LAWFUL INTERCEPTION FOR 3G AND 4G NETWORKS

White Paper

March, 2010

Aqsacom Document No. 100458

Copyright 2003-2010 Aqsacom Inc. and Aqsacom SA. No portion of this document may be reproduced without the expressed permission of Aqsacom. The data and figures of this document have been presented for illustrative purposes only. Aqsacom assumes no liability for errors or omissions.

Table of Contents

1 Introduction 4

2 Mobile Network Types 4

2.1 3G Technology and Deployments 4

2.1.1 Earlier Generations (Pre-3G) 5

2.1.2 3G and Later 6

2.2 4G Evolutionary Paths 8

3 Wireless Network Architecture Overview 11

3.1 3.XG Networks 11

3.2 4G Type Networks 15

3.2.1 LTE Networks 15

3.2.2 WiMAX 17

4 The Architecture of Lawful Interception 19

5 Lawful Interception Configurations for 3G and 4G Networks 21

5.1 3G Network Interception 21

5.2 LTE Network Interception 23

5.3 WiMAX Network Interception 25

5.4 Location-Dependent Interception Issues 26

6 Aqsacom's ALIS Mediation Platform 27

7 ALIS Implementation in 3G / 4G Networks 29

8 Summary 34

9 References 36

Aqsacom SA (Europe)
Les Conquerants, Bât B Everest
1 avenue de l'Atlantique
Les Ulis Courtabeouf Cedex
F-91976 France
Tel.+ 33 1 69 29 36 00
Fax +33 1 69 29 84 01

Aqsacom pty (Southeast Asia)
Suite 1009
530 Little Collins Street
Melbourne VIC 3000
Australia
Tel. +61 399 097 280
Fax +61 399 097 275

Aqsacom Inc. (Americas)
Washington, DC
Tel/fax +1 202 315 3943
New York +1 917 750 8614

Aqsacom (EMEA)
PO Box 125 139
Dubai, United Arab Emirates
Tel. +971 (0) 4 3990048
Fax +971 (0) 4 3990228

sales@aqsacom.com
www.aqsacom.com

Lawful Interception for 3G and 4G Networks

Aqsacom SA and Aqsacom Inc.

1 Introduction

Since the original 2004 publication of our earlier White Paper *Lawful Interception for 3G Networks*, considerable progress in the evolution of mobile networks has taken place. Original 3G specification drafts and deployments were oriented towards a migration from legacy GSM / GPRS architectures. More recently, 3G networks have taken on newer architectures for higher data throughputs with enhanced subscriber capacity, giving way to the deployment of so called "4G" networks.

Given that commercially deployed wireless networks are at various stages of deployment, a common methodology for the implementation of interception systems is evermore critical. This White Paper therefore shows how Aqsacom addresses lawful interception requirements as applied to 3G networks and paths to the 4G realm.

This document will first provide a brief description of the various evolutions of public mobile networks that have been commercially deployed, followed by a discussion on the evolution toward the newer "long term evolution" technologies. We then discuss possible configurations for lawful interception of the evolving mobile networks, followed by descriptions of approaches to 3G / 4G interception solutions now available from Aqsacom.

2 Mobile Network Types

In this section we cover the various types of networks currently in use by commercial mobile network operators, starting with 3G networks as a baseline of comparison for past and future types of services. We conclude this section with a description of current and evolving "4G Networks."

2.1 3G Technology and Deployments

Despite the publicity and earlier hype of carriers promoting their 3G wireless services, the term "3G" is rather loosely used. 3G mobile's broad definition calls for the support of enhanced multimedia services (voice, data, video) and applications (E-mail, cell phone, paging, Web browsing), all at data rates higher than those of the earlier generations of wireless services. Strictly speaking, the "official" definition of 3G is a series of performance specifications and reference architectures set forth by the International Telecommunications Union (ITU) International Mobile Telecommunications IMT-2000 group. These requirements call for a network to conform to the Universal Mobile Telephone System (UMTS) and possess uplink/downlink data transmission speeds at 2 Mbs, 384 kbs, and 144 kbs for indoor pico cell, outdoor micro cell, and outdoor macro cell settings, respectively (see Table 2-1).

Table 2-1: Summary of IMT 2000 Requirements for "3G"

Coverage	Min. up/down data rate
Indoor (Pico Cell)	2 Mbps
Local Pedestrian (Micro Cell)	384 kbs
Regional or Vehicular Traffic (Macro Cell)	144 kbs

True UMTS, otherwise informally known as WCDMA because of the UMTS' use of Wideband CDMA (Code Division Multiple Access) modulation in the air space, conforms to the IMT-2000 "3G" requirements. Nevertheless, many transmission standards do not fit the speed requirements even though their proponents continue to classify such standards as 3G. Some networks use technologies that allow for data rates that substantially exceed the IMT-2000 standards. These networks can be considered 3.XG or even 4G (discussed later in this document).

2.1.1 Earlier Generations (Pre-3G)

For background purposes, we begin discussing pre-3G wireless network architectures and implementations. Such networks remain important in the context of lawful interception because they continue to be widely used given the backward compatibility of the newer wireless technologies to the earlier ones; i.e., most so-called 3G handsets and devices will operate on the earlier 2G networks. Furthermore, 2G networks remain the norm in many parts of the developed and developing worlds where 3G networking technology has not yet been deployed, or has been delayed in anticipation of 4G deployments.

The following summarize the capabilities of the transmission standards, some of which may be better described as "2.5G" (e.g., *EDGE* or *CDMA2000 1X*).

GPRS (General Packet Radio Service):

> This service complements GSM voice and rides within the 200 kHz band reserved for GSM channelization. It is a packet-based service with a theoretical transmission speed of up to 172 kbs, although current operator implementations and handsets typically operate at much slower speeds. The packet mode enables the service to be "always connected." GPRS remains a commonplace wireless networking technology wherever GSM is deployed, mainly for support of the large base of legacy GPRS handsets and modems still in use as well as fall-back radio infrastructure from more advanced networking.

EDGE (Enhanced Data Rates for GSM and TDMA Evolution):

EDGE updates GPRS technology by using higher-order data coding schemes for the radio links; however, EDGE's radio modulation maintains the time slot TDM methods of GSM. This backward compatibility to GSM makes network upgrades to EDGE manageable, although not necessarily trivial to perform on a large scale. Because it maintains GSM legacy, it is referred to as a "2.5G" network evolution. Despite its theoretical transmission speed of over 300 kbs, users will be more likely to find rates of from about 20 to 100 kbs. EDGE continues to be a heavily used data service worldwide given the ubiquity of legacy GSM network infrastructure and the simple fact that many users still do not possess 3G handsets and other devices.

CDMA2000 1X RTT:

This standard follows from the CDMAOne (CDMA IS95) group in that it applies the same 1.25 MHz channel bandwidths as its earlier generation system (hence the term 1X). RTT stands for Radio Transmission Technology. This standard supports theoretical data transmission rates of 307 kbs. CDMAOne and CDMA2000 are widely deployed in the US, Canada, China, the Asia/Pacific region, as well as in Africa [1], but market pressures are now encouraging CDMA network operators to migrate towards 4G technologies.

2.1.2 3G and Later

So-called 3G services presently dominate the operations and services of wireless network operators through the developed world. Wireless network operators have embraced 3G technologies, especially at the radio level, because of WCDMA's more efficient use of radio spectrum, thereby enabling the support of more voice customers for a given amount of bandwidth resources. Of course, 3G networks support ubiquitous data services as well, which are taking on exponential customer growth thanks to the disruptive nature of newer generations of smart phones (e.g., the Apple iPhone and iPhone-like devices), smart phone applications ("apps"), and emerging tablets and other devices that will be linked to wireless networks and rely on wireless data services.

UMTS (WCDMA):

UMTS (Universal Mobile Telephone System) has been developed under the 3GPP (3rd Generation Partnership Project) Working Group and proposed as the underlying architecture supporting the "true" 3G standard It is commonly called "WCDMA" (Wideband CDMA) because of its use of CDMA in the air space modulation. The standard makes use of 5 MHz for transmission and 5 MHz for reception, thereby consuming relatively more bandwidth than its distant cousin GSM (200 kHz). WCDMA has been widely rolled out throughout Europe, Asia, and the US by the legacy GSM carriers and constitutes the predominant later-generation network architecture presently in place worldwide [2].

CDMA2000 1X EV-DO:

This represents the next evolutionary step up from networking based on the CDMAone standard (hence the term "EV"). The standard makes use of Qualcomm's High Data Rate (HDR) system, which supports packet data rates of up to 2.4 Mbs. Qualcomm holds core patents to this technology, as it does in the other technologies behind the CDMA and WCDMA standards. CDMA2000 1X EV-DO has supplanted 1x RTT in most markets served by CDMA, and can support true mobile 3G services according to the IMT-2000 3G definition [1]. Nevertheless, 1x RTT is still used as a "fall back" by handsets when EV-DO is not available.

HSPA (High Speed Packet Access) and HSPA+

This technology mainly constitutes an upgrade to the radio interface of 3G UMTS networks, thanks to more advanced data coding schemes. In effect, it is a 3.XG type networking technology, and has enabled carriers to facilitate their race towards 4G-type services. Deployments are divided into High Speed Downlink Packet Access (HSDPA), which can offer up to 14.4 Mbs, and High Speed Uplink Packet Access (HSUPA) which can allow for up to 5. 8 Mbs. HSPA+, otherwise known as *HSPA Evolution*, attains higher data rates (42 Mbs downlink, 11 Mbs uplink) through the use of MIMO antenna technologies and advanced data coding and radio channel combining methods (see Figure 2-1). In analogy to EDGE's upgrade path from GPRS, HSPA can be built over existing UMTS networking infrastructure; however, increased user bandwidths with reduced latency can be achieved by migrating the underlying network core infrastructure to an all-IP network. Such migrations, in effect, prepare operators for Long Term Evolution deployments, which are currently just beginning (discussed further below). HSPA and HSPA+ networks are now becoming prevalent in developed markets where existing 3G infrastructure is already deployed, especially in the US, Europe, and parts of the Asia / Pacific.

Rel-99	Rel-5	Rel-6	Rel-7	Rel-8	Rel-9 and beyond
WCDMA	HSDPA	HSUPA	HSPA+	HSPA+	HSPA+
DL: 1.8 – 14.4 Mbps UL: 384 kbps		DL: 1.8 – 14.4 Mbps UL: 5.7 Mbps	DL: 28 Mbps UL: 11 Mbps	DL: 42 Mbps UL: 11 Mbps	DL: 84 Mbps and higher UL: 23 Mbps and higher

2009 2010 2011 2012

Figure 2-1. Migration of 3G networking towards higher speeds, thanks to HSPA and HSPA+ advancements in the radio layer (based on [3]).

TD-SCDMA (Time Domain Synchronous Code Division Multiple Access)

This standard was developed by the Chinese Academy of Telecommunications Technology, Datong, and Siemens [4]. The standard addresses the Chinese government's concern that China was too dependent on 3G mobile technology from Western companies. TD-SCDMA is an alternative air interface to WCDMA in UMTS networks, and proponents of the standard claim that it can achieve 3G functionality at a substantially lower cost than WCDMA / UMTS. The standard is covered in 3GPP Release 4 and its commercial deployment was timed with the 2008 Summer Olympics in Beijing. TD-SCDMA was intended not only to serve as a platform for 3G data services for mobile subscribers, but also to facilitate the deployment of conventional voice services that competes against wireline voice or where wireline is not available. TD-SCDMA supports data links of up to 2 Mbs, thereby qualifying it (in theory) as a true 3G standard. Its deployment began in earnest during 2009 (after years of delay) by China Mobile, China's largest wireless operator. Given the similarity of TD-SCDMA's and Western UMTS' core network elements beyond the radio level, lawful interception network implementations for TD-SCDMA are similar to those for UMTS.

2.2 4G Evolutionary Paths

As was the case with 3G terminology, the use of "4G" to describe later evolutions in commercial wireless technology and architecture remains rather loose. In marketing by carriers and equipment suppliers, 4G often encompasses networks based on HSPA+, various forms of Long Term Evolution (LTE) networking, and WiMAX. However, the strict definition of "4G" is generally recognized as coming from the International Telecommunications Union (ITU)'s *IMTS-Advanced* (IMT-A) systems specifications (much as IMT-2000 paved the way towards defining true 3G network services). It should not be forgotten that important aims of 4G services (and its close precursors) are not only to provide high bandwidth data services to end users, but also to make more efficient use of spectrum to accommodate more users of traditional voice and text messaging in a given service area.

The two dominant networking paths that are typically considered as "4G," whether strictly complying to the above definition or not, are Long Term Evolution (LTE) and WiMAX.

Long Term Evolution (LTE)

LTE represents a series of evolutions proposed by the 3GPP that build from the 3GPP's recommendations on 3G networks. The incumbent operators of wireless networks are advocating LTE for future 4G services. These operators include those who have pursued legacy WCDMA/HSPA/EDGE as well as CDMA2000 paths. This industry constitutes a formidable base with which to produce economies of scale in 4G networking infrastructure and user equipment.

LTE draws from earlier 3GPP technical specification releases, culminating in Release 8, which covers the first formal LTE specification. LTE Release 8 features include:

- High spectral efficiency through the use of an OFDM downlink and DFTS-OFDM uplink between the base stations and user equipment, utilizing bandwidths of 1.4, 3, 5, 10, 15 and 20 MHz. This will support peak data rates of up to 300 Mbs on the downlink and 75 Mbs on the uplink.
- Very low latency.
- Support of variable bandwidths.
- Simplified networking and protocol architecture, where many of the user equipment control functions are moved to the radio base station (now called "eNodeB" in LTE parlance).
- Compatibility with legacy networks, including CDMA2000.
- Efficient multicast and broadcast.
- Support of self organizing network operation.

Despite the advances advocated by LTE Release 8, many of which are currently under deployment in early LTE networks, only those networks conforming to the 3GPP's *LTE-Advanced* specifications will truly conform to the IMTS-A 4G network definition. LTE-Advanced specifications and recommended technical approaches are currently work in progress and to be reflected in 3GPP Release 10 and beyond. Although IMT-A is still under review and subject to change, its overall aim is to provide much higher data rates (100 Mbps and 1 Gbps data rates for high and low mobility, respectively, and in the uplinks and downlinks), backward compatibility with networks based on earlier IMT-compliant networking technologies, support of multiple radio access systems, ubiquitous availability of user equipment, high quality mobile services, and worldwide roaming [5]. LTE-A will also impact both the radio layers as well as the core of the wireless network, and therefore require substantial investment by the carriers, albeit such investments can be incremental over time through incremental network development steps. Section 3 of this White Paper will go into specific details of the network developments.

WiMAX (Worldwide Interoperability for Microwave Access):

WiMAX[1] was born from the success of WiFi,[2] the latter of which has spread the use of low cost IEEE 802.11 wireless local area networking and cross-vendor interoperation. The philosophy has been re-applied by the WiMAX Forum, an industry group formed by companies to promote the WiMAX standards and ensure equipment interoperability. One important aim of WiMAX is to provide ubiquitous broadband access over metropolitan area scale. The technology is based on a series of upgrades to the IEEE 802.16 wireless standard. Originally intended for fixed-position broadband point-to-point network backhaul and point-to-multipoint metropolitan area networking, this standard has been ex-

[1] WiMAX® stands for "Worldwide Interoperability for Microwave Access." The term was created and trademarked by the WiMAX Forum. The WiMAX Forum® is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard.

[2] The term Wi-Fi is a trademark of the Wi-Fi Alliance, a group of industry players advancing the deployment of 802.11 systems and their compatibility.

tended to support ubiquitous fixed access (802.16-2004) and mobility (IEEE 802.16e-2005). To achieve transmission efficiency, WiMAX calls for the use of scalable OFDMA operating within Time Domain Division (TDD) or Frequency Domain Division (FDD) profiles, with channel sizes ranging in size from 3.5 to 10 MHz. Data rates of dozens of Mbps are theoretically possible up 50 km and less for mobile; however, these rates will be subject to environmental, line-of-site, and distance factors. WiMAX data rates up to 1 Gbs are envisioned through the use of MIMO antennas and other enhancements, as covered in the IEEE 802.16m standard. This standard has been proposed for Mobile WiMAX Release 2 and also submitted to the ITU as a possible IMT-A technology.

WiMAX compliant network services are now being deployed in the US under the *Clear* brand, which is offered by Clearwire (a venture of Sprint, Intel, Google, and the cable TV companies Comcast, Time Warner, and Bright House). The service operates over a licensed 2.5 GHz band that had been held by Sprint.

To achieve a competitive jump in capturing the nascent 4G market space while the incumbent wireless operators await their LTE deployments, Clearwire is presently positioning their service as an alternative to wireline and 3G wireless broadband services for mobile as well as home users. The company offers WiMAX-compliant modems and smart phones as part of the service. For mobile users, these modems fall back to Sprint's 3G broadband data service where WiMAX coverage is not present. WiMAX speeds are advertised to be in the range of 3 to 6 Mbs for downlinks and up to 1 Mbs for the uplink. Although impressive compared to the effective speeds of today's common 3G offers, these rates are far from the true 4G specifications.

South Korea also constitutes an early driver of WiMAX, thanks in part to the heavy investment in this technology by Korean telecoms equipment manufactures. Major carriers such as KT and SK Telecom offer WiMAX 802.16e services here. Numerous WiMAX services are found worldwide, often offered by smaller entrepreneurial firms competing against incumbent fixed and wireless carriers.

Considerable controversy in the communications industry persists on the merits of WiMAX vs. LTE. Generally, WiMAX deployments are being driven by entrepreneurial organizations desiring to capture early access to the broadband wireless market. By contrast, LTE deployments are driven by established wireless network operators and the equipment suppliers who have traditionally served them. From the point of view of performance and cost of operation, no definitive preference towards WiMAX or LTE can be reached given the current status of deployments of both services. Both use similar radio technologies and spectrum, which essentially levels the playing ground on the air side of the networks. Issues of interaction or migration from one network type to the other, as driven by market demand, remain to be explored. As mentioned above, the IEEE Mobile WiMAX Release 2 has been submitted to the ITU as a possible IMT-A technology, thereby blurring the lines between WiMAX vs. LTE.

3 Wireless Network Architecture Overview

Before discussing the specifics of how lawful interception is applied to 3G and later networks, it is instructive to review the overall network topologies of 3G UMTS, CDMA2000, WiMAX, and LTE. These technologies have either been deployed by most of the wireless network operators throughout the world, undergoing deployments, or will be deployed in the immediate years to come.

3.1 3.XG Networks

Networks based on UMTS and CDMA are quite similar, particularly within the core networking functions. Figures 3-1 and 3-2 provide generalized descriptions of UMTS and CDMA2000 networks. Both interconnect a group of Base Transceiver Stations (BTS) through a common Base Station Controller (BSC – see terminology definitions following each figure). From the BSC, circuit switched and packet data are sent, respectively, to some form of a Mobile Switching Center and packet manipulation system (Packet Data Serving Node or PSDN for CDMA2000, and Serving GPRS Support Node or SGSN for UMTS). There is also some level of commonality in the signaling and database functions within the two networking technologies. Note each network device shown does not have to represent a separate physical device, and many of the network elements can be combined into a single network device. Slight variations in the network architecture can occur depending on the choice of vendors and desired features.

Upgrades of UMTS networks to accommodate HSDPA and HSDPA+ are performed mainly at the level of the BTS, where earlier generation WCDMA transmitter / receiver subsystems are augmented for HSDPA / HSDPA capabilities. Other than impacting the overall data rates and volumes within the underlying core networking, there is no significant change in the lawful interception architecture or mechanism (discussed in Section 5).

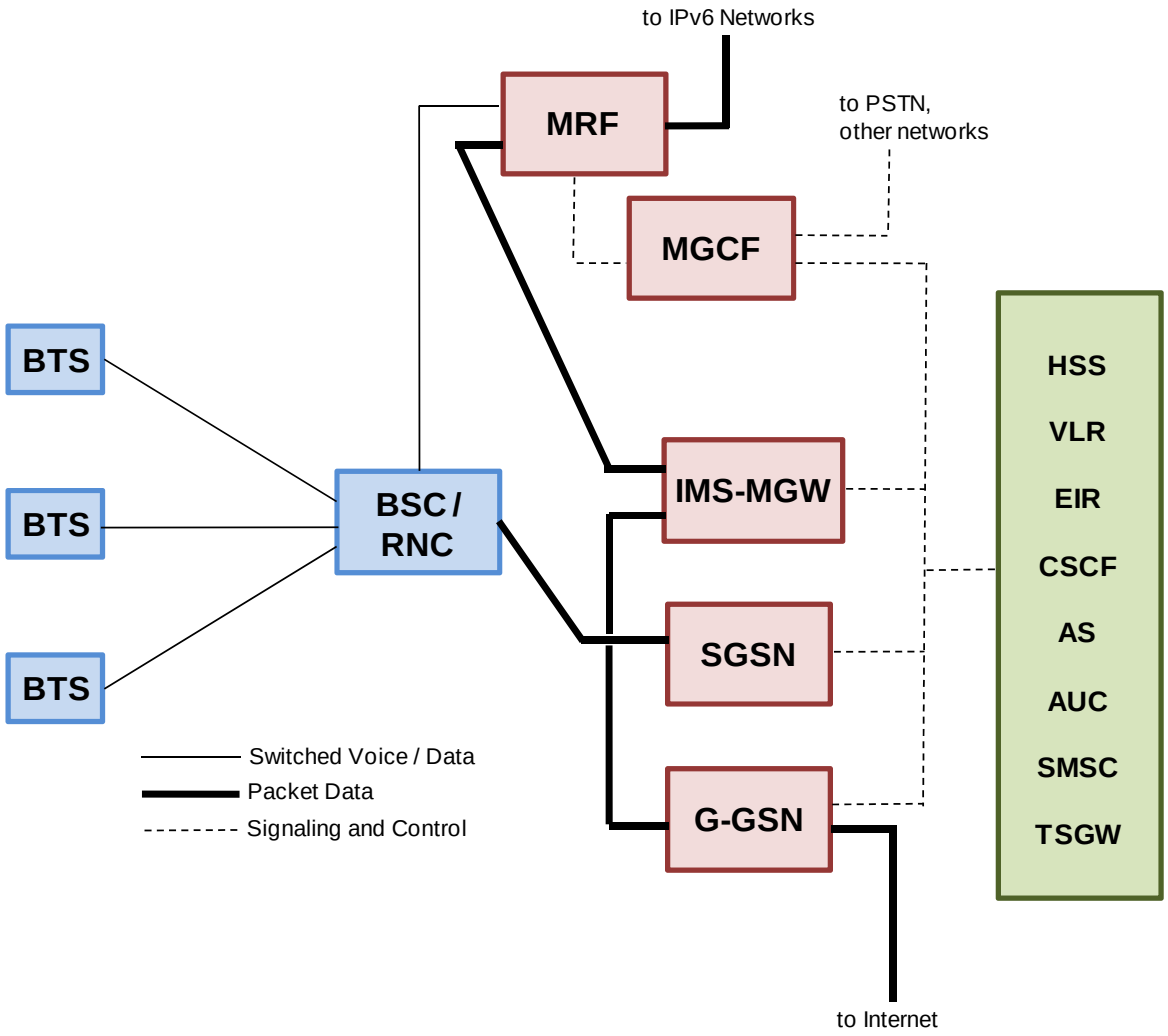


Figure 3-1. Generalized view of a mobile 3G network based on UMTS. This diagram corresponds to Release 5 and later of the UMTS specification. Configuration is nominal and varies by equipment vendors. Some functions may be combined into a single network entity.

UMTS Network Terms [6,7]

BSC (Base Station Controller). Controls and coordinates the function and data flow to/from a group of BTSs that are connected to it.

BTS (Base Transceiver Station). Contains RF and other network elements serving as the air interface between the network and mobile handsets.

GGSN (Gateway GPRS Support Node). Enables packet flow between the SGSN and the outside world, the latter typically the public Internet. This is a relic of GPRS that is also implemented in UMTS.

IMS-MGW (IP Multimedia Subsystem - Media Gateway). Routes switched data from the BSC/RCN, via IP, ATM, or other NGN type networks, to the PSTN and other public or private networks. Used in later revisions to UMTS (e.g., Releases 5 and later).

MGCF (Media Gateway Control Function). Controls the Media Gateway, in part, by interacting with network signaling (e.g., SS7). Used in later revisions to UMTS (e.g., Release 5).

MRF (Media Resource Function). Manages enhanced services and other applications over 3G networks, including voice mail, conferencing, pre-paid calling, messaging, etc.

RNC (Radio Network Controller). Same as BSC. Controls a group of base stations covering a given territory.

SGSN (Serving GPRS Support Node). Core element of GPRS networks and also used in UMTS. Responsible for routing of packets between the BSC/RNC and the GGSN. More specifically, the SGSN handles: a) encryption, decryption, and authentication of packets; b) session management and communication set-up with the mobile subscriber; c) logical link management to the mobile subscriber, d) packet flow and signaling to/from other nodes (HLR, BSC/RCN, GGSN, etc.); and e) tracks charges to subscriber based on services consumed. In some vendor implementations, the SGSN and GGSN can reside on the same equipment chassis.

TGSW (Transport Signaling Gateway). Serves as signaling interface (e.g., SSL) between MGW and PSTN.

Registers, Controllers, Signaling Devices

AS (Application Server). Operates in conjunction with the MRF for executing enhanced calling and data services.

AUC (Authentication Center). Stores user information for authentication purposes to prevent unauthorized use of a subscriber's account.

HSS (Home Subscriber Server). Includes the functions of the Home Location Register (HLR) as well as other functions for managing user mobility and multimedia applications over IP networks.

VLR (Visitor Location Register). When the user moves outside of the home territory of the HLR, the VLR records the presence of the user in a new territory and relays this information back to the user's home HLR. If the user roams into the network of a different carrier, the new network's VLR will record this action.

EIR (Equipment Identity Register). Lists all devices that the network considers valid. If a mobile device is stolen, the EIR would prevent access of this device to the network.

CSCF (Call Session Control Function). Handles call set up and termination, state and event management, billing information, location-based services and other functions according to vendor implementation.

SMSC (SMS Center). System for managing Short Message Service through network signaling.

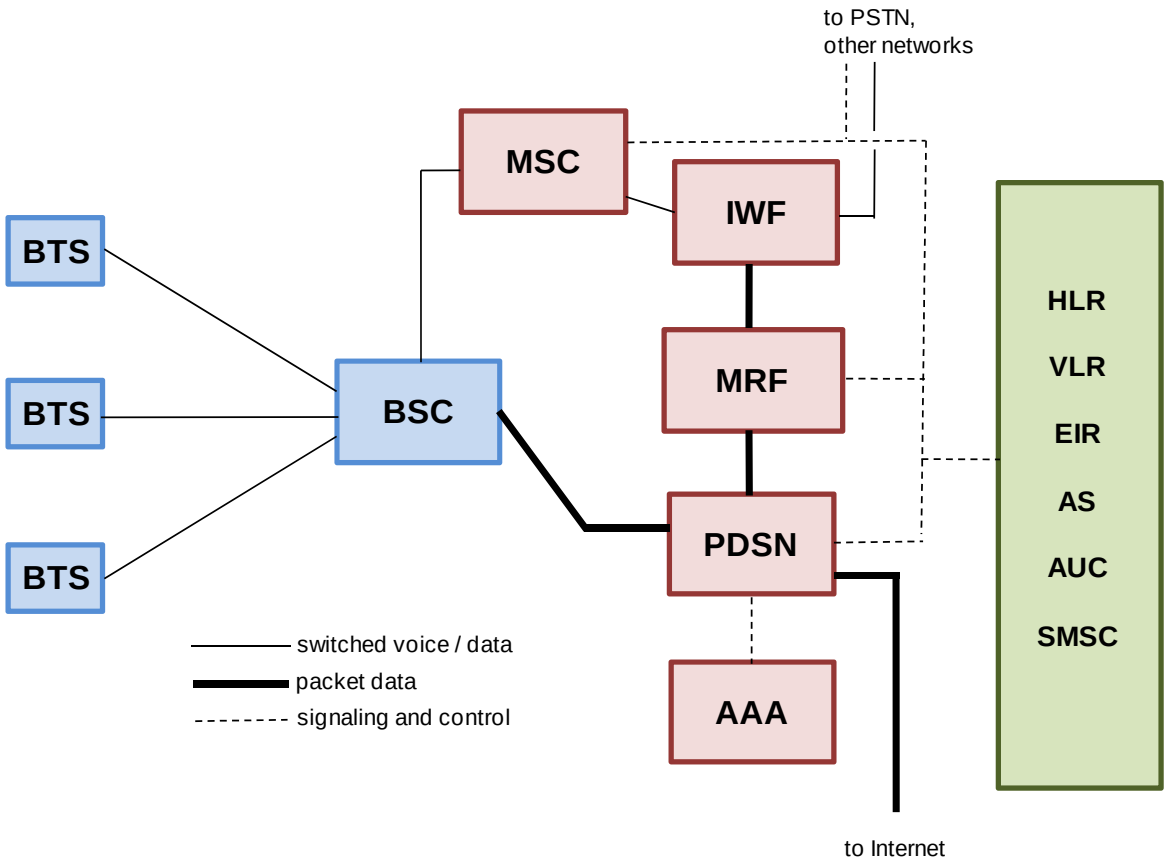


Figure 3-2. General overview of a typical 3G mobile network based on CDMA2000 technology.

CDMA2000 Network Terms

AAA (Authentication, Authorization, and Accounting server). Handles user access to the Internet in typical 3G configurations.

BSC (Base Station Controller). Controls and coordinates the function and data flow to/from a group of BTSs that are connected to it.

BTS (Base Transceiver Station). Contains RF and other network elements serving as the air interface between the network and mobile handsets.

IWF (Inter-working Function). Generally serves as a gateway between circuit-switched CDMA networking and outside public switched networks. Different manufacturers provide different levels of functionality in their IWF systems (e.g., remote access, interface to Internet effectively making the IWF operate as a PDSN).

MRF (Media Resource Function). Manages enhanced services and other applications over 3G networks, including voice mail, conferencing, pre-paid calling, messaging, etc.

MSC (Mobile Switching Center). A switch that provides a connection between the local BSC and the MSC of a remote network. The MSC establishes circuit-switched call between two networks, while accounting for signaling (e.g., from SS7 networks).

PDSN (Packet Data Serving Node). Extracts packets from BSC that are destined for transmission over the Internet, and likewise routes packets from the Internet to the BSC.

Registers, Controllers, Signaling Devices

AS (Application Server). Operates in conjunction with the MRF for executing enhanced calling and data services.

AUC (Authentication Center). Stores user information for authentication purposes to prevent unauthorized use of a subscriber's account.

HLR (Home Location Register). Contains user profile and handles updates to billing based on usage of the subscribed to services.

VLR (Visiting Location Register). When the user moves outside of the home territory of the HLR, the VLR records the presence of the user in a new territory and relays this information back to the user's home HLR. If the user roams into the network of a different carrier, the new network's VLR will record this action.

EIR (Equipment Identity Register). Lists all devices that the network considers valid. If a mobile device is stolen, the EIR would prevent access of this device to the network.

SMSC (SMS Center). System for managing Short Message Service through network signaling.

3.2 4G Type Networks

We now briefly describe the architecture of 4G networks. Note we use the term "4G" rather loosely here to refer to the newer generations of wireless network services based on WiMAX and LTE.

3.2.1 LTE Networks

Long Term Evolution networking attempts to provide a transition path from 3G type networking towards a true LTE-A network with a fully IP (Internet Protocol) core known as the Evolved Packet Core (EPC – earlier known as the System Architecture Evolution or SAE). Figure 3-3 describes the LTE architecture, whose aim is to "flatten" the overall topology to allow for more efficient packet transfer between the User Equipment (UE) and Packet Data Network (PDN – typically the public Internet), while also allowing for the service of legacy wireless networks. In reality, different network operators will be at different states of LTE implementation; therefore, only parts of the network architecture shown in Figure 3-3 may be present in the networks of carriers claiming to run "LTE services."

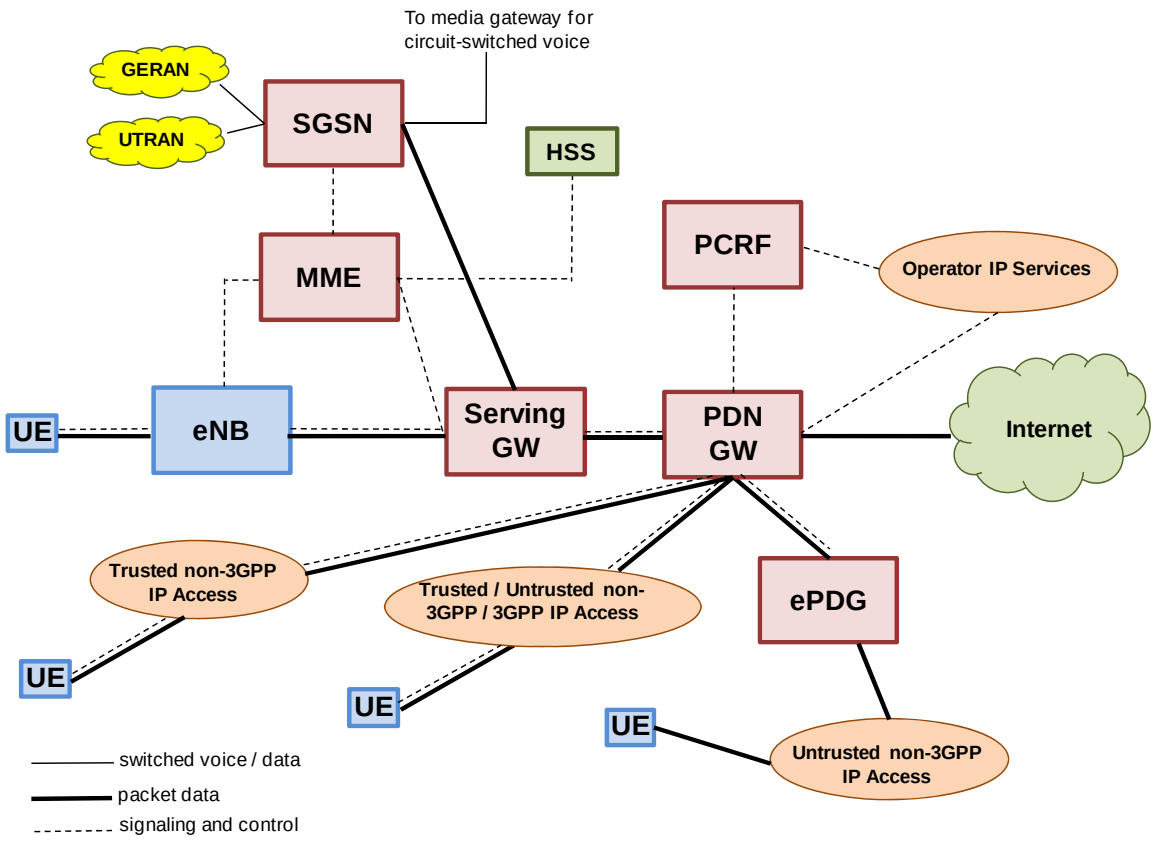


Figure 3-3. General overview of an LTE network.

The Network Elements of Figure 3-3 will now be briefly described:

eNB. This represents the Evolved Radio Access Network, otherwise known as eNodeB. This network element operates the radio interfaces to the User Equipment (UE) through Radio Link Control, Medium Access Control (MAC), data compression, Radio Resource Control, and other functions to access the radio portion of the network. In contrast to 3G, eNodeB is aimed to reflect a simpler aspect of 4G architecture by condensing the BTS and Base Station Controllers of the earlier technology into one network element. In effect, this enables a closer tie-in of the radio side of the network to the underlying packet network.

Serving GW (Serving Gateway). This element routes and forwards user data packets from the eNodeB, as well as from the SGSN of earlier generation parts of the network (namely the GPRS / EDGE Radio Access Network and UMTS Terrestrial Access Network, or GERAN and UTRAN, respectively). The Serving Gateway also supports handovers between multiple eNBs and storage of UE "contexts," which are parameters associated with the user's IP data stream and corresponding User Equipment. More importantly, the Serving Gateway is an important collection point for lawful interception purposes, as will be discussed in Sections 5 and 7.

MME (Mobility Management Entity). This network element tracks when UE attempts to access the network, while maintaining the connectivity of UE devices already within range. Among its many functions, it assigns the Serving Gateway upon network re-attachment of a UE to another eNB within the same LTE network, interacts with the Home Subscriber System (HSS) for user authentication, enforces roaming restrictions, manages ciphering of signaling, etc. The MME also handles signaling with earlier generation networks (through its interface to the SGSN of such networks), while also providing support for lawful interception signaling capture.

PDN GW (Packet Data Network Gateway). This serves as the interface between the UE and one or more packet data networks. The PDN GW performs numerous functions, including packet filtering on a user-by-user basis, policy enforcement, and collection of the Content of Communication for lawful interception.

ePDG (Evolved Packet Data Gateway). The ePDG provides an interface that enables the connectivity of untrusted UE (such as that connected to a WiFi network) between the Evolved Packet Core and non-3GPP network.

Also shown in Figure 3-3 is the **SGSN** (Serving GPRS Support Node), which as described in Section 3.1 handles user connectivity and control for earlier 3GPP networks. In the context of the LTE, updated versions of the SGSN are equipped with an interface to the Evolved Packet Core (through the MME). The **PCRF** (Policy and Changing Rules Function) is a 3GPP-defined network entity that controls network resources (e.g., allocation of subscriber bandwidth, quota management, service tiers), applications, and subscriber interaction in real time.

3.2.2 WiMAX

The overall architecture of WiMAX networks is depicted in Figure 3-4 [8]. This figure conforms to the Network Reference Model established by the WiMAX Forum. The network elements are defined as follows, bearing in mind that some of these functions can be combined into a single piece of equipment:

ASN (Access Service Network). The ASN encompasses network functions required to support radio access to the Mobile Station (MS – which is the User Equipment in the parlance of the 3GPP LTE description in the previous section). These functions include:

- Radio Resource Management.
- WiMAX Layer 2 connectivity with the MS.
- Transfer of Authentication, Authorization, and Accounting (AAA) messages to the subscriber's WiMAX subscriber Home Network Service Provider (SNP).
- Network discovery and selection of the WiMAX subscriber's preferred NSP.
- Relay functionality for establishing Layer 3 connectivity (e.g., IP) between the MS and the network.

The ASN also supports how the communications from the MS to the terrestrial network is tunneled.

The network functions of the ASN are embedded within one or more Base Stations (BS) and the ASN Gateway (ASN GW). The Base Stations are the network elements responsible for the radio access(through the MAC and PHY layers of the IEEE 802.16 standards suite. Connectivity to the underlying IP networks and subscriber services management are handled via the ASN Gateway (ASN GW), as indicated in Figure 3-4.

CSN (Connectivity Service Network). This represents a set of network functions that provide IP network connectivity to the subscribers using the WiMAX services. It contains routers, AAA proxy servers, subscriber databases, and interconnections to other WiMAX service networks. Specific functions within this block include:

- MS IP address endpoint allocation.
- Internet access.
- AAA proxy or server.
- Policy and Admission Control according to user profiles.
- ASN-CSN tunneling support.
- WiMAX subscriber billing and inter-operator settlement.
- Inter-CSN tunneling for subscriber roaming.

- Inter-ASN mobility.
- WiMAX services for location based services, peer-to-peer services, authorization and / or connectivity to IP multimedia services.

It is at the CSN that lawful interception collection takes places, as will be discussed in detail in Sections 5 and 7. As indicated in Figure 3-4, multiple CSNs may interconnect to the ASN Gateway of a common radio infrastructure. Likewise, multiple ASNs can serve a given MS. While these features of WiMAX allow for flexibility in the services offered to the subscriber, they can also make lawful interception more challenging.

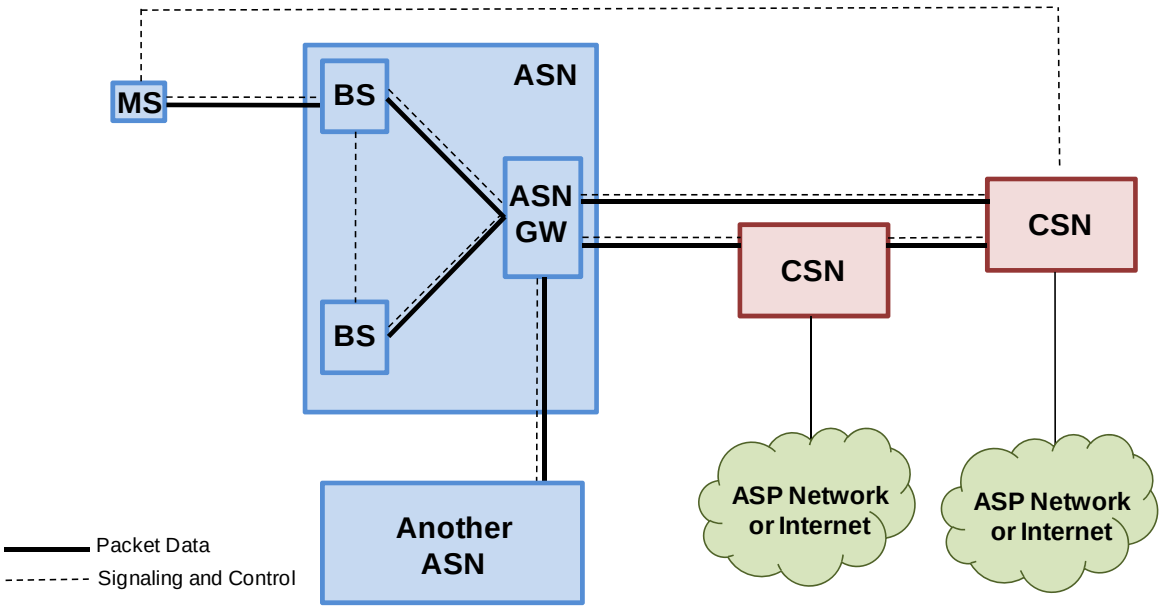


Figure 3-4. General architecture of a WiMAX network (from [8]).

4 The Architecture of Lawful Interception

Figure 4-1 depicts a generalized view of the lawful interception process, which typically calls for the use of a mediation platform to handle the provisioning of the interceptions as well as the collection and delivery of intercepted traffic from various forms of communications services provided by a wireless carrier. Here the use of mediation is critical for assuring legally and standards-compliant interception capabilities as wireless carriers add capacity, add features, and transition their networks through the numerous evolutions described in Sections 2 and 3. Of note is the separation of Law Enforcement Agency (LEA) functions from the interception functions performed by the network operator. This is indicated in Figure 4-1 by the demarcation line between the Network and Services Operator Domain and the Law Enforcement Domain. The cloud to the left of Figure 4-1 represents a conceptual network that contains one or more Network Elements (NE) that perform a function in the lawful interception processes, such as in the collection of intercepted traffic from switches, routers, or network probes (explained further below).

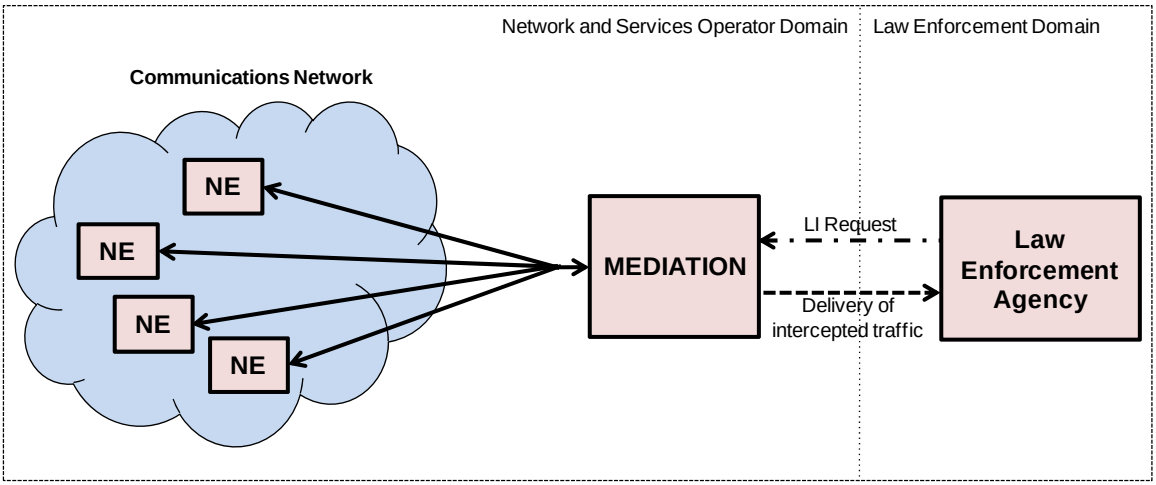


Figure 4-1. Simplified view of lawful interception architecture. Of primary interest is the use of a Mediation Platform to convey intercepted data from the network to the LEA in a standards-compliant manner.

The Reference Architecture for lawful interception, as proposed by European Telecommunications Standards Institute (ETSI), is shown in Figure 4-2 [9]. This architecture attempts to define a systematic and extensible means by which network operators and LEAs interact, especially as networks grow in sophistication and scope of services. The architecture is widely applied worldwide, albeit with slight variations in terminology for different parts of the world. The architecture is also general in that it applies to both legacy voice services (wireless or wireline) as well as interception of packet data networks. Of particular note is the separation of lawful interception management functions (mainly interception order set-up and tear down, as demanded from the LEA), delivery of intercepted call data from the network operator to the LEA, and conveyance of call content, also from the network operator to the LEA.

Communications between the network operator and LEA are via the Handover Interfaces (designated **HI**). **Handover Interface 1** (**HI1**) supports the provisioning of the interception order via the **Administration Function**. **Handover Interface 2** (**HI2**) supports the delivery of **Intercept Related Information** (**IRI;** e.g., destination of call, source of a call, time of the call, duration, etc.) from the network to the LEA. **Handover Interface 3** (**HI3**) supports the delivery of the **Content of Communications** (**CC**) from the network to the LEA. Also of importance are the "**Collection Functions**," which gather the intercepted data from various switches and probes in the network, and the "**Mediation Functions**," which format the collected IRI and CC data into standardized data representations. The mediation functions for IRI and CC are also responsible for delivering their products to one or more LEAs.

The Collection Functions operate in two manners: as an **External Interception Function** (**EIF**) and as an **Internal Interception Function** (**IIF**). The Internal Interception Function collects intercepted traffic from within network elements that have such capabilities. For example, voice switches, gateways, and routers are often supplied with built-in lawful interception capabilities that collect and replicate targeted subscriber traffic. These capabilities may or may not be useful, depending on the implementation of such equipment in the service provider's network. The External Interception Function makes use of probes that are attached to points in the network that provide the requisite visibility to the types of traffic being collected for interception purposes. These collection points will be discussed in Section 5. EIFs are used when the network elements do not support IIFs or the network entity IIFs are inadequate.

Also indicated in Figure 4-2 is the **Handover Interface HI-a**, which is not a formal part of the ETSI architecture but included here to represent the feedback of an Operations and Maintenance function to the LEA. This interface supports, for example, the conveyance of alarms indicating failure of an interception process.

In the context of Figure 4-2, Aqsacom addresses the function of Collection by providing probes for EIF or support for the IIF capabilities of networking equipment from major vendors. Likewise, Aqsacom plays a major role in providing Mediation capabilities to the network operators, as will be described in Section 6.

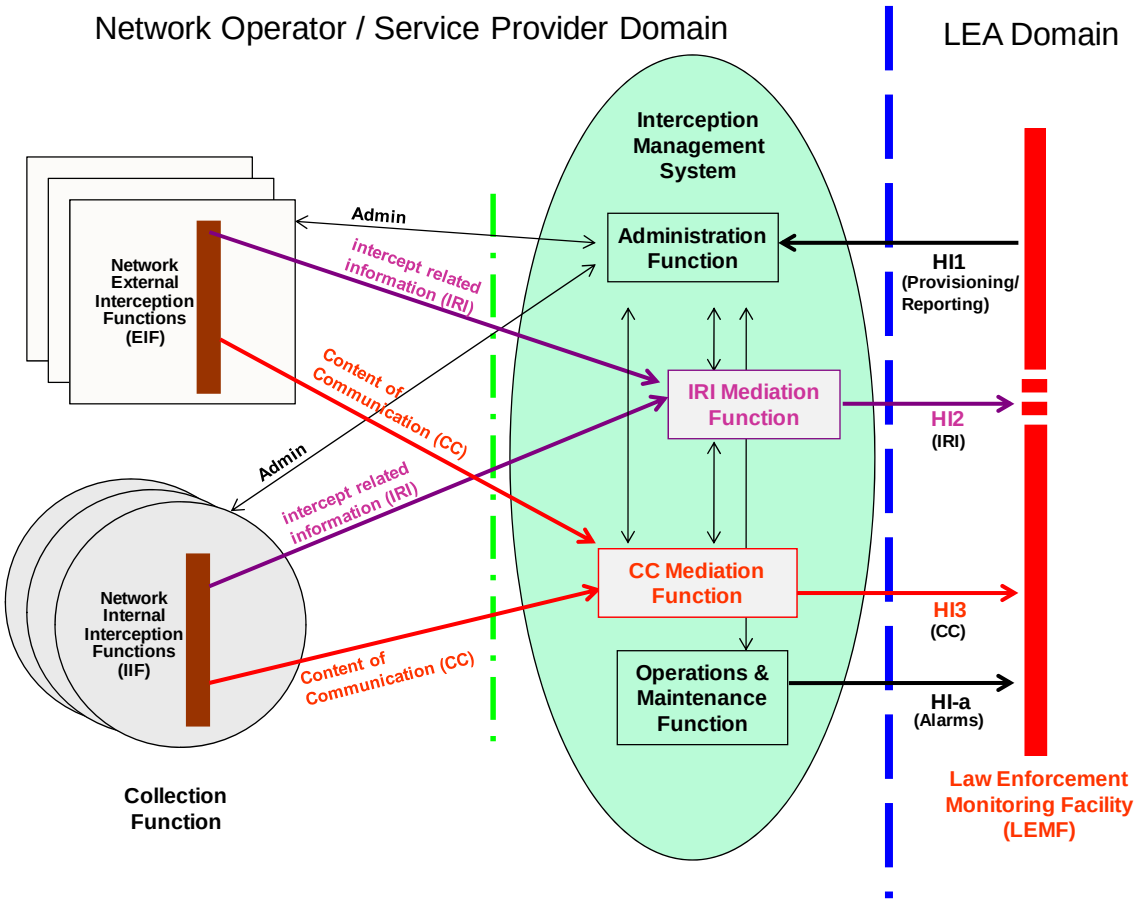


Figure 4-2. ETSI-defined Reference Architecture for lawful interception. Note the separation of lawful interception management functions (HI1), call-related data (HI2), and call content (HI3) in the interaction between the LEA and communication service provider (based on [9]).

5 Lawful Interception Configurations for 3G and 4G Networks

5.1 3G Network Interception

Given the general background discussion that has been provided thus far on the wireless network and lawful interception (LI) technologies, we describe the reference architectures for LI as these architectures relate to the specific types of wireless networking.

3G CDMA and UMTS are generally very similar in their lawful interception implementations, albeit slight differences do occur. For example, UMTS target identifiers apply the Subscriber Identify Module (or SIM card) ID of the target's mobile device, whereas CDMA phones often do not use these cards. Figure 5-1 depicts the Reference Model for the interception of 3G networks; in this case the model pertains to the interception of circuit-switched networks. This depiction (based on that published by 3GPP) is sufficiently general to include both UMTS and CDMA2000. In summary, it shows that:

- LI management commands are conveyed between the Administrative Function (ADMF) and other network elements via the X1 interface,
- Intercepted Intercept Related Information (IRI) is conveyed via the X2 interface, and
- Intercepted Content of Communications (CC) is gathered via the X3 interface.

The MSC Server, GMSC Server, MGW, and IWF functions shown in Figure 5-1 were described in Section 3; in the context of the interception model their corresponding boxes represent interception processes which can rely on Internal Interception Functions or External Interception Functions (probes), as described in Section 4. The diagram also mentions the Gateway Mobile Switching Center Server (GMSC Server), which interconnects the MSC to the networking of other wireless operators.

Note X3 can convey both bulk content (bearer) and signaling information, which are ultimately conveyed to the LEA via Handover HI3. The shaded boxes represent functions performed by Aqsacom's core product, the *ALIS Mediation Platform* (discussed further in Sections 6 and 7).

A similar diagram pertaining to packet data services is provided in Figure 5-2. The models of Figures 5-1 and 5-2 apply a Mediation Function to separate the LEA from the data gathering functions within the network. This separation is the core contribution of the ETSI Reference Architecture and the LI standards based on it (Figure 4-2). It is this separation that enables LEAs and network operators to configure interception systems in a generalized manner, covering a wide range of services and technologies, including wireline voice, wireless voice, wired and wireless data, and emerging services such as VOIP.

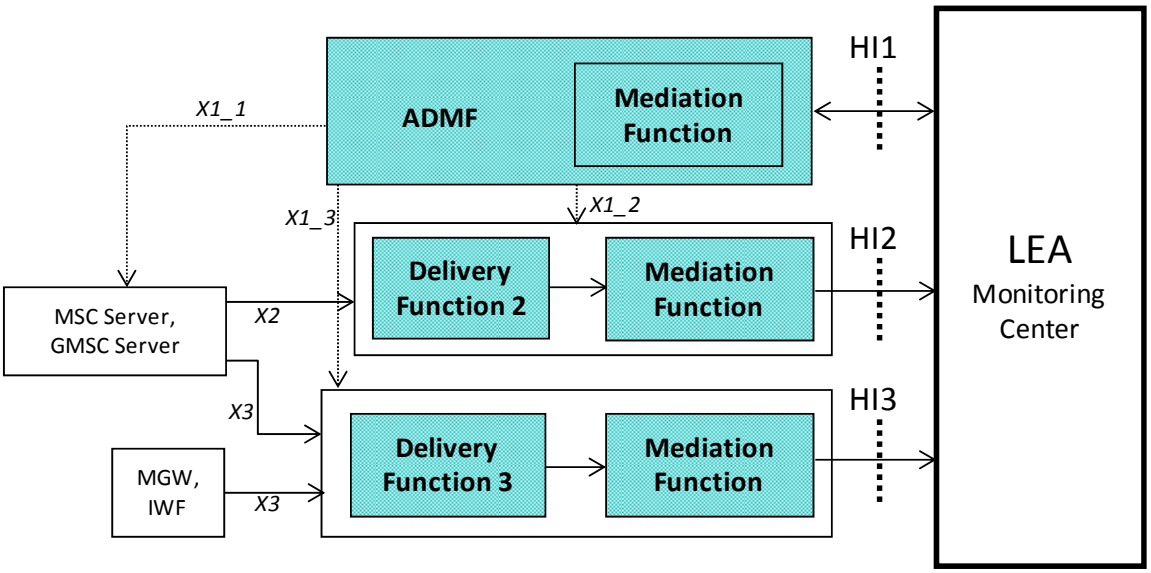


Figure 5-1. Interception model for circuit-switched services within a 3G mobile network (generalized for CDMA2000 and UMTS) (based on [10]). Functions in shaded boxes are implemented in the Aqsacom ALIS mediation platform (described in Sections 6 and 7).

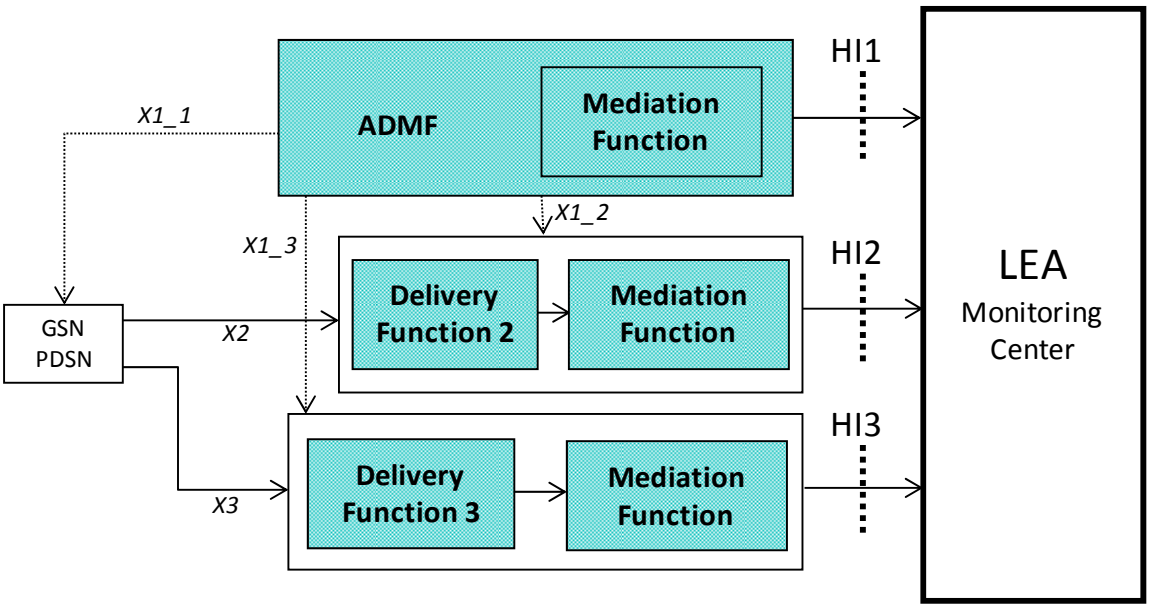


Figure 5-2. Interception model for packet data services (including IP) within a 3G mobile network (generalized for CDMA2000 and UMTS) (based on [10]). Functions in the shaded boxes are implemented in the Aqsacom mediation platform (described in Sections 6 and 7).

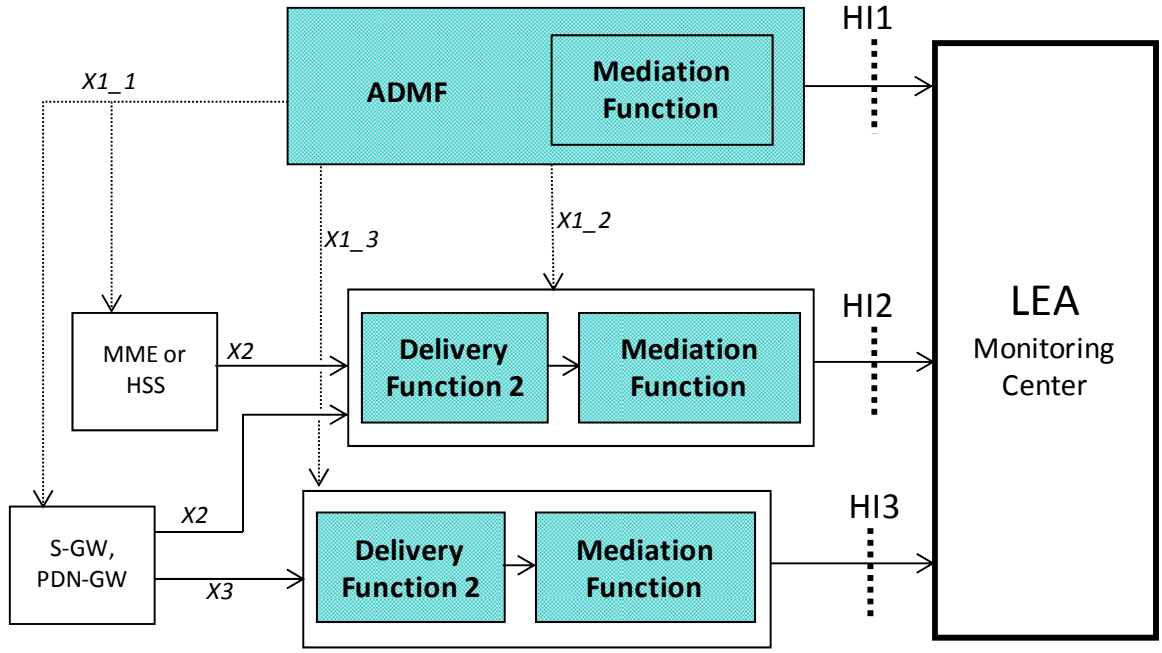
5.2 LTE Network Interception

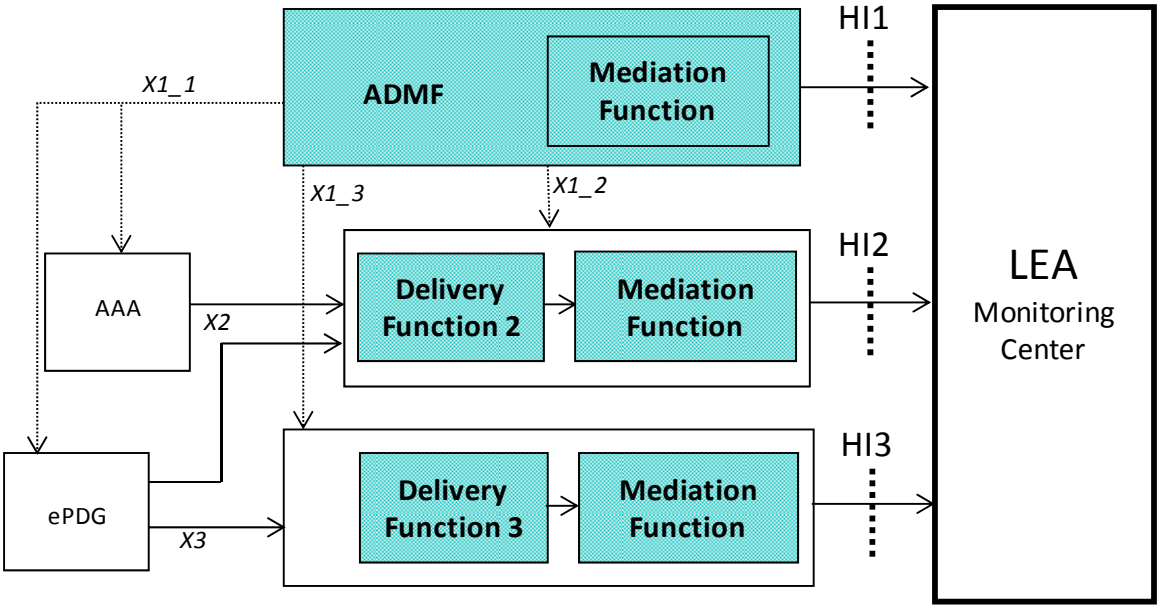
As mentioned in Section 3, "LTE" networks are more typically 3G UMTS or even CDMA2000 networks with added elements to increase radio transmission bandwidth and / or to support evolution towards the Evolved Packet Core (EPC). Therefore, the interception of typical LTE networks nowadays follows that described for 3G networks above. For LTE networks that support EPC elements, Figures 5-3a and 5-3b describe the interception model. Noteworthy in this model is the central role of the Mobility Management Entity (MME) in collecting IRI from the data streams to and from the eNode of home and visiting subscribers. Likewise, the Home Subscriber Server (HSS) provides mapping information between subscriber-related network events (e.g., logging in / out from the network), subscriber identity, and subscriber mobility for IRI.

CC is obtained through the Serving Gateway (S-GW) and / or PDN Gateway (PDN-GW) elements. When these elements apply an Internal Interception Function, they duplicate the targeted packets and route them to the Mediation Function. Alternatively, an External Interception Function through a probing system can be deployed for the CC collection. In this case the probe must monitor the packets to and from the S-GW or PDN-GW, then duplicate the targeted packets and deliver the copies to the Mediation Function.

Also shown are the interfaces to the Evolved Packet Data Gateway (ePDG) and AAA services, which would be applied for the interception of traffic from non-3GPP sources (e.g., WiFi). AAA information is typically needed to obtain the mapping between a subscriber's identity and the allocated IP address of their packets. Traffic can be collected from

AAA and ePDG devices via Internal Interception Functions (when available) or probes – the latter likely to become more common practice.





Figures 5-3. (**5-3a** – *top*): Interception model for LTE networks. (**5-3b**- *bottom*): Interception model for the support of non-3GPP subscribers (both figures based on [11]). Functions in the shaded boxes are implemented in the Aqsacom ALIS mediation platform (see Sections 6 and 7).

5.3 WiMAX Network Interception

Figure 5-4 provides the lawful interception Reference Model for WiMAX. Overall, it resembles the models for the other wireless network interception models discussed above, except that the WiMAX Forum introduced the notion of "Internet Access Points (IAPs)" to serve as the interface between the network elements and the interception functions. The IAPs may take the form of Internal Interception Functions, such as those built into the ASN-GW and routers within the network, or External Interception Functions, which are implemented using probes. Of importance are the roles of Authentication, Authorization, and Accounting (AAA) and Home Agent (HA) elements in the interception processes. AAA information from the CSN, usually extracted by a probe (supplied by Aqsacom), contains essential IP-to-subscriber mapping information. The Home Agent, which is contained within the CSN (see Figure 5-4), is used to establish a "home base" for the subscriber such that when the subscriber roams, packet flow that otherwise would connect to the subscriber's home ASN is tunneled by the HA to the ASN in which the subscriber is visiting. Thus, the HA provides important roaming information about the subscriber as well as capture of packets that are routed to / from a foreign ASN that the subscriber is visiting.

WiMAX interception calls for the use of a Charging User Identifier (CUI), which serves as an alias of the target. The CUI prevents disclosure of the target's identification as network elements within the home or visiting network are instructed, by way of the CUI, to carry out interceptions of the target's traffic. The mapping of the CUI and target identity is performed by the AAA entity, and disclosed to the LEA who subsequently uses the CUI in the LI requests. When intercepting a roaming subscriber, interception takes place in the visited network in a manner similar to interception in the subscriber's home network.

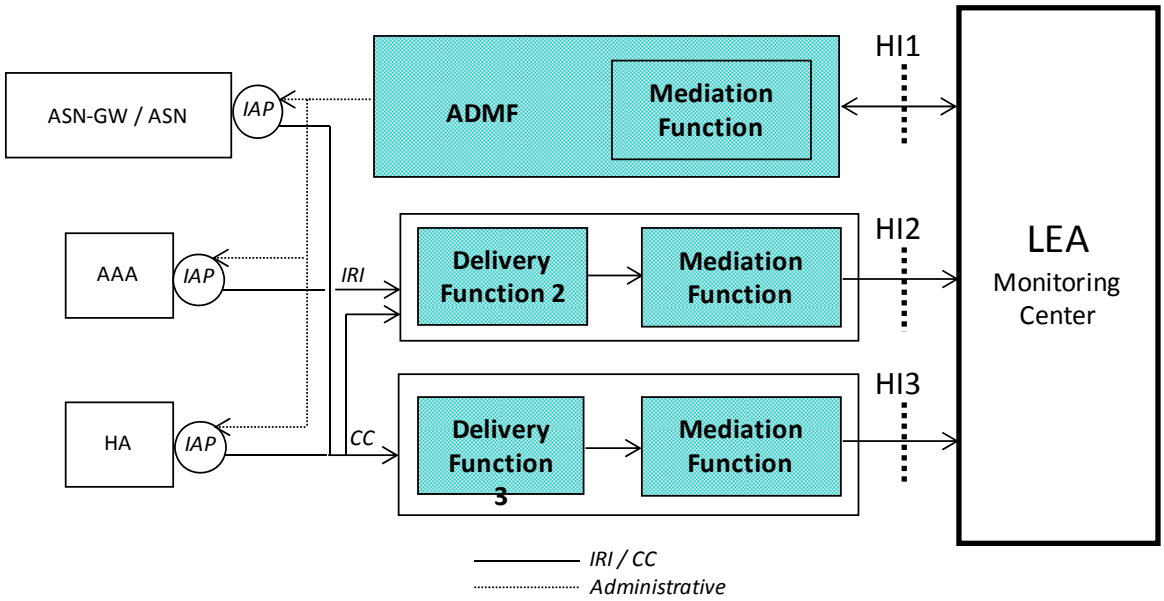


Figure 5-4. Network Reference Model for the interception of WiMAX networks (adapted from [12]).

5.4 Location-Dependent Interception Issues

The issue of location of the interception target may come into play for two reasons:

1) To track the location of the target in real time as he / she moves about.

Here the use of location information for LI remains rather vague in that no formal standards have been introduced to formally track the movement of a target for lawful interception purposes, despite how useful as this information may appear. This situation has arisen, in part, because of the vagueness of laws in many jurisdictions concerning the application of mobile phone data for surveillance. Location-dependent interception can also be hampered because the required accuracy, typically to within the range of the nearest base station, may not be adequate to pinpoint the location of the target. Technical means are generally available to enhance the accuracy of position determination to 50 m or so; systems that perform such positioning rely on Global Positioning Satellite (GPS), triangulation methods that apply multiple towers, statistical methods that track the motion of the target, or any combination of these. Nevertheless, formal LI procedures incorporating these positioning technologies have yet to be ratified by standards bodies.

2) To restrict lawful interception only to geographical territories that authorize or allow it.

Legal complications can arise when the target crosses boundaries controlled by different LEAs, not all of which have authorized the interception or have the same interception policies. Consider the case where a given Base Station Controller, eNode, or equivalent wireless network entity may cover many different Interception Areas (IAs). When a moving target's communications must be intercepted, a check must therefore be made to ensure that the corresponding LEA initiating the interception can in fact receive intercepted information from the IA where the target is located at a given point in time. Checks for valid IAs, when such checks are called for, need to be performed by the LI delivery functions and other network elements such as the MSC, GMSC, CSCF, and IWF.

There is also the notion of geographic vs. identity-driven interception. The first is when all subjects at a given location become targets of an LI procedure. This can be useful when tracking the presence of targets in sparsely populated zones. Identity-driven LI is the more common form of LI where targets are identified by specific identity information (e.g., the SIM card's International Mobile Subscriber Identity or IMSI; the handset's International Mobile Equipment Identity or IMEI). In both cases, novel target detection methods must be employed to include the notion of location in the surveillance.

6 Aqsacom's ALIS Mediation Platform

The Aqsacom real time Lawful Interception System, known as ALIS, reflects Aqsacom's ongoing philosophy of meeting the challenges of lawful interception in a highly systematic, low cost manner over networks supporting a diversity of services. The platform makes the deployment of lawful interception systems easier for the communications operator, while simplifying the processes of data collection and analysis for the law enforcement agency (LEA). It also addresses the growing lawful interception needs and requirements of newly emerging services, including those based on wireless 3G, 4G, broadband IP, satellite, voice-over-IP, and other technologies.

The system's client/server "multilayered" architecture comprises two functional elements: ALIS-M for target interception provisioning, and ALIS-D for the mediation and delivery of interception content (see Figure 6-1). The processes of Mediation, Delivery, and Provisioning are represented by each layer of the architecture. The vertical bidirectional arrows represent "technology connectors" that provide the interfaces to network elements and probes for the interception provisioning and traffic collection. ALIS-D carries out delivery of the intercepted traffic to the LEA, after national-compliant interception data formatting. Provisioning of the interceptions is by the LEA or via a court-mandated procedure. Both ALIS-M and ALIS-D may reside on the same computing and data collection platform, or they may reside on separate platforms. If necessary, ALIS-D platforms may be distributed throughout networks depending on the services, geography, and anticipated surveillance load to be supported.

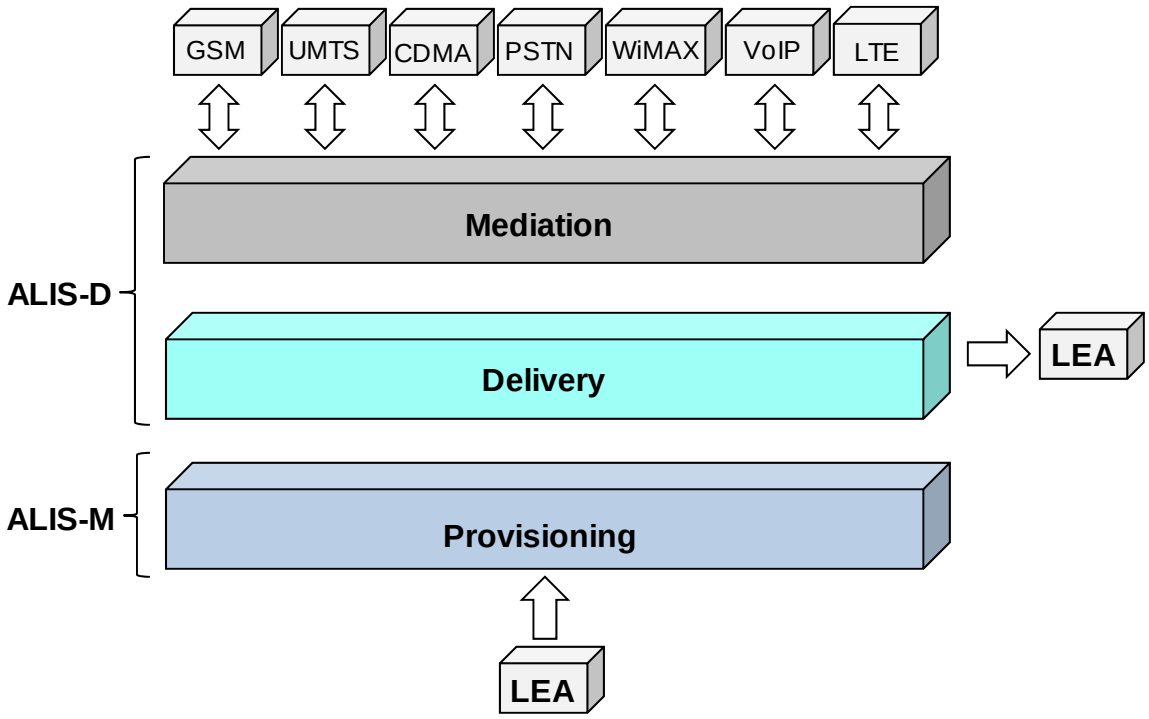


Figure 6-1. Architecture of the Aqsacom ALIS platform.

Features and functions of ALIS include:

Provisioning

ALIS-M is responsible for provisioning a lawful interception session. Provisioning falls under the ADMF (Administrative Management Function), discussed in Figures 5-1 through 5-4 above. Specific tasks of provisioning include start, stop, query and modification of lawful interception operations, audit, consistency checking, etc. These tasks are generally invoked by the LEA, and securely communicated to ALIS, which typically resides within the network operator's premises. ALIS' user-friendly graphical interface allows for the easy automation of many operational interception tasks, such as the automatic triggering or stopping of an interception operation at predefined dates and times.

Multi-administration

More than one LEA can independently manage surveillance sessions over one ALIS platform, even when tracking the same target. All data flows are secure to ensure that no interception data are leaked between LEAs.

Mediation and Delivery Management

Mediation is carried out by the ALIS-D platform, which gathers data from diverse intercept points within the network, formats the data, and delivers the information to the LEA over a secure network (typically a VPN, secure FTP, and ISDN). As discussed in Section 4, intercept data takes the form of Call Data (otherwise known as Intercept Related Information) and Content of Communication (Call Content). Both types of data are delivered via separate channels. The data are also formatted by ALIS-D to conform to national standards such as CALEA. To ensure reliable real time delivery of interception information to the LEA, ALIS implements adequate buffering to account for nominal transmission outages or other unforeseen interruptions between the network operator and LEA.

Secure Access

Clearly ALIS, as any lawful interception system, must have highly controlled and secure access allowing for operation only by cleared personnel. Aqsacom takes this point very seriously, and has incorporated a number of safeguard technologies to assure secure access. These technologies include smart tokens and biometrics.

Billing

ALIS can be adapted to provide a variety of billing plans where the network operator invoices the LEA. These plans include billing on a per-LI session basis, per LI change basis, flat rate, per special service, and other plans. Likewise, billing can be configured to facilitate the operation of a LI service bureau, where several network operators share a common LI infrastructure. This configuration is attractive to those operators that are too small to invest in LI equipment and who claim that the frequency of LI requests from LEAs is not sufficient to justify the investment. In this case, billing can be addressed to the subscribing network operator, or one of many LEAs ordering the interception request.

Alarms, Statistics, Logging

ALIS provides a wide array of alarms (e.g., notification when a session is interrupted), statistics (number of active interceptions in a given interval in time, utilization of LI system resources), and logs for tracking of past LI events.

Hardware / Operating System

ALIS makes use of off-the-shelf industrial strength PC hardware. This allows for easy parts replacement and reduced cost. All software runs under the Windows, Solaris, and Linux operating systems.

7 ALIS Implementation in 3G / 4G Networks

Figure 7-1 depicts the implementation of ALIS as a mediation platform in a UMTS network. The network's interception configuration follows the Interception Reference Models described in Section 5. Of note are the call data (IRI), call content (CC), and LI management paths leading between ALIS-D and ALIS-M and the appropriate network elements and functions. For simplicity, the diagram does not distinguish between the use of probes and Internal Interception Functions of the network elements, the availability of which vary by vendor and implementation. Furthermore, not all of the connections between the ALIS platforms and the network elements need to occur – this diagram is mainly intended to illustrate the possible connections. Note that the Law Enforcement Agency (LEA) receives the formatted IRI and CC interception products from ALIS-D via a VPN, ISDN link, or dedicated line (none of which are shown). The LEA's Law Enforcement Monitoring Facility (LEMF) should follow LI standards to allow acceptance of the CC and IRI data through FTP, ROSE, or TCP/IP-based protocols.

Provisioning of the interceptions typically start as a court order that presents the interception order to the Network Operator, who then manually enters the interception parameters into the ALIS-M Graphical User Interface (GUI). In some countries, the LEA is permitted to remotely enter the interception order directly into ALIS-M, although this is not standard practice for lawful interception.

Figure 7-2 provides a similar diagram for CDMA2000, where the LI network configuration is quite similar. As in Figure 7-1, we depict a number of different possibilities for collecting the intercepted traffic and sending this traffic to ALIS-D.

Figure 7-3 illustrates the use of ALIS in the interception of LTE "4G" networks. Given that LTE networks can constitute a mix of legacy 2G, 3G, and 4G network architectures and technologies, it is somewhat difficult to pinpoint a single, representative interception scheme for LTE networks. Nevertheless, the diagram of Figure 7-3 makes such an attempt. Following the Interception Reference Architectures of Section 5, the Serving GW and / or PDN-GW operate as interception traffic collection points for IRI and CC collection (assuming the use of their Internal Interception Functions, when available). IRI and

CC from legacy subscriber services can be collected from the Evolved Packet Data Gateway (ePDG). Also indicated is the collection of IRI data, or data that can support the assembly of IRI data, from the Home Subscriber Server (HSS). Interceptions can also be conducted at the level of the SGSN when a 2G / 3G network is supported. This would follow the schema described for 3G UMTS or CDMA networks described in Figures 7-1 and 7-2. Alternatively, interception for these legacy networks could be conducted via the Serving GW. The operations with the LEA are as described for Figure 7-1.

Figure 7-4 describes how the ALIS platforms can support the interception of WiMAX networks. CC is typically collected from the Access Service Network Gateway (ASN-GW) via a probe or from an Internal Interception Function if supported by these gateways. CC may also be collected by the Home Agent, or by probes connected to the networking supporting the HA. The AAA resources within the CSNs also provide important information in the assembly of the IRI (e.g., subscriber log-in / log-out and IP address mappings to the subscriber). The interception of AAA packets is typically performed with a probe, such as that supplied by Aqsacom. The operations with the LEA are as described in Figure 7-1.

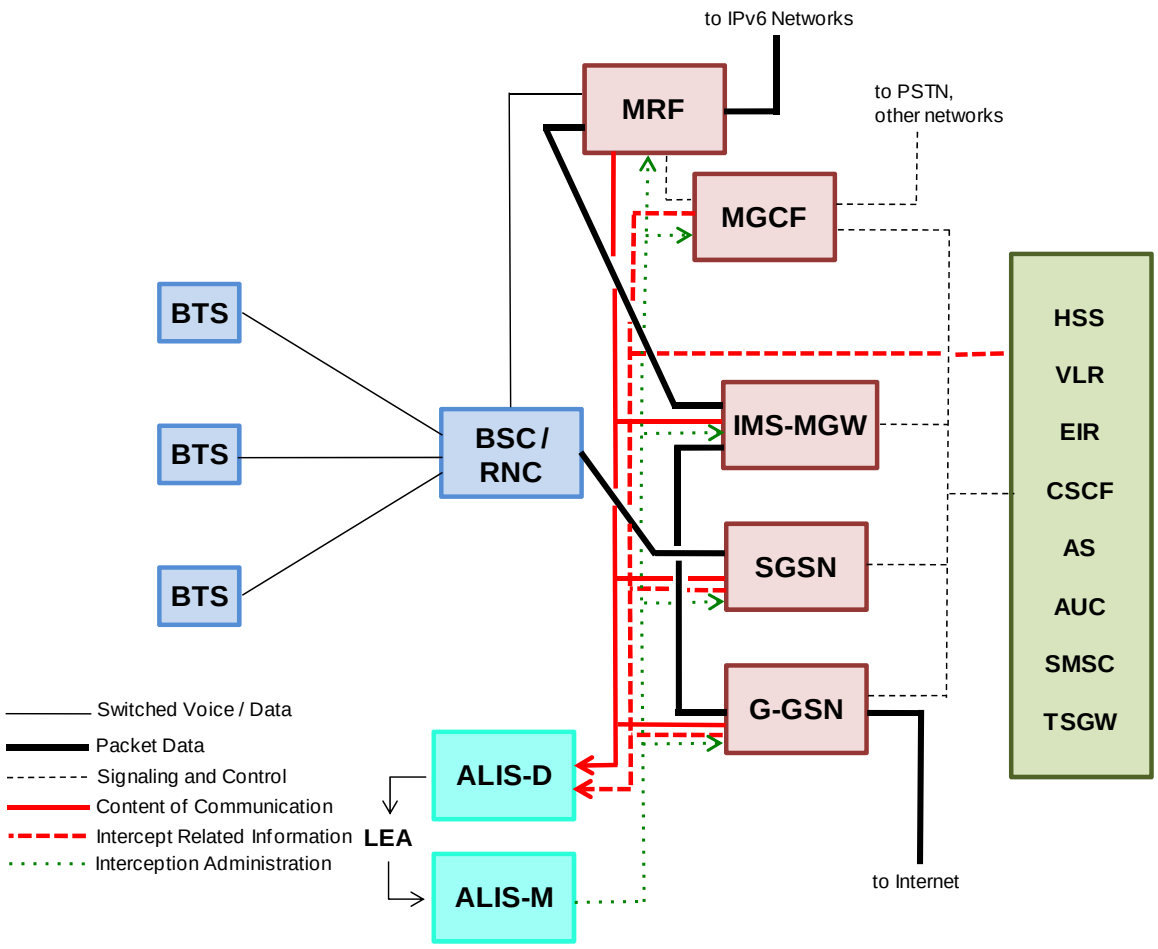


Figure 7-1. Role of the Aqsacom ALIS mediation system in the interception of UMTS 3G mobile networks (Release 5 and later).

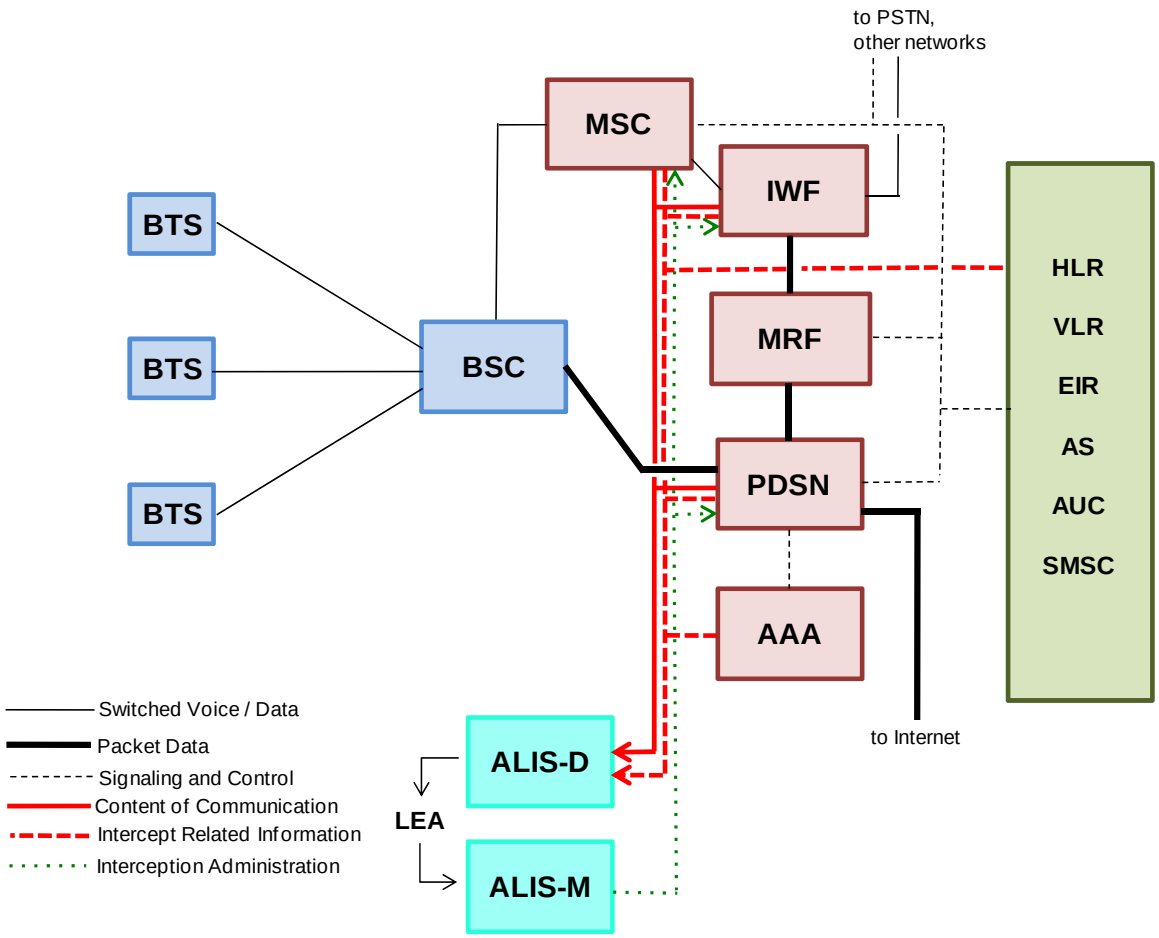


Figure 7-2. Role of the Aqsacom ALIS mediation system in the interception of CDMA 3G mobile networks.

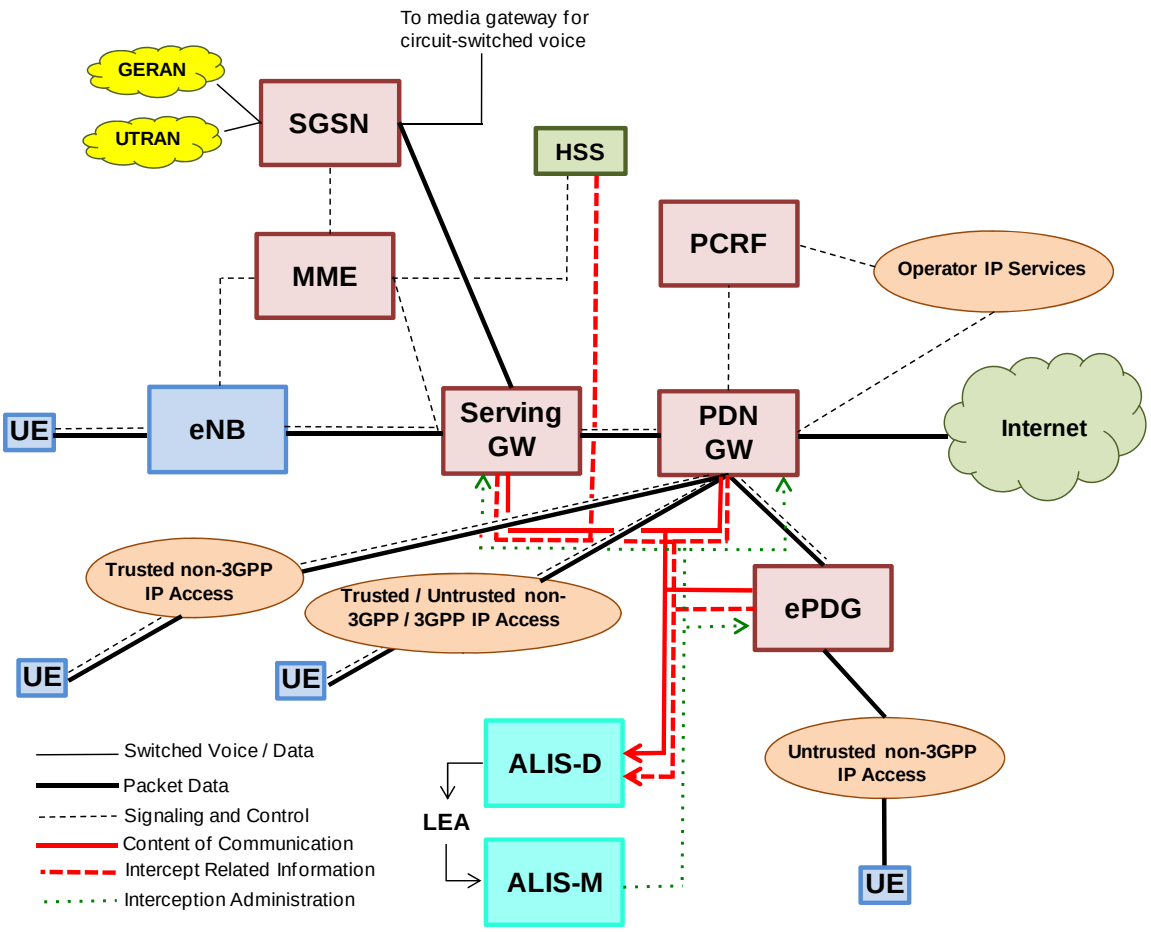


Figure 7-3. Role of Aqsacom ALIS mediation system in the interception of mobile networks based on LTE architectures containing the Evolved Packet Core (EPC) and legacy wireless networks.

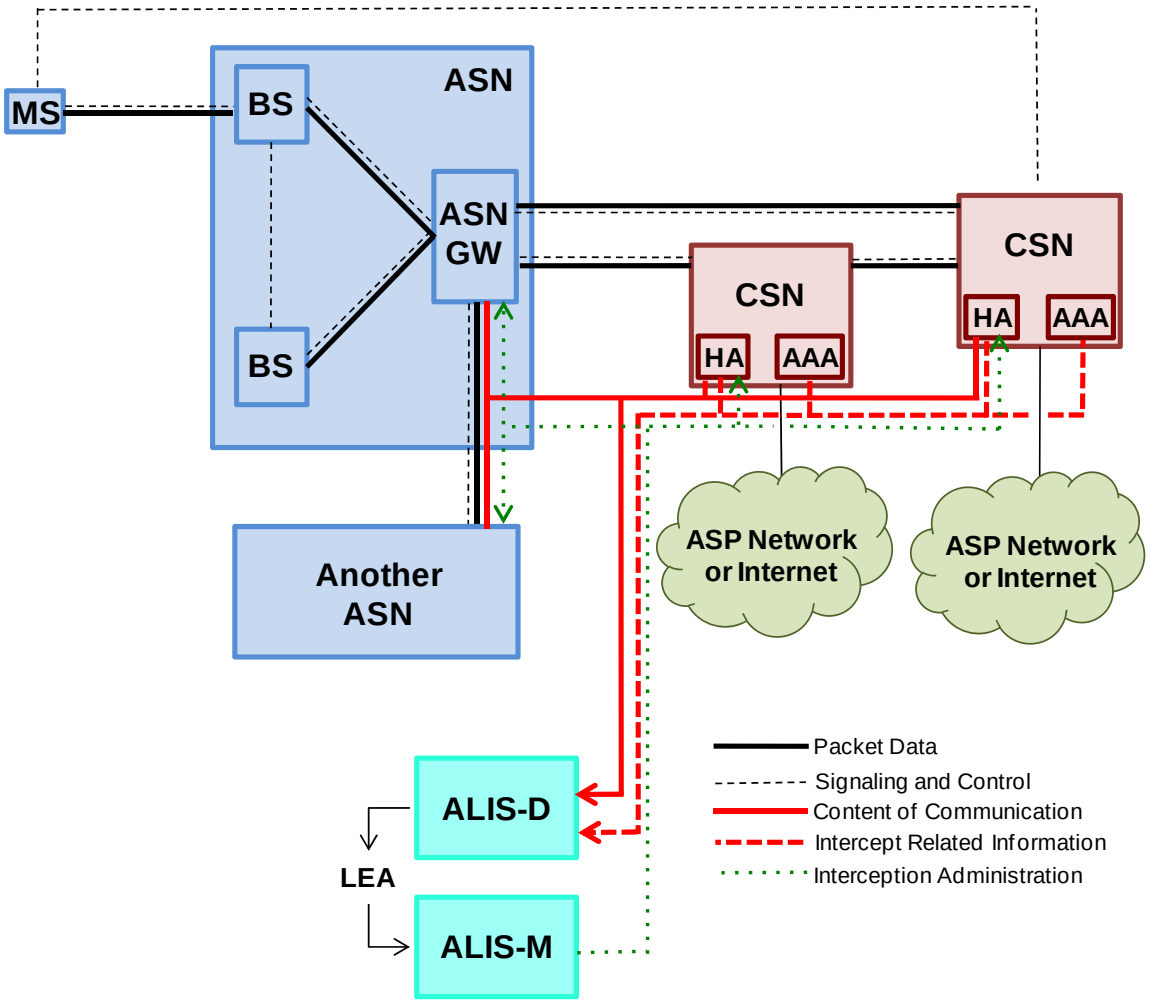


Figure 7-4. Role of Aqsacom ALIS mediation system in the interception of WiMAX mobile networks.

8 Summary

This White Paper has presented an overview of 3G and 4G mobile services and methods supporting the lawful interception of targets subscribing to these services. The LI processes are delineated by architectures, such as those specified by ETSI, 3GPP, the WiMAX Forum, and other standards bodies, that facilitate systematic implementations and provisioning of lawful interception systems. However, challenges to lawful interception remain, including the need to support a diversity of services, vendor technologies, wireless networking technologies, voice, and a multiplicty of high speed speed data services.

Aqsacom's ALIS mediation platform offers a comprehensive solution to the above challenges, while conforming to emerging mainstream networking architectures and lawful interception regulations worldwide:

No Network Modifications

Designed for seamless integration and interoperation with existing mobile networks, ALIS interoperates with switching and networking equipment from most major vendors. This equipment vendor independence ensures that no network modifications are needed to support cumbersome vendor-dependent lawful interception configurations, and that networks comprising a mix of vendors can be equally well supported. The result is rapid lawful interception installation, at reduced costs, while supporting future network evolutions.

Most Technologies and Services Supported

ALIS operates over UMTS, CDMA2000, LTE and WiMAX networks, as well as IP, wireline, and legacy 2G (e.g., GSM) networks. Thus, subsribers to a network operator's mixed service offer of wireline and mobile 3G / 4G services can be targeted, regardless of what services they are using. Perhaps more important, operation of the ALIS platform is essentially identical over the types of services implemented. For example, a common platform and operator interface can handle the interception of subscribers using a Network Operator's wireline, Internet access, GSM, 3G or 4G services. This alows the operators of the interception system to quickly adapt to new services. As a result, operator training costs diminish.

No Detection by the Mobile Subscriber

Subscribers are completely unaware of whether or not they are being tracked, thanks to Aqsacom's patented use of signalling information that is inherently processed within mobile networks.

No Detection by the Mobile Subscriber

Standards-compliance also means interoperability of the network with the LEA. Thus a LEA's investment in analysis tools remains intact as new networks and services come on line.

ALIS' complete set of funcitonalities

The comprehensive set of features and capabilities of the ALIS platform ensures easy, reliable, and secure operation of the system from both the network operator's and LEA's point of view.

9 References

[1] CDMA Development Group worldwide statistics (see www.cdg.org)

[2] UMTS Forum. Data are as of January 2005. See http://www.umts-forum.org

[3] *HSPA+ for Enhanced Mobile Broadband*, White Paper, Qualcomm Inc., February 2009.

[4] TD-SCDMA Forum. See http://www.tdscdma-forum.org

[5] Recommendations from the ITU-R M.1645

[6] 3rd Generation Partnership Project *TR 21.905 V6.6.0 (2004-03)*, "Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 6)," March 2004.

[7] 3rd Generation Partnership Project *TS 23.002 V6.4.0*, "Technical Specification Group Services and Systems Aspects; Network architecture (Release 6)," March 2004.

[8] *WiMAX Forum Network Architecture: Architecture Tenets, Reference Model and Reference Points Base Specification*, WiMAX Forum, WMF-T32-001-R015v01, 21 November 2009.

[9] ETSI Standard *ETSI ES 201 671 V2.1.1 (2001-09)*, "Handover interface for the lawful interception of telecommunications traffic," September 2001.

[10] 3rd Generation Partnership Project, *Technical Specification 3GPP TS 33.107 V6.0.0 (2003-09)*, "Lawful interception architecture and functions (Release 6)," September 2003.

[11] 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions*, 3GPP TS 33.107 V8.8.0 (2009-06), June 2009.

[12] *WiMAX Forum Network Architecture: Architecture Tenets, Reference Model and Reference Points, WiMAX Broadband Access Lawful Intercept: Overview*, WiMAX Forum, WMF-T32-106-R015v01, 21 November 2009.