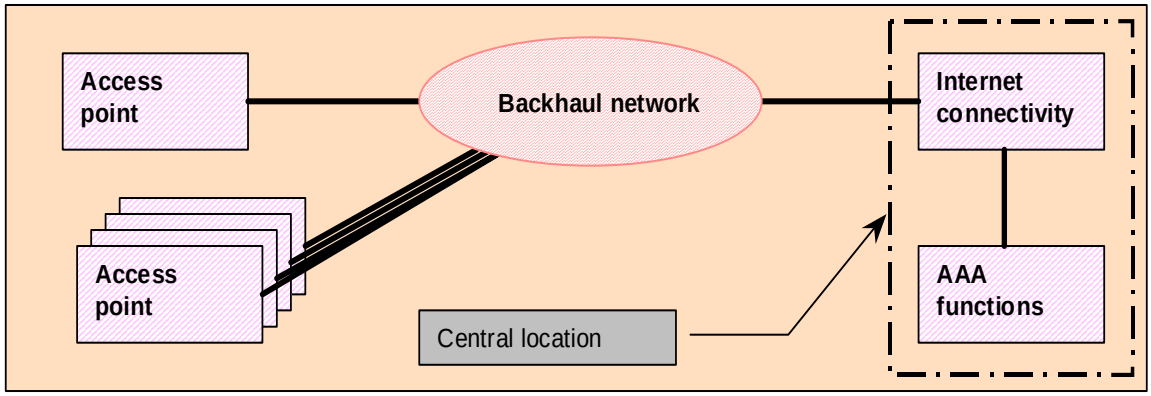


Figure 2: The elements of a centrally controlled IEEE 802.11 access service

The observant reader will realize that Lawful Interception (LI) is, in principle, easy to achieve at the central location where account information, activity information and the associated traffic are all readily available.

This arrangement may support the free access and paid access business models. If paid access is offered from federated networks, then the arrangement described above could be used with some extra complication relating to AAA, but with all traffic being backhauled to the central location.

4.3.3 Central access control and federated access to the Internet

Figure 3 shows centralized access control and federated access to the Internet. The essence of the arrangement is that access control is managed centrally, but Internet connectivity is provided by the federated network.

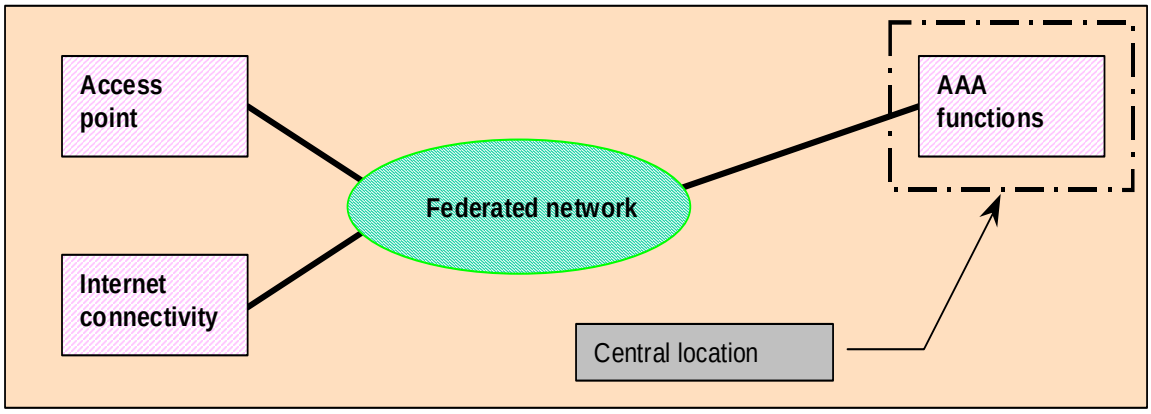


Figure 3: The elements of federated access to the Internet

The observant reader will realize that LI has become more problematic. Identity information is held at the central location, but traffic between a mobile terminal and the Internet is dealt with by the federated network. Such traffic is never seen at the central location. Traffic may be seen by the federated network, though.

The feature of this arrangement as compared with figure 2 is that there is no backhaul to the central location. This would generally be cheaper than using such backhaul. A service provider is always under economic pressure to reduce the costs of operation.

4.3.4 Central access control and local access to the Internet

Figure 4 shows an arrangement in which access control is the only function reserved to the central location. Access to the Internet is provided by each access point, individually.

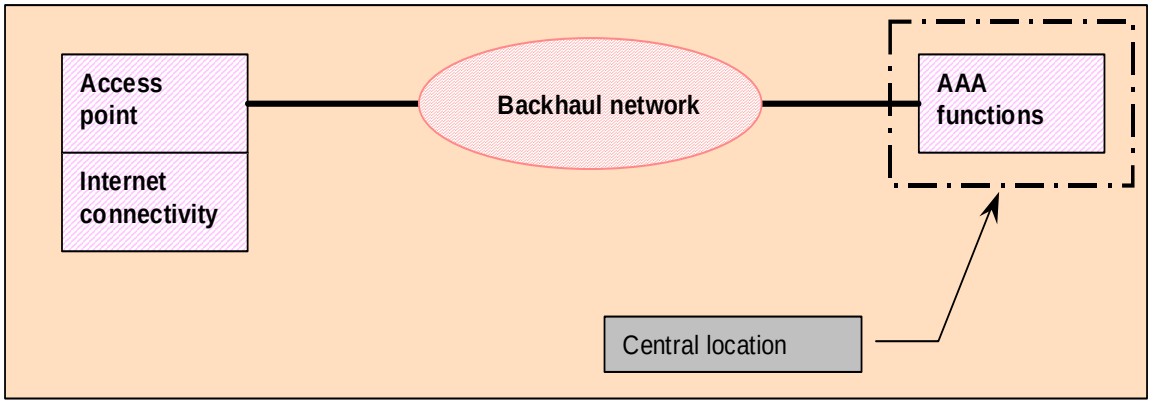


Figure 4: Elements of local access to the Internet

The observant reader will realize that LI has become very difficult. Although the central location still knows that an account is active, Internet connectivity is associated with each access point.

The driver for the adoption of this access model is simplicity, and reduction in cost.

4.3.5 Distributed access

Figure 5 shows an arrangement in which the functions of the central location are limited to account administration. Access control is devolved to the access point.

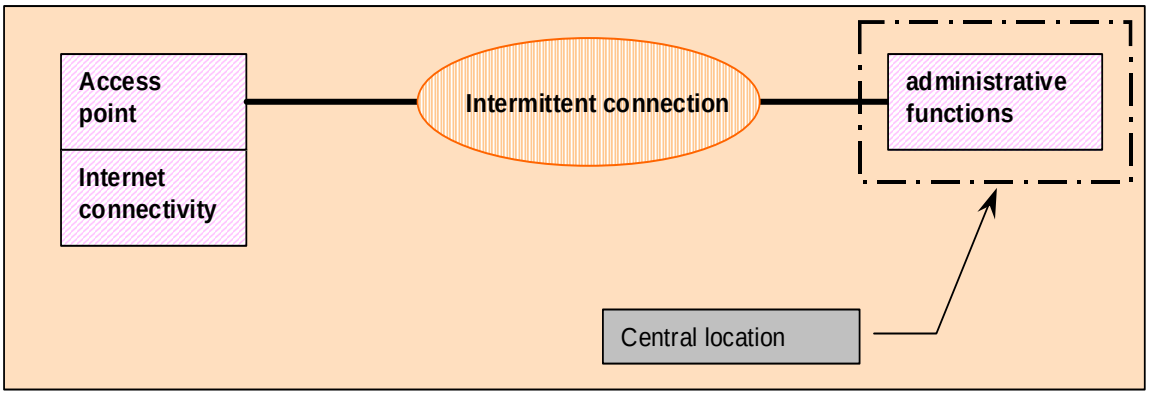


Figure 5: Elements of distributed access control

The observant reader will observe that LI has become very difficult. The central function has no knowledge of when an account is active. Such arrangements could support a pre-pay service, or an account-based service using cryptographic tickets.

NOTE: Perhaps using Kerberos or similar technology. (See http://web.mit.edu/kerberos/www/, for example.)

4.4 Technical issues

There are a number of technical issues which arise from the use of IEEE 802.11 [2] technology.

4.4.1 Link sharing

The IEEE 802.11 protocols are designed to permit the sharing of the radio link's capacity between several mobile terminals. Thus one access point can simultaneously support a number of mobile terminals. The number of mobile terminals which can satisfactorily share an access point depends on the services which those mobile terminals are accessing.

4.4.2 Distance issues

The **access range** between a mobile terminal and an access point will be somewhere between 100 m, if there are few obstructions, and 30 m or less in an urban environment. Within a building the range may be 10 m, or less, if there are walls between the mobile terminal and the access point.

As the distance between a mobile terminal and its current access point increases, so, typically, the **data rate** supported by the radio link will drop. The sequence of link speeds defined for IEEE 802.11b is 11 Mbit/s, 5,5 Mbit/s, 2 Mbit/s, 1 Mbit/s, 0,5 Mbit/s.

4.4.3 Interference

IEEE 802.11b [2] and IEEE 802.11g [2] both use unprotected and unlicensed (see note 1), but regulated (see note 2), spectrum in the 2,4 GHz Industrial, Scientific and Medical (ISM) band. However users of this allocation have no rights of protection against interference from other users, and must accept any interference which is received. Other users of this spectrum include microwave ovens and Bluetooth.

The 5 GHz spectrum used by IEEE 802.11a [2] enjoys a similar licensing regime.

NOTE 1: Unlicensed in the sense that an individual mobile terminal or access point does not require a specific license to operate.

NOTE 2: Regulated in that national authorities may define permitted power levels and spectral restrictions.

4.4.4 Channelization

There are about a dozen channels defined for IEEE 802.11b [2], which also apply, in principle, to IEEE 802.11g [2]. However, the sad truth is that the dozen channels only apply at very poor protection ratios. No more than half-a-dozen access networks can, realistically, simultaneously be active in the same geographic area at once.

The channelization does, however, improve co-existence between adjacent networks.

As the link speed drops, the interference between adjacent networks also drops.

4.4.5 Registration

When a mobile terminal wishes to receive Wireless LAN service at a hotspot, it must first register with the service. The terminal communicates with the access point, which in turn communicates with the AAA functionality. Traditionally, this happens through a web page with encrypted access, although other methods could, in principle, be used.

After registration a terminal remains registered until a timeout expires.

4.4.6 Handover

There is no standardized handover procedure between one access point and another. If a mobile terminal wishes to maintain its Internet access as it leaves one access point and comes in to range of another, then it must generally manage the registration procedures itself.

(This will be an issue for the future commercial success of Wireless LANs.)

4.5 Security issues

4.5.1 Access protection

Wireless LAN is known for its poor security record. The first incarnations of home and office access points had no protection at all, so any wireless device could connect and use services. "War-driving" (taking a notebook in a car and driving around while searching for open access points) soon became a popular hobby within hacker groups.

Industry responded and introduced security mechanisms like MAC address filtering and access control mechanisms like Wi-Fi Protected Access (WPA).

It is important to note that even nowadays the majority of non-commercial public wireless access points is (intentionally or unintentionally) offering unrestricted access, often to the complete Internet. From a lawful interception perspective this means that caution must be undertaken when assuming certain intercepted traffic belongs to a certain (residential) user. It could well be that a malicious person performed a "drive-by job" and put the blame on the innocent target.

4.5.2 Link protection

The first generation of wireless access points included a traffic encryption mechanism called Wireless Equivalent Privacy (WEP). WEP is based on RC4 encryption using a 40 bit key with a 24 bit Initialization Vector (IV). Because of the weak encryption, WEP can easily be cracked when the attacked obtains enough data (100 MB of data is sufficient).

The next generation of access points offers WPA, which is also using RC4. However, WPA incorporates a protocol called Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger Initialization Vector of 48 bit, this defeats the well-known key recovery attacks on WEP.

From a lawful interception perspective, it may be possible to intercept traffic while "sniffing" the ether, provided the law enforcement officer is near the target. This is of course only a feasible solution when the target is not using link protection at all or is using a weak encryption like WEP.

4.6 Wireless LAN UMTS roaming

LI target may have User Equipment (UE) that supports WLAN, UMTS and GSM radio access technologies. This kind of cases is addressed by 3GPP. 3GPP has defined a framework for 3GPP-WLAN interworking (I-WLAN as defined in TS 23.234 [8], TS 29.234 [9], TS 33.107 [10], TS 33.108 [11]). Two major categories of scenarios were identified.

Scenario 1 defines case when UE authenticates with given WLAN, and uses WLAN for accessing internet services. This scenario is considered to be out of 3GPP scope because of the following reasons. In case UE is 3GPP operator's customer (i.e. is registered at HSS/HLR) but UE opts to use scenario 1, then 3GPP network considers the UE detached from the network. The reason is that neither UE nor WLAN network make aware 3GPP network about UE activities.

Scenario 2 and up define various cases when UE simply uses WLAN radio access network to attach to UMTS/GSM networks. That is, in these scenarios UE authenticates with UMTS/GSM HSS/HLR and receives all services defined in HSS/HLR. In these scenarios UE may change WLAN radio access to UMTS/GSM radio access and vice versa.

TS 33.107 [10] defines interception domain aspects of I-WLAN LI solution. TS 33.108 [11] defines handover domain aspects for I-WLAN LI solution.

5 Lawful Interception of Public Wireless LAN Internet access

5.1 Lawful Interception requirements

5.1.1 Relation to other standards

TS 101 331 [7] describes the LEA requirements for lawful interception. These requirements also apply to interception of wireless LAN. No additional requirements for the interception of wireless LAN exist.

5.2 Lawful Interception reference model

5.2.1 Generic LI architecture

The overall interception framework is extended from the model described in clause 5.2 of ES 201 158 [3] and from the architecture identified in clause 5 of TS 101 671 [4] (see figure 6).

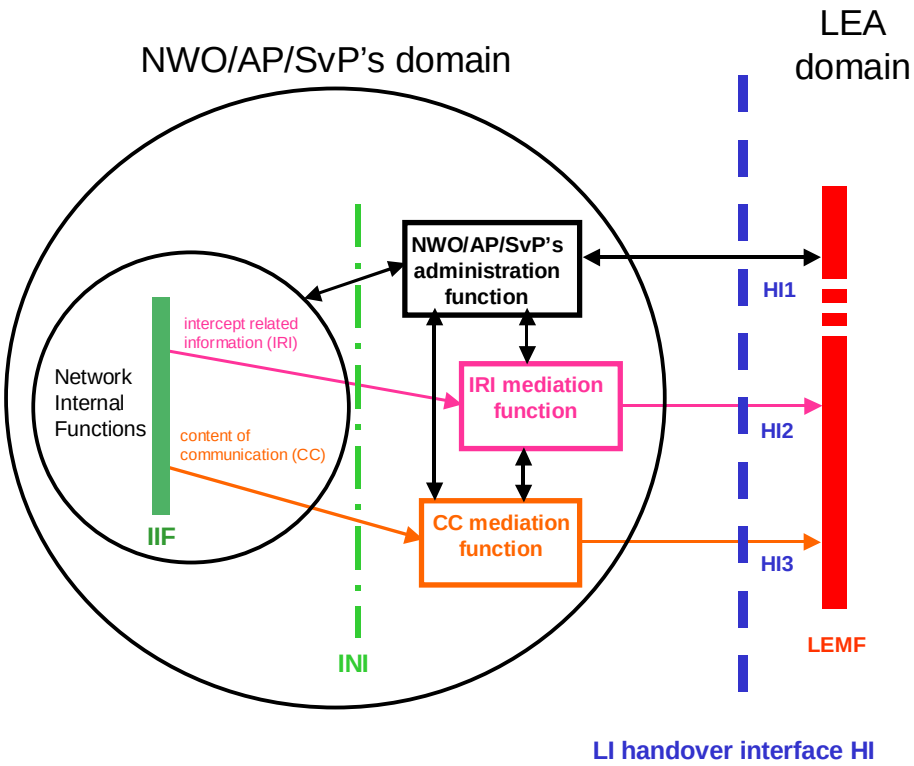


Figure 6: Functional block diagram showing Handover Interface HI

The scope of the present document is the NWO/IAP/SvP's domain as shown in figure 6. The present document describes the internal interfaces INI1, INI2 and INI3 as shown in figure 7.

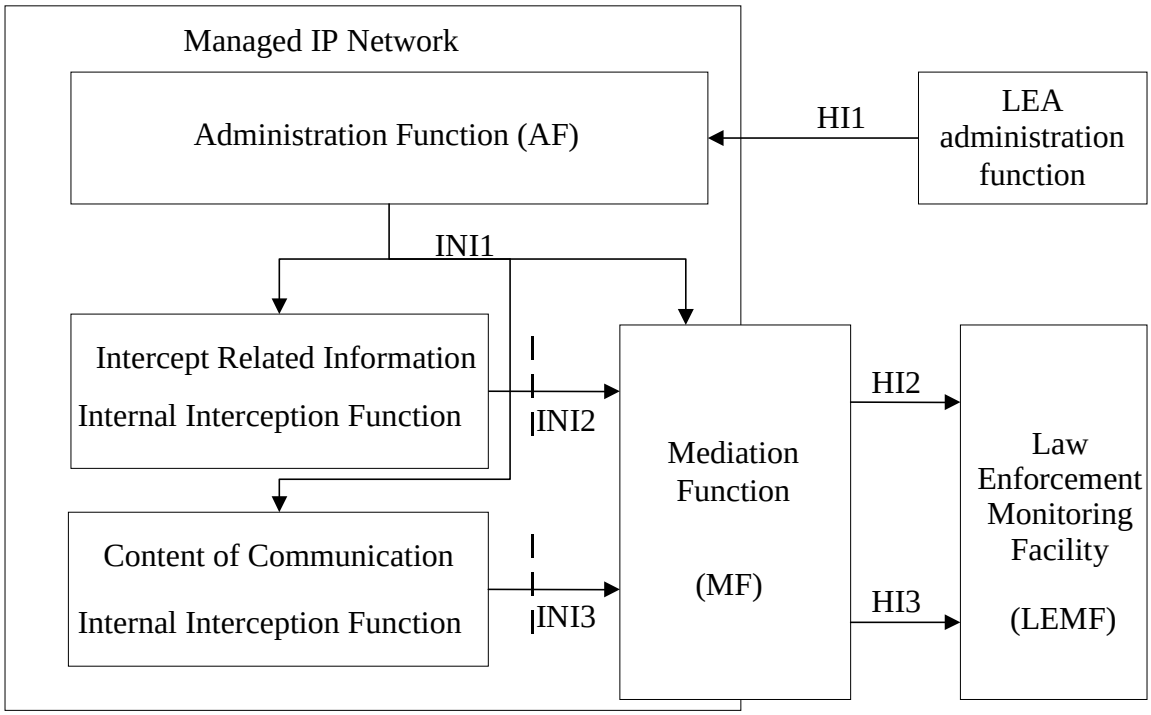


Figure 7: Reference Model for Lawful Interception

The administrative information is exchanged via the Internal Network Interface INI1.

Internal Network Interface INI2 carries Intercept Related Information (IRI). Internal Network Interface INI3 carries Content of Communication (CC) information.

5.2.2 Description of functional elements

5.2.2.1 Intercept Related Information Internal Interception Function

The purpose of the IRI IIF is to generate information related to calls or and other information involving interception targets identified by Law Enforcement Agency (LEA) sessions, i.e. IRI.

The IRI information is sent to the Mediation Function (MF) to be delivered to the Law Enforcement Monitoring Facility (LEMF) over interface HI2.

5.2.2.2 Content of Communication Internal Interception Function

The CC IIF shall cause the CC to be duplicated and passed to the MF. The content may be duplicated within the Media Layer or within the Transport Layer and this may be achieved by any means such that the sender and recipient(s) are unaware of the copying process and cannot take steps that will reveal the copying process is taking place.

The CC is formatted in accordance with later clauses for delivery to the LEMF over interface HI3.

5.2.2.3 Lawful Interception Mediation Function

Within each administrative domain there shall exist a functional entity - the MF. This entity receives information from the IRI IIF(s) and CC IIF(s) within the administrative domain and formats that received information to be passed on to the LEMF. If there is more than one IRI IIF within an administrative domain the MF shall manage the reporting state of the call so that information is sent to the LEMF as if it were from a single IRI IIF. In this case the MF shall ensure that the reported information elements represent a consistent and single view of the intercept.

The MF incorporates the mediation functions as defined in ES 201 158 [3] as "A function which selects sequences and transforms information, including CC when necessary, between a number of IIFs and the HI. Sometimes the mediation function may be a null function, e.g. direct delivery of CC to the LEMF via HI3 with no changes".

5.2.2.4 Lawful Intercept Administration Function

In each administrative domain there shall exist an Administrative Function to manage requests for interception. This function ensures that the request from an LEA to send IRI and or CC information to an LEMF is acted upon. This function is not the subject of this specification and is described here only for completeness.

5.3 Lawful Interception issues

5.3.1 Multi - provider environment

In the service architectures depicted in clause 4.3 of the present document, we can discern different parties; the Wireless Internet Service provider (WISP), the Internet Service Provider (ISP) and the Service Provider (SvP). Since the architecture with Central access control and backhaul to the Internet can be intercepted like a regular IAP environment, this clause concentrates on the architecture with Central access control and federated access to the Internet; a common architecture.

The WISP typically manages and maintains the Wireless Access Points as well as the portal and the logical network infrastructure and AAA services required for first-line identification and authentication of customers.

Internet connectivity may be provided by one or more IAPs; typically the Wireless Access Points are connected to the Internet through a (consumer grade) broadband Internet connection. In turn, the IAP may provide Internet connectivity to multiple WISPs.

Wireless LAN Internet Access may be provided to customers by the WISP, by Service Providers, such as a Mobile Operator offering Wireless LAN Internet Access to its mobile customers, or by both on the same set of Wireless Access Points.

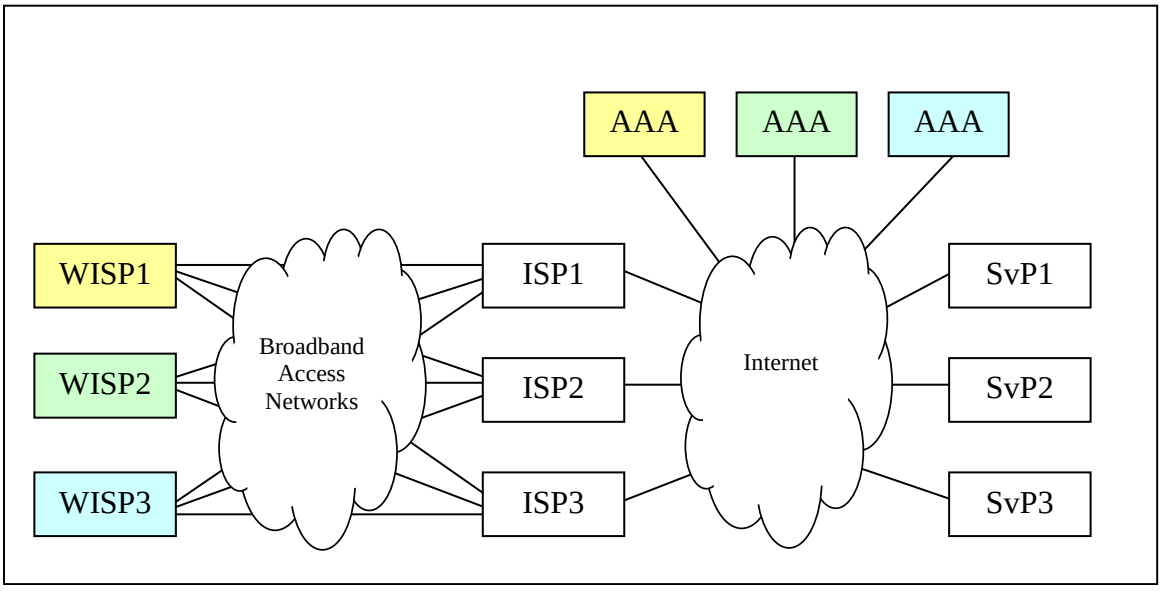


Figure 8: The Multi-provider environment

As an example, in figure 8, the WISP represents a collection of Wireless LAN Access Points, connected through broadband Internet connections obtained from multiple IAPs. The WISPs have a central Internet connected location, typically provided by a hosting provider, housing the equipment for the AAA services. In order to authenticate SvP customers, the WISP may forward AAA requests to the SvP, thereby acting as an AAA proxy for the SvP.

5.3.2 Network Address Translation

Since Wireless LAN Access Points are typically connected through the Internet by a regular broadband Internet connection, in most cases the Wireless LAN Access Points will have only one public IP address. As a consequence, concurrent users of the Wireless LAN Access Points will use a private IP address, handed out at after successful authentication, all sharing the single public IP address. To route traffic to and from the Internet, The Wireless LAN Access Points will in this case apply Network Address Translation (NAT). The use of NAT complicates the interception of Wireless LAN Internet Access immensely, since on the Internet one can not discern the traffic of individual users.

5.3.3 Availability of Intercept Related Information

The Intercept Related Information (IRI) for Wireless LAN Internet Access is similar to that of regular Internet Access; the reference scenario's, events and attributes described in TS 102 234 [1] apply. As an additional attribute, specific for Wireless LAN Internet Access, the "private IP address" may be required.

IRI is typically derived from the AAA events. Therefore, all information required for composing the IRI will be available to the WISP. In cases where the customers of SvP logon to a Wireless LAN Access Point, the WISP may perform the AAA on behalf of the SvP or forward the AAA request to the SvP. If the latter is the case, SvP also has the information required for composing the IRI; obviously only for its own customers.

5.3.4 Availability of Content of Communication

The content of communication for Wireless LAN Internet Access consists of, in line with TS 102 234 [1], the IP packets routed to and from a target using a Wireless LAN Access Point. The only difference with regular Internet Access is, that once the IP packets leave the Wireless LAN Access Point, NAT has been applied and therefore, the public IP address the target is using does not suffice to obtain the traffic. The WISP is the only party capable of obtaining the IP traffic based on the private IP address. If any other party is to obtain the IP traffic, decoding of the NAT algorithm is required; NAT may have to be applied by the WISP in a way that aids decoding. Whether such an approach is feasible requires further study.

5.3.5 Identification of the target

In theory, any attribute used by a target for identification to the WISP, may be used for identification of the target. In the preparation of an intercept, efficient, fast, and structured means should be provided to obtain attribute bindings where lookups are required in subscriber data management systems. In general, the preparation process must provide identifying information that is exchanged between the potential target and the AAA service as part of the logon procedure in the access domain. Attributes which may be used include a real name or alias, a credit card number, public cryptographic key, or anything else that may provide target identification.

For information exchanged as part of the logon in the access domain, one can think of the following attributes:

Username: This applies only to subscription users. The username may be provided by the WISP as part of a WISP subscription or by a SvP that offers Wireless Internet Access to its customers via the particular WISP. In the latter case the username may be, for example, a cell phone number for a Mobile Operator or an IAP username, which may be forwarded by the WISP AAA service to the SvP AAA service for authentication. As in every identification and authentication procedure, spoofing and masquerading are an issue that must be taken into account.

MAC address: Alternatively the target may be identified by means of the MAC address of the device used for Internet Access. The device may be a laptop, a PDA or even a cell phone with wireless LAN capability. It must be noted that the MAC address can very easily be spoofed and traffic obtained by this means should be treated as such.

Scratch card number: Although not likely, it is possible that a target uses a scratch card with a number, or number in a range, that is known in advance by the LEA. If such is the case, the scratch card number may be used to identify the target.

5.3.6 Capabilities of Wireless LAN Access Points

If one plans using Lawful Intercept facilities on the Wireless LAN Access Points itself, one must consider the capabilities of the device offering the Wireless LAN Access. The actual device may be either a proprietary box or an open device such as a PC in a box running Linux. In the case of a proprietary device, its supplier must provide Lawful Intercept facilities. In the case of an open device, Lawful Interception software may be developed to run on the device.

In the latter case, one must realize that a PC in box typically has a relatively slow CPU (in the range of a couple of hundreds of MHz), typically has no hard disk but more likely a flash RAM memory and limited volatile RAM. This limits the possibilities of the Lawful Interception software for using high speed processing and CPU intensive tasks such as asymmetric encryption.

5.3.7 Security of the Wireless LAN Access Points

The Wireless LAN Access Point is typically located in a hostile environment, i.e. not physically secured and in a worst case even prone to theft. Therefore, target information stored on Wireless LAN Access Point, if any, must not be stored persistently.

5.4 Lawful Interception solution approaches

Lawful Interception of public Wireless LAN Internet Access can basically be approached in two different ways, each applicable to particular architectures as presented in clause 4.3 of the present document.

5.4.1 Centralized Lawful Interception

The architecture with Central access control and backhaul to the Internet allows for centralized interception, since all IP traffic of all Wireless LAN Access Points is routed over a central spot in the infrastructure. Although one may have to cope with private and public IP addresses, e.g. NAT, the interception approach described in TS 102 234 [1] fully applies. Therefore, centralized interception will not be elaborated upon any further.

5.4.2 Decentralized Lawful Interception

The architectures with Central access control and federated or local access to the Internet require another interception approach, since the IP traffic is routed from an to the internet without ever reaching a central location held by either WISP or SvP. Therefore, interception must take place in a decentralized fashion; preferably on the Wireless LAN Access Points or Wireless LAN Access Point concentrators itself.

A possible approach to this kind of decentralized interception is presented in the figure 9 and will be explained there under.

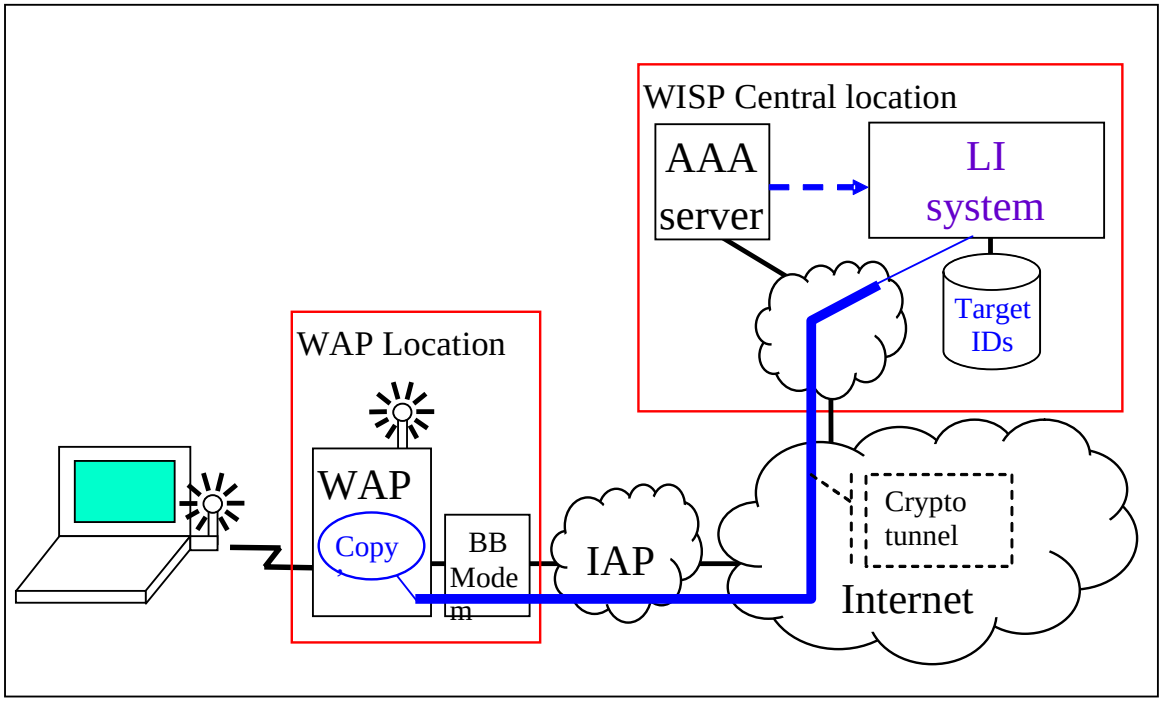


Figure 9: Decentralized Lawful Interception approach

Centralized TargetID storage: In order to prevent disclosure of target IDs, the list of targets IDs is kept inside a well-protected central location, under control of the WISP.

Secure inspection of AAA traffic: The Lawful Intercept system is provided with a copy of every AAA event handled by the AAA server. This way scanning of AAA traffic for target IDs can take place inside the LI system, thereby avoiding extreme security measures for the AAA server.

Secure communication with the WAP: Every WAP is connected with the WISP's central location via a secure, encrypted tunnel. This tunnel is preferably dedicated for LI purposes; for regular management purposes another tunnel may be maintained.

Collection of IP traffic: Once the LI system encounters a target logon in the AAA traffic, a collection process ("copy") on the WAP is provisioned with the private IP address of the target. This collection process takes copies of all IP packets from and to the particular private IP address and forwards these through the tunnel. The transport of intercepted traffic may entail encapsulation inside an LI specific protocol. Note that redirection of target traffic, as opposed to copying, is not an option, since the alternate traffic path may be spotted using tools such as "tracert".

NOTE: The use of an asymmetric, low-bandwidth network connection to the WAP, such as low-end, consumer-grade ADSL, may prohibit application of decentralized interception, since the available upstream bandwidth may not be sufficient to carry the intercepted traffic. In case of a high-bandwidth asymmetric, network connection, throttling the downstream bandwidth per user is still required to prevent choking the upstream when transmitting intercepted traffic.

6 Conclusion and recommendations

6.1 Conclusions

In most cases, wireless LAN may be seen as "just another way of internet access". However, a few differences with other ways of internet access can be summed up:

1) Collection of the content of communication can be hard, especially in cases where a federated network is used. Because IP addresses are translated before entering the public internet, interception should take place in or close to the access point. This is an implementation issue and requires no further action from TC-LI.

2) Because the target can be a roaming user, providing location information in the HI2 is important. TS 102 234 [1] already contains ASN.1 for targetLocation with remark "for further study".

6.2 Recommendations

It is recommended that TS 102 234 [1] is expanded so that it also applies to interception of wireless LAN. Specifically, the ASN.1 should be updated so that a geographic location can be included.

Annex A (informative): Information flows on Internal Network Interfaces

This annex describes the requirements for the INIs. It introduces the required information flows as well as the required data for both the IRI IIF and the CC IIF. For the purpose of simplification of the diagrams IRI IIF and CC IIF are both called Internal Interception Function (IIF) in this clause.

It is not the intention of this annex to define a protocol for INI. It rather aims to show which kind of information is necessary to be contained in the communication between Administrative Function (AF) and a IIF. The means of transport may be UDP, TCP or embedded in an application protocol such as SNMP or COPS.

A.1 Activation of LI

Clause (*reference to AF definition*) shows a list of data available at the AF. This information has to be conveyed to the IIF for the activation of the LI.

The information passed from the AF to the IIF for the purpose of the activation of LI shall include at least:

- LIID;
- Identities to intercept;
- Start, stop time, respectively the duration of the interception;
- Destination address of the DF for IRI, CC;
- Credentials to fulfil the security service requirements for the delivery to the DF.

Figure A.1 illustrates the information flow for the activation of LI. Depending on the architecture that implements this flow the IIF may be either the AM, PS or CMTS. The number of concurrent LI activations in one message is an implementation issue and may or may not be allowed by the chosen protocol. However, the activation of an entered LI at the HI1 shall be forwarded to the LI functions immediately on reception.

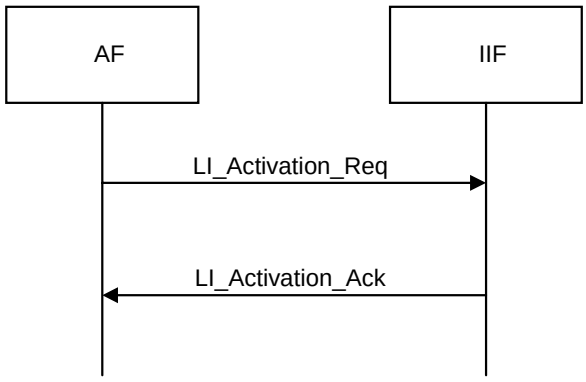


Figure A.1: Information flow for the activation of LI

Table A.1 lists the parameters of the message `LI_Activation_Req`. For a detailed break-down of all parameters see, the ASN.1 encoding (FFS).

Table A.1: Message LI_Activation_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
TargetAddress	M	Application level address of the target to intercept; may be a.o. a telephone number
TargetName	O	Name of the target
AdditionalTargetData	O	Additional information about the target
MonitorServiceList	M	A List of services to intercept
MFIRIAddress	O	Transport address of the MF to send intercepted IRI data to; be negotiated on the fly
MFCCAddress	O	Transport address of the MF to send intercepted CC data to; be negotiated on the fly
LIParameterList	O	List of additional parameters like traffic filters

Table A.2 illustrates the answer of the IIF, message `LI_Activation_Ack.`

Table A.2: Message LI_Activation_Ack

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
ActivationResult	M	Result of the activation operation

A.2 Modification of LI

This information flow is used to update a LI activity, e.g. to change the interception period or the communication identity used by the target.

Important information that shall be conveyed includes:

- LIID;
- Parameters to be changed.

The information flow is depicted in figure A.2. The message to acknowledge the request contains the positive or negative result of the processed request.

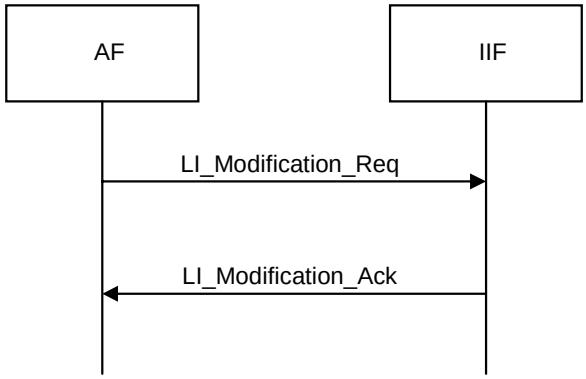


Figure A.2: Information flow for the modification of an LI activity

Table A.3 lists the parameters of the message `LI_Modification_Req.`

Table A.3: Message LI_Modification_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
LIMediationEntry	O	It contains the required parameters for a session between the MF and a IIF
LIStreamEntry	O	It allows the definition of a particular stream to be used for the interception
LIIPStreamEntry	O	It specifies an IP traffic filter for the stream
LI802StreamEntry	O	It specifies a MAC traffic filter for the stream

Table A.4 illustrates the answer of the IIF, message `LI_Modification_Ack`.

Table A.4: Message LI_Modification_Ack

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
ModificationResult	M	Result of the modification operation

A.3 Deactivation of LI

This flow is used to deactivate the LI of an LIID's identity or of all LIID related interceptions, as implemented. The required fields are:

- LIID;
- CID.

This request may be used to stop an ongoing interception for a certain communication identity before the interception period is finished. Reasons for such requests may include that the interception of a certain communication service is no longer required. The information flow is shown in figure A.3.

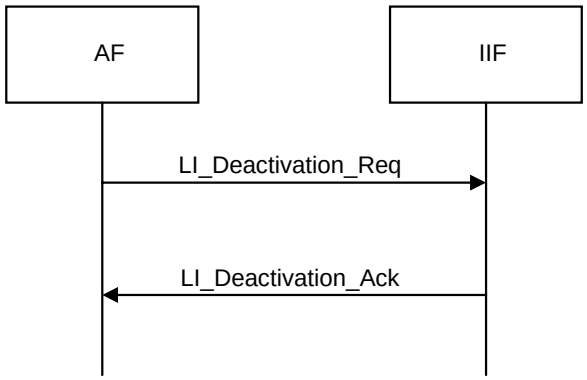


Figure A.3: Information flow for the deactivation of an LI activity

Table A.5 lists the parameters of the message `LI_Deactivation_Req.`

Table A.5: Message LI_Deactivation_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
DeactivateServiceList	O	It specifies the services for which interception shall be ceased

Table A.6 illustrates the answer of the IIF, message `LI_Deactivation_Ack.`

Table A.6: Message LI_Deactivation_Ack

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
DeactivationResult	M	Result of the deactivation operation

A.4 Interrogation of LI

This information flow allows for requesting status information about certain LI activities at the IIF. The following fields shall be included:

- LIID;
- Relevant CID;
- Type of requested information.

Figure A.4 demonstrates the corresponding message exchange.

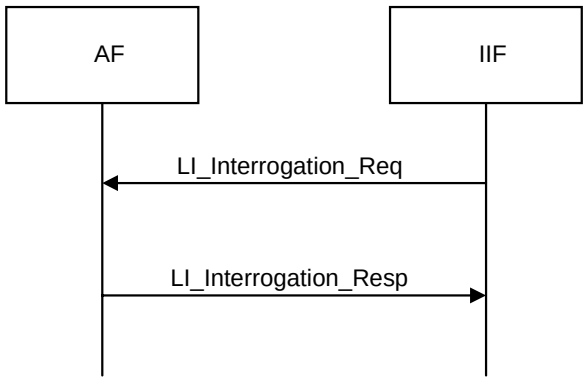


Figure A.4: Information flow for requesting status about an LI activity

Table A.7 lists the parameters of the message `LI_Interrogation_Req.`

Table A.7: Message LI_Interrogation_Req

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
LIInterogateList	M	A list of parameters to be retrieved from the IIF

Table A.8 illustrates the answer of the IIF, message `LI_Interrogation_Resp.`

Table A.8: Message LI_Interrogation_Resp

Parameter name	Status	Description
ProtocolVersion	M	Version number of the protocol
LIID	M	The identifier for the interception
Timestamp	M	Time of sending for sequencing of information and for application layer security measures
CryptoCheckSum	O	Checksum for application layer security, like integrity and source authentication
ModificationResult	O	Result of the modification operation
LIMediationEntry	O	Describes where intercepted data shall be sent to at the MF
DevceCapabilities	O	Describes the interception capabilities of the IIF
LIIPStreamCapabilities	O	Describes the capabilities for the specification of IP traffic filters
LI802StreamCapabilities	O	Describes the capabilities for the specification of MAC traffic filters
LIStreamEntry	O	Describes the current stream that is intercepted
LIIPStreamEntry	O	Describes the current IP traffic filters
LI802StreamEntry	O	Describes the current MAC traffic filters

Annex B (informative): Change Request History

Status of the present document Lawful Interception of public Wireless LAN Internet Access		
Date	**Version**	**Remarks**
February 2006	1.1.1	First publication of the TR after ETSI/TC LI#11 (31 Jan – 2 February 2006, Saint Martin) approval. Version 1.1.1 prepared by Johan Bakker (KPN) and Mark Lastdrager (Pine) (rapporteur).

History

Document history		
V1.1.1	May 2006	Publication