Lawful Interception Systems.

(A Brief Technical Overview)

Hakan EKIZER
Chief Advisor, Monitor to KP
UNMIK-DOC / Support&Services
Cybercrime&Computer Forensics Expert
Telecommunications&Networks Specialist

What is Lawful Interception ?

Lawful interception (LI) is the legally authorized process by which a network operator or service provider gives law enforcement officials access to the communications (in every kind of telephone calls, internet traffic and satellite communications etc) of private individuals or organizations. Lawful interception is becoming crucial to preserve national security, to combat crimes and to investigate serious criminal activities.

The work in Lawful Interception has its foundation in the European Council Resolution of January 1995 [29] which outlined the International Requirements for the Lawful Interception of Telecommunications now known widely as the IUR. This was the result of several years of work by the European governments in cooperation with Australia, New Zealand, Canada and the USA.

The standardization of lawful interception is vital to provide an economically and technically feasible solution that complies with national and international conventions and legislation. ETSI has played a leading role in the standardization of lawful interception since 1991; today work is concentrated in Technical Committee Lawful Interception (TC LI), which enjoys the active participation of the major telecom manufacturers, network operators, Law Enforcement Agencies and regulatory authorities of Europe and from around the world. ETSI's LI work covers the whole spectrum of interception aspects, from a logical overview of the entire architecture and the generic intercepted data flow, to the service-specific details for e-mail and Internet.

According to ETSI standards my aim within this white paper is briefly describing How a LI system can build up. You can also find out ETSI documentations for much more detailed and technical information.

LI Overview from ETSI Perspective.

Lawful Interception (LI) is a requirement placed upon service providers to provide legally sanctioned official access to private communications. With the existing Public Switched Telephone

Network (PSTN), Lawful Interception is performed by applying a physical 'tap' on the telephone line of the target in response to a warrant from a Law Enforcement Agency (LEA). However, Voice over IP (VoIP) technology has enabled the mobility of the end-user, so it is no longer possible to guarantee the interception of calls based on tapping a physical line.

Whilst the detailed requirements for LI may differ from one jurisdiction to another, the general requirements are the same. The LI system must provide transparent interception of specified traffic only and the subject must not be aware of the interception. The service provided to other users must not be affected during interception.

Architecture Overview

Although the detail of LI may vary from country to country we can look at the general logical and physical requirements and also explain much of the common terminology used. The primary purpose of the service provider network is to enable private communications between individuals; any LI functionality built into the network must not affect the normal service to those individuals. The architecture requires a distinct separation of the Public Telecom Network (PTN) and the networks used for distribution and processing of LI information. The interfaces between the PTN and the Law Enforcement Monitoring Facility (LEMF) are standardized within a particular territory.

LI deals with two 'products', these are; Contents of Communications (CC) and Intercept Related Information (IRI). Contents of Communications is exactly what it sounds like: the voice, video or message contents. Intercept Related Information refers to the signaling information, the source and destination of the call etc.

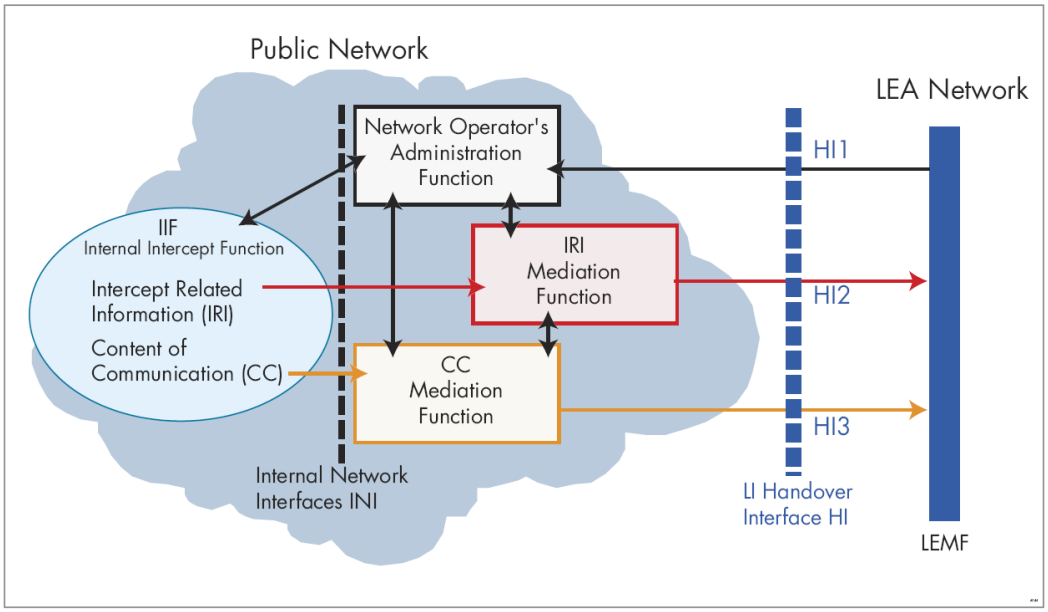

Figure 1 - General Network Arrangements for Interception (ETSI)

Figure 1 shows the logical flow of Intercept Related Information (IRI) and Contents of Communications (CC) from its collection in the Public Network to the handover interface to the Law Enforcement Monitoring Facility (LEMF) as defined by ETSI. In North America CALEA (Communications

Assistance for Law Enforcement Act) requires operators to provide LI capabilities. The network architecture and handover specifications are based on the PacketCable™ surveillance model shown in **Figure 2** below, the general architectural similarities can be seen.

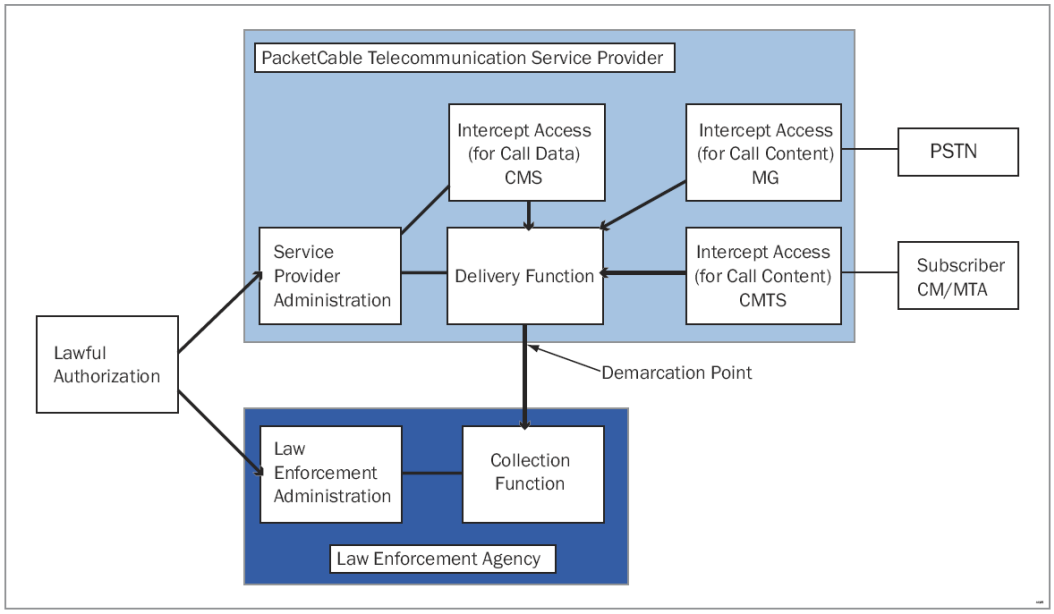

Figure 2 – PacketCable™ Surveillance Model

Figure 3 below shows the high-level functions and interfaces as defined by ETSI, the Mediation Function (MF) provides standardized interfaces, HI2– Intercept Related Information, and HI3 – Call Contents, from the Public Telecom Network to the LEA Network.

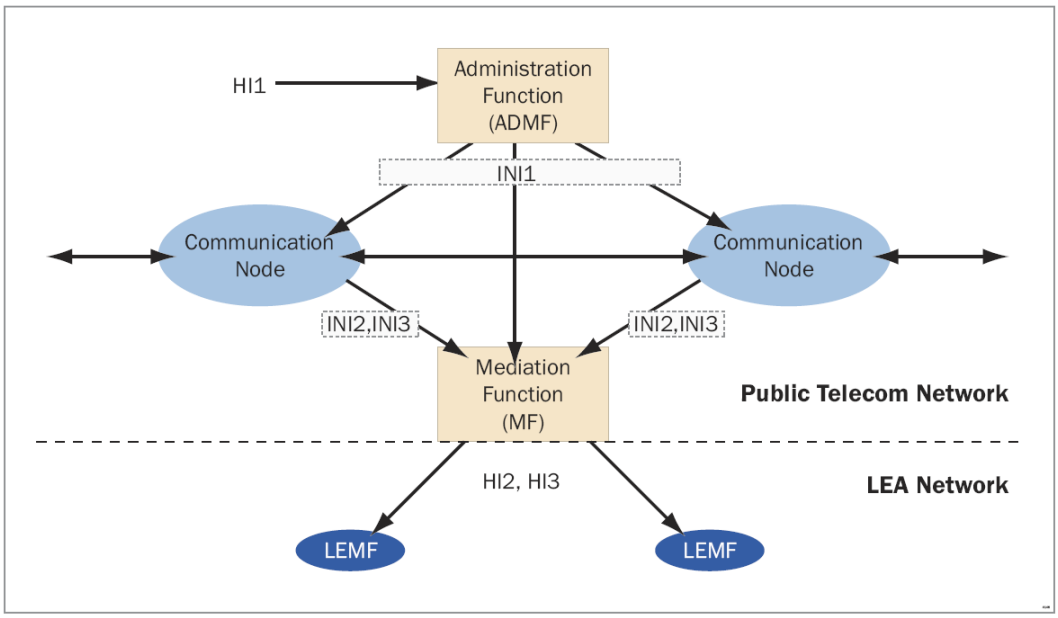

Figure 3 - Distinction between PTN and Law Enforcement Network

Basic Elements of LI in a Public Telecom Network

There are three primary elements required within the public network to achieve Lawful Interception, these are:

- An Internal Intercept Function **(IIF)** located in the network nodes.
- A Mediation Function **(MF)** between the PTN and LEMF.
- An Administration Function **(ADMF)** to manage orders for interception in the PTN

Internal Intercept Function (IIF):

These functions are located within the network nodes and are responsible for generating the Intercept Related Information (IRI) and Contents of Communications (CC).

Mediation Function (MF):

This function clearly delineates the PTN from the LEMF. It communicates with the IIFs using Internal Network Interfaces (INIs) which can be proprietary. The MF communicates to one or more LEMFs through locally standardized interfaces: the Handover Interfaces (HI2and HI3).

Administration Function (ADMF):

This function handles the serving of interception orders and communicates with the IIFs and MF though an Internal Network Interface.

Implementing LI within an VoIP Network

One of the primary problems that service providers face when managing VoIP and multimedia calls is the separation of the signaling and media streams. In other words it is quite possible that the two streams may take completely different paths through the network. In addition, even when they do pass through the same device, it may not be aware of the relationship between the streams. Some devices within the network are however specifically designed to understand and manage the separate signaling and media streams – session border controllers. Typically located at the borders of the service provider's network, these offer an ideal location to implement the IIF as they receive Intercept Related Information from the signaling stream and can intercept Contents of Communication directly from the media stream.

Figure 4 below shows the physical elements of the LI system, their logical functions and the interfaces to the LEMF. (all page)

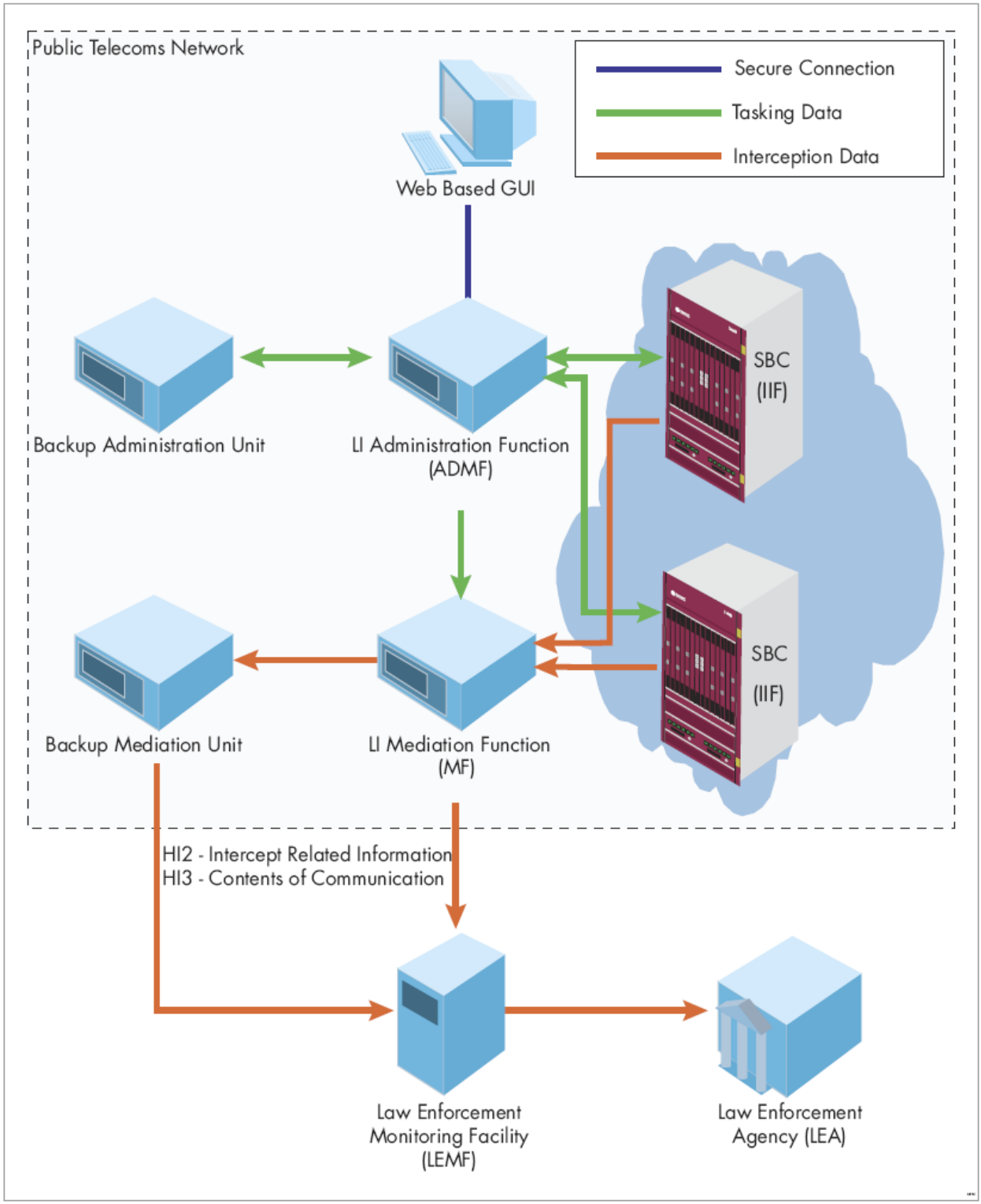

Figure 4 –Example Physical Architecture

LI Administration Function (ADMF):

ADMF is typically implemented on a hardened Management Unit; it provides a secure method to enable traffic to be targeted and routed. The ADMF uses a secure connection to one or more of the IIFs and to one or more Mediation Units. The ADMF is often backed up by a warm standby, which replicates all data between the units.

LI Mediation Function (MF):

MF performs the mediation and delivery functions, it is typically implemented on a hardened Mediation Unit; it receives generic formatted IRI and CC data from one or more IIFs and translates it into the country specific format for the Handover Interfaces (HI2& HI3) to the LEMF. The MF receives target details from the ADMF and validates the received IRI and CC data to ensure that only the warranted data is passed to the LEMF. The MF usually supports the forwarding of intercepted traffic to many LEMF interfaces simultaneously. The Mediation Unit is often backed up by a slave unit which takes over in case of failure of the primary unit.

Internal Intercept Function (IIF):

IIF is most effective when implemented in hardware within the network nodes in order to provide the most effective and rapid detection without incurring additional software processing and delays which may allow the presence of the intercept to be detected. The IIF collects Intercept Related Information (IRI) and Contents of Communication (CC) ask requested by the ADMF, and converts these to a generic format which is passed to the MF.

Administration Functions

The ADMF must only be accessed by authorized users. It will manage the deployment of tasks to the other LI elements.

Tasking Targets – Each target will require a Warrant ID and Case ID assigned by the LEA. Each case may require IRI or CC or both to be intercepted. Each task is assigned a start date and an end date, upon which the case will expire.

Auditing Tasks – The ADMF is typically responsible for auditing the network of IIFs to ensure that the target lists match; differences should be automatically reconciled.

Mediation Function Configuration – Each interface to the LEMF must be individually specified to match the required standard output.

Information Volatility

Essential target information must be encrypted by the ADMF and any information stored in the IIF in encoded form, thereby preventing unauthorized access to sensitive warrant information. Any information stored within the IIF should be stored in volatile memory, so that this information is erased

if a component of the network node is removed or powered down. Only the encrypted database of the ADMF should be maintained during power-down situations.

In the event of a link failure between the MF and the LEMF the intercept products may be buffered for a short time in memory only. Any long term failure of the interface will result in intercept products being lost – this information must not be spooled to permanent storage.

Conclusion

Recently it has become increasingly clear that VoIP services will be expected to provide Lawful Intercept and Emergency Call Handling services to the same level experienced in the PSTN. The FCC in North America for example has mandated that both emergency calls and Lawful Intercept must be available. Whilst not all countries mandate this capability, any network operator building a publicly available voice or multimedia over IP service today will need to plan a network which is flexible enough to implement these regulatory services in the future. Session border controllers are being deployed at strategic points within VoIP networks to execute a number of access, security and quality management roles; they offer an ideal location to implement a Lawful Intercept solution. Carrier class SBCs already offer the levels of redundancy and resilience to provide 'five 9s' availability, further endorsing their suitability for the location of the IIF.

Terminology

ADMF	Administration Function
CALEA	Communications Assistance for Law Enforcement Act
CC	Contents of Communication
ETSI	European Telecommunications Standards Institute
HI	Handover Interface
IIF	Internal Intercept Function
INI	Internal Networks Interface
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
PSTN	Public Switched Telephone Network
PTN	Public Telecom Network
VoIP	Voice over IP

References

ETSI TS 101 331 - Telecommunications security; Lawful Interception (LI) Requirements of Law Enforcement Agencies
ETSI TR 101 943 - Telecommunications security; Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture
ETSI TS 101 671 - Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
PKT-SP-ESP1.5-I01-050128; PacketCable™ 1.5 Specifications; Electronic Surveillance
A summary of the ETSI LI specs is located at:http://portal.etsi.org/li/Summary.asp
Current ETSI specs can be downloaded from:http://portal.etsi.org/li/status.asp
Current PacketCable™ specs can be found at:http://www.packetcable.com/specifications/