# Table of Contents

1. Introduction .................................................................................................................. 4
2. Bringing Voice to LTE Networks .................................................................................... 5
3. The Architecture of Lawful Interception ...................................................................... 7
4. AQSACOM’s ALIS Mediation Platform ........................................................................ 10
   4.1 ALIS Overview ....................................................................................................... 10
   4.2 ALIS in More Detail ............................................................................................... 11
5. Applying Lawful Interception to Voice Services ......................................................... 13
   5.1 Introduction.......................................................................................................... 13
   5.2 Circuit Switched Fall Back (CSFB) ......................................................................... 13
   5.3 Single Radio Voice Call Continuity (SRVCC).......................................................... 16
   5.4 Simultaneous Voice LTE (SVLTE) ........................................................................ 17
   5.5 Voice over LTE Via Generic Access (VoLGA)......................................................... 18
   5.6 “Over the Top” (OTT) Voice over LTE ................................................................... 18
   5.7 True Voice over LTE (VoLTE) ................................................................................. 19
   5.7.1 Overview ....................................................................................................... 19
6. Lawful Interception Implementations ........................................................................ 19
   6.1 Coordinating Lawful Interception of Legacy 2G/3G Networks with LTE ............. 19
      6.1.1 Overview ....................................................................................................... 19
      6.1.2 Target Identities for Transitional LTE Networks ........................................... 21
      6.1.3 Implementation with AQSACOM ALIS .......................................................... 21
   6.2 Interception of Voice over LTE (VoLTE)................................................................. 22
      6.2.1 Overview ....................................................................................................... 22
      6.2.2 Target Identities for VoLTE ........................................................................... 23
      6.2.3 Interception of VoLTE by ALIS ....................................................................... 25
7. Solution Scaling ........................................................................................................... 26
8. Summary ..................................................................................................................... 28
9. References .................................................................................................................. 30

ANNEX A. Description of IMS ............................................................................................. 31
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 and + 33 1 69 29 84 00
Fax +33 1 69 29 84 01

Aqsacom Inc. (North America)
222 W. Las Colinas Blvd
Level 16, Suite 1650 Urban Towers - East
Irving, TX 75039
Tel. +1 972 591 5919

AQSACOM South America
Rua Vitor Konder, 125
Sala 402
Centro
Florianopolis, SC Brazil CEP 88015-400
Tel: ++55 48 9916 9834

sales@aqsacom.com
www.aqsacom.com

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

AQSAOM India
Gachchi Bawli
Hyderabad, Andhra Pradesh
India
Tel: +91 99999 61066
Lawful Interception for Voice Services with LTE Networks

Aqsacom SA and Aqsacom Inc.

1 Introduction

Deployments of Long Term Evolution (LTE) networks continue unabated on a worldwide scale, thanks to the wireless communications services providers’ drive to deliver new, bandwidth consuming services to an ever growing and accepting user base. LTE makes such services possible because of a) more efficient use of scarce radio spectrum resources through advanced signal transmission, modulation and encoding schemes, b) packet-based network infrastructure driven by rapid technological Moore’s law advancement, and c) a clear path of migration from existing network infrastructures towards fully packetized infrastructures. However, and perhaps ironically, traditional voice and SMS messaging services still constitute the dominant application of cell phones, constituting well over half of the revenues to the cellular wireless services providers. Thus, while end user demand and marketing hype may make “apps” and video streaming the center of attention for wireless users and marketing, wireless providers must also preserve their revenue streams from legacy voice and SMS services. Herein lies the challenge to the wireless providers – namely their need to support high quality voice communications while rolling out data-driven services over network infrastructures which evolve from a circuit switched model to a fully packetized infrastructure. This challenge is compounded by the regulatory situations that the wireless providers face, including the need for continued support of lawful interception for traditional voice and messaging services, along with interception for evolving data services as the underlying network infrastructures evolve.

The lawful interception of LTE networks is described in detail in a number of reference documents released by the Third Generation Partnership Project (3GPP) organization (e.g., refs. [1, 2]). The interception of LTE networks, including LTE Advanced networks, is also described in AQSACOM’s companion White Paper Lawful Interception for 3G and 4G Networks [3]. We refer the reader to that White Paper for a general overview of LTE and the practices of providing intercepted data flows from such networks to law enforcement. Given that commercial wireless networks are at various stages of deployment, a common and systematic methodology for the implementation of lawful interception systems for voice is ever critical. AQSACOM has therefore prepared the White Paper herein, with the goal of addressing a systematic approach to lawful interception as it applies to the interception of voice services in conjunction with LTE services, including Voice over LTE (VoLTE).
2 Bringing Voice to LTE Networks

LTE is a set of standards, architectures, and practices that imparts an evolutionary approach to a wireless carrier’s adaptation to more advanced network capabilities. This evolution has been pushed by advancements in packet network technology that enable voice and even video carried over packet networks to achieve the expectations of quality that were once the main selling and preservation point for circuit switched networks\(^1\). Meanwhile, the evolutionary nature of LTE enables the carrier to gradually build out new network infrastructure while maintaining the investment in existing network equipment and services. Voice is no exception; i.e., as a wireless carrier builds out a packet-based LTE network infrastructure, the carrier will likely desire to preserve its investment in voice networking from prior 2G and 3G deployments while or before moving over to true Voice-over-LTE (VoLTE) architectures as market conditions and network investment decisions dictate. Likewise, handset roaming capability must include evolutionary capabilities since a user might roam to locations where LTE deployments are not as well developed.

To understand how wireless carriers coordinate the support of LTE networks along with voice and text messaging services, we begin with the overall description of an LTE network, as shown in Figure 2-1. What is immediately clear from the figure is the support of new LTE packet-based services through the “Evolved Node B” (or eNB radio), packet gateways, and subsequent packet-based processing systems. Also included in Figure 2-1 are simplified representations of legacy 2G and 3G network components to emphasize the evolutionary nature of LTE. These legacy network components connect to the handsets via the Generic Access Network (GERAN) and Universal Terrestrial Radio Access Network (UTRAN) networks. Key components making up LTE and associated legacy networks are:

- **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 or SGW).** 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 Section 6. Note the GERAN and UTRAN include the Mobile Switching Centers of the corresponding legacy networks.

\(^1\) The standards for assuring Quality of Service in evolved packet networks are spelled out in 3GPP TS 22.278 [4].
**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, and policy enforcement. The PDN GW also serves as the interception point for delivering Call Content to Law Enforcement. This will be discussed in more detail in Section 6.

**ePDG** (Evolved Packet Data Gateway). The ePDG provides an interface that enables the connectivity of untrusted UE (e.g. WiFi network) between the Evolved Packet Core and non-3GPP network.

**SGSN** (Serving GPRS Support Node). This is a core element of 2G and 3G networks. It is responsible for routing of packets between the legacy base station / radio network controllers (BSC/RNC) and the Gateway GPRS Support Node (GGSN) (the latter two are not shown). 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.

**MSC Server** (Mobile Switching Center Server). Provides the high capacity switching within mobile switched circuit networks. Historically, the MSC Server (otherwise known as the “MSS”) pertained to the switching of 2G networks, but the term can also apply to the switched WCDMA voice services provided through 3G networks.

**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. It contains information about the subscriber and the services subscribed to.

**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.

**Operator IP Services** include support for IMS (IP Multimedia Subsystem), which will be further described below.

With the basic layout of an LTE network and its interplay with 2G/3G networks in hand, we will soon discuss specific implementations of voice support over and in conjunction with LTE networks. However, in the next section we provide a quick review of the fundamental practices of Lawful Interception as they pertain to public wireless networks.
3 The Architecture of Lawful Interception

Figure 3-1 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 the network operator. 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 numerous technical and services evolutions. 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 3-1 by the demarcation line between the Network and Services Operator Domain and the Law Enforcement Domain. The cloud to the left in Figure 3-1 represents a conceptual wireless network that contains one or more Network Elements (NE – otherwise called “Network Entities”) which perform parts of the lawful interception functions, such as in the collection of intercepted traffic from switches, routers, or network probes (explained further below).

AQSACOM is a leading supplier of mediation platforms to network operators worldwide. Its mediation platforms are specifically designed to support lawful interception while meeting the evolving needs of its network operator customers.
Figure 3-1. Simplified view of lawful interception architecture. Of primary interest is the use of a Media-

Figure 3-1. Simplified view of lawful interception architecture. Of primary interest is the use of a Media-

The Reference Architecture for lawful interception, as proposed by the Third Generation 

The Reference Architecture for lawful interception, as proposed by the Third Generation 

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 (including the USA), albeit with slight variations in terminology for different parts of the world. The architecture is also general in that it applies to both legacy wireless and wireline voice services 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), delivery of intercepted call data from the network operator to the LEA, and conveyance of call content from the network operator to the LEA.

In the case of LTE networks that support voice services or operate in conjunction with 2G and 3G networks, the application of the 3GPP model can occur at two levels. The first level is at the level of interception of data packets that traverse a network operator’s LTE network. This type of interception has been described elsewhere [1-3] and will be described for VoLTE in Section 6. In the case of voice services, a second level of interception must also occur at pertinent network elements supporting circuit switched voice, as will be described in the Sections to come.

Communications between the network operator and LEA are via the Handover Interfaces 

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 indicated in Figure 3-2 is the **Handover Interface HI-a**, which is not a formal part of the 3GPP architecture but included here to represent the feedback of an Operations and Maintenance function to and from the LEA. This interface supports, for example, the conveyance of alarms indicating failure of an interception process.

*AQSACOM plays a major role in providing Mediation capabilities to the wireless network operators*, as will be described in Section 6.

![Diagram of 3GPP-defined Reference Architecture for lawful interception](image)

**Figure 3-2.** 3GPP-defined Reference Architecture for lawful interception (derived from Figure 4.1 of ref. [2]). Note the separation of lawful interception management functions (HI1), delivery of call-related data (HI2), and delivery of call content (HI3) in the interaction between the LEA and communication service provider. AQSACOM supports IRI, CC, and Alarms transmission over TCP connections.
4 AQSACOM’s ALIS Mediation Platform

4.1 ALIS Overview

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, scalable, low cost manner over networks supporting a diversity of services. The platform makes the deployment and provisioning of lawful interception system 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 4G, broadband IP, satellite, voice-over-IP, and other technologies while supporting the lawful interception needs of legacy networks and their services (e.g., wireless 3G, wireline voice, wireline broadband, etc.)

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 4-1). The processes of Mediation, Delivery, and Provisioning are represented by each layer of the architecture. The vertical bidirectional arrows represent “technology connectors (TC)” and “network connectors (NC)” that provide the interfaces to vendor-specific network elements as well as to probes for the interception provisioning and traffic collection. ALIS-D carries out delivery of the intercepted traffic to the LEA in accordance with national-compliant interception data formatting. Provisioning of the interceptions is via ALIS-M. 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 (this is discussed further below).

![Figure 4-1. Architecture of the AQSACOM ALIS platform.](image-url)
4.2 ALIS in More Detail

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 the figures of Section 6 below. Specific tasks of provisioning include start, stop, query and modification of lawful interception operations, as well as audit, consistency checking, etc. These tasks are generally entered and controlled by the network operator in response to the receipt of a court order. In some cases, the interception provisioning can be communicated directly from the LEA to ALIS in a secure manner. 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 receive surveillance products from 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 resulting interception products to the LEA over a secure network (typically a VPN, secure FTP, or ISDN). As discussed in Section 3, intercept data takes the form of Call Data (otherwise known as Interceptor 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 those published by 3GPP, ETSI, and ATIS (for US CALEA compliance). To ensure reliable real-time delivery of interception information to the LEA, ALIS implements adequate buffering to account for nominal transmission outages, slow-downs 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. All ALIS code is tested against intrusion. When requested, AQSACOM can provide certification that all code is free of backdoor entry and resistant against other types of attacks.
Reliable Operation

ALIS systems can be configured with hot-swappable component parts (e.g., disk drives, power supplies, CPU cards, network cards, etc.) to assure uninterrupted operation in the event of component failure. Likewise, multiple ALIS platforms can be configured for application-level redundancy to enable the switch-over of one ALIS system to another in the rare event that an ALIS platform fails. See the following figure for further details.

![ALIS-D Load Sharing cluster diagram]

Redundancy is at both the hardware and software “application” levels. Standby system maintains state of primary system.

**Figure 4-2.** Multiple ALIS-D servers enable scaling to share interception traffic processing. A standby ALIS-D server can be added in the event of failure of active ALIS-D equipment. Redundancy is implemented at the software, hardware, and operating state levels to ensure fast switch-over of platforms during platform failure switchover.

Distributed Operation

One ALIS-M management system can control multiple ALIS-D mediation systems. This enables the balancing of interception traffic load processing among multiple ALIS-D systems. One ALIS-M can also control multiple ALIS-D systems that are placed throughout geographically diverse network points in the CSP’s network. This is described in more detail in Section 7.

Billing

ALIS can be adapted to provide a variety of billing plans to support how the network operator invoices the LEA for lawful interception services. 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 is not sufficient to justify the investment in LI infrastruc-
ture. In this case, billing can be addressed to the subscribing network operator, and / 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), sta-
tistics (number of active interceptions in a given interval in time, utilization of LI system 
resources), and logs for tracking of past LI events. Alarms can be configured in a “soft” 
manner to indicate the approach of a condition. All log data are encrypted and accessi-
ble only by vetted personnel.

**Hardware / Operating System**

ALIS makes use of off-the-shelf industrial strength PC hardware. This allows for easy 
parts replacement and reduced cost, while taking advantage of continuous improve-
ments in the computing power and reduced power consumption of commodity comput-
ing equipment. All software runs under the Windows and Linux operating systems.

# 5 Applying Lawful Interception to Voice Services

## 5.1 Introduction

As discussed in the introduction, the evolutionary nature of LTE enables the gradual de-
ployment of packetized networks that initially support high speed data and ultimately a 
mix of voice, messaging and high speed data services. Because initial deployment of LTE 
by a carrier might not provide for explicit voice services, network configurations and hand-
sets must be deployed that allow for use of legacy switched voice services over 2G and 3G 
networks. Two such configurations are Circuit Switched Fall Back (CSFB) and Single Radio 
Voice Call Continuity (SRVCC), which will be described below followed by descriptions of 
how these network configurations can be intercepted. Other evolutionary approaches are 
also discussed, followed by a description of true Voice over LTE (VoLTE). Methods for law-
ful interception implementation are likewise described following descriptions of the vari-
ous methods in which voice services are coordinated with LTE.

## 5.2 Circuit Switched Fall Back (CSFB)

Circuit Switched Fall Back constitutes a common means of supporting legacy voice and 
messaging based on 3G/GSM/GPRS during the early phase of a network operator’s LTE 
deployment. As the name implies, CSFB leverages the use of a network operator’s in-
stalled base of legacy 2G and 3G infrastructure to support voice calls and messaging. 
CSFB implementations generally follow 3GPP TS 23.272 [5]. This standard applies to both 
legacy 3G UMTS and CDMA networks, although most implementations of CDMA utilize
Simultaneous Voice and LTE (SVLTE), which is described further below\(^2\). CSFB constitutes an evolutionary approach that enables voice services to be sold with a high speed LTE data service offer. Most network operators that roll out CSFB will ultimately replace CSFB with true VoLTE. Note CSFB applies only to newly placed calls to or from a CSFB-capable handset; i.e., a call that is already in place cannot be switched to CSFB.

CSFB, as recommended by 3GPP TS 23.272, operates as follows:

Preliminaries:

1. The wireless network operator establishes a static mapping of 4G tracking areas to 3G location areas. This mapping is stored in the LTE network Mobile Management Entities (MMEs), and determines the appropriate 3G Mobile Switching Center to be used during a voice call when the mobile handset is in a given area of LTE coverage.
2. The handset must be CSFB-capable; i.e., contain the necessary hardware and software to switch between 4G packet data communications and 2G/3G voice communications with the wireless network operator.

CSFB Steps – Call Originates from Handset

1. An LTE 4G handset registers on the MME via the eNB indicating that the handset is CSFB-capable.
2. The CSFB is next registered on the appropriate legacy SGSN and Mobile Switching Center. The selected SGSN/MSC is determined by the 4G/3G mapping described above.
3. As the handset moves about, updates to the appropriate SGSN and Mobile Switching Center occur to ensure that the network will be ready to handle voice calls and messaging to/from the handset.
4. When the handset initiates an outgoing voice call\(^3\), the MME is informed of the event.
5. The MME then informs the handset to switch over the Radio Access Technology (RAT) to the 3G radio access network. The handset registers on the 3G network, including the 3G network’s Mobile Switching Center and the Visitor Location Register.

---

\(^2\) One exception has been Sprint in the US, who deployed “Enhanced CSFB” which makes use of a single radio to simplify the design and reduce battery consumption. This was presumably motivated by their support of three radio bands which would have made the handsets complicated and costly in a Simultaneous Voice LTE (SVLTE) implementation (described below).

\(^3\) In CSFB, both voice and SMS text messaging can be handled over the legacy circuit switched network as per 3GPP 23.272; however this standard also supports SMS over LTE. Therefore, it becomes an implementation choice for the network services provider as to whether SMS runs over LTE or falls back to a circuit-switched network. For brevity, we will only refer to voice calling with the implied inclusion of text messaging.
6. Once registration is completed, the call is connected. See circled steps 1 through 3 in Figure 5-1.

CSFB Steps – Call Terminates at Handset

1. When the handset terminates an incoming call from the network, the call is first routed to the designated Mobile Switching Center (as identified in the target area mapping described above).

2. The MSC informs the MME, which has already registered the handset, that a call is attempting to reach the handset.

3. The MME forwards an incoming call indication via LTE eNB to the handset.

4. The handset suspends the LTE connection, switches over to the legacy 3G radio network and connects the call. See the circled steps of Figure 5-1.

CSFB only supports one radio operating in the handset at a given moment. Newer CSFB handsets contain a single radio supporting LTE, 3G, and 2G radio access and network protocols. CSFB also has its own evolutionary stages, in particular with respect to the support of roaming.
SRVCC represents an evolutionary path towards full LTE deployment, accounting for the situation where a network operator must enable a handset to fall back to a 3G network when LTE coverage is not available or not yet deployed. The 3GPP describes recommended practices for SRVCC, but substantial network investment by the operator is still required to support it. As the name implies, SRVCC uses one radio in the handset that can be immediately reconfigured when the handset moves from an LTE and 3G radio network or back. One radio in the handset, in theory, reduces handset costs and conserves battery charge compared to SVLTE (see following paragraph). In contrast to CSFB, SRVCC a) assumes that a voice call has already been initiated and b) supports the seamless transition of the call between VoLTE to a legacy circuit switched network or between the legacy circuit switched network and the VoLTE network. (Recall that CSFB arranges for the
handover of a newly incoming or outgoing call from an LTE network to a circuit switched
legacy network, and back to the LTE network upon the call’s completion.) Figure 5-2 [6]
provides a simplified view of the SRVCC handover process, in this case when a 3G circuit
switched call hands over to a VoLTE call. As can be seen in the figure, this process in-
volves SIP signaling between the IMS services and the handset.

Figure 5-2. SRVCC handover from 3G circuit switched voice call to packet-based VoLTE call (based on [6]).

5.4 Simultaneous Voice LTE (SVLTE)

This evolutionary approach calls for the use of handsets containing two separate radios,
one for connection to the carrier’s packet LTE network and the other to the carrier’s leg-
acy circuit switched network. The radios can operate in a simultaneous “on” state,
thereby supporting simultaneous voice calls and data transmissions4. This feature is es-
pecially attractive when the user wants to tether a device to a handset for Internet con-
nectivity while using the same handset for a voice call. However, the multiple radios are
typically implemented in multiple integrated circuit chip sets with supporting radio fre-
quency switching components. This elevates the costs of the handsets and battery con-
sumption. On the other hand, defenders of the approach claim that with enhanced Sys-
tem on a Chip (SoC) integration, such cost and battery drain factors are diminished. The
dual radio approach has been mainly used by the CDMA network operators as an early

---

4 The data transmission can reside over the LTE or the legacy 3G network. Voice calls would be connected
to the legacy circuit switched voice network via the 2G/3G radio infrastructure.
and intermediate stage step in LTE network build-outs towards true VoLTE. Note, although a network might support SVLTE, some phones may only operate in a CSFB manner (e.g., iPhone5).

5.5 Voice over LTE Via Generic Access (VoLGA)

This is another evolutionary approach, this time leveraging the 3GPP “Generic Access to A/Gb interfaces” specification [7] to enable access to packet based services via alternative wireless networking services, most prevalently Wi-Fi (802.11). Generic Access was originally established to facilitate a capability whereby phones could connect to a core 2G or 3G network via a local wireless IP packet network, such as Wi-Fi or Bluetooth. This was meant to fill gaps in the cellular coverage at reduced expense to the cellular network operator, and to relieve network congestion at cellular base stations. Of course, the drawback here is that the phone must be equipped with Wi-Fi or Bluetooth, but this is less of an issue nowadays given the expectation of Wi-Fi and Bluetooth support in present day smartphones. The VoLGA Forum [9] extended this concept to make use of the LTE radio access network to facilitate the wireless IP interconnection between the handset and core 2G/3G network through reuse of part of the GAN infrastructure. Referring to Figure 5-3, the VoLGA Access Network Controller (VANC) serves as the bridge between the legacy network and evolved core network, where the connection to the handset remains as a broadband LTE packet connection, even during voice calls. Proponents of VoLGA claim that the switchover to voice calls made over VoLGA appears more seamless to the user than CSFB. The VoLGA Forum has specified practices for assuring quality of service, emergency calling, and roaming [8]. VoLGA has been deployed by a number of carriers worldwide as a transition towards true VoLTE.

5.6 “Over the Top” (OTT) Voice over LTE

This approach makes use of the packet data connection between an LTE handset and IP network infrastructure. Such a connection supports the use of Skype, WhatsApp, WeChat, Google Voice, and other calling and multimedia messaging services. With OTT,
the carrier is not responsible for managing the call and treats the data flow of the call set-up and media packets as that for any data packet. The high data rates and reliability of LTE networks make such services quite attractive and popular with the general public and can eventually supplant the use of carrier-offered wireless voice telephony and messaging services. However, their interception is treated as the interception of data packets and therefore will not be covered further in this White Paper. We refer the reader to our companion White Paper Lawful Interception of 3G and 4G Networks [3].

5.7 True Voice over LTE (VoLTE)

5.7.1 Overview

True VoLTE handles all voice calls and messaging over packet-based streams between the handset and throughout the LTE network. While there is no official definition of “VoLTE”, it is generally accepted that VoLTE conforms to the specification published by the GSM Association GSMA VoLTE I.92 [9], which calls for the use of an IMS (IP Multimedia System) core network to manage Voice-over-IP (VOIP) calls.

Referring back to Figure 2-1, the right side of the figure, Operator IP Services, represents where voice and other multimedia services are managed within an LTE network. Here it is assumed that Operator IP Services are based on an IMS architecture. Annex A provides a deeper look into the IMS architecture. The reader might immediately be struck by the IMS’ complicated nature. It does call for many interacting elements, which is one reason why its adaptation has been slow – especially when competing third party OTT VOIP, videoconferencing, streaming, and other services have gathered widespread acceptance while running over LTE’s generic data transport capabilities.

Regardless of trends in how value added services are to be provided, AQSACOM’s highly flexible approach to lawful interception will ensure that the network operator’s investment in a lawful interception solution today will be readily adaptable to services and networking practices of tomorrow.

6 Lawful Interception Implementations

6.1 Coordinating Lawful Interception of Legacy 2G/3G Networks with LTE

6.1.1 Overview

We first consider evolutionary network infrastructures that offer LTE high speed packet connectivity to wireless handsets, while leveraging legacy 2G/3G infrastructure for the...
offering of voice services over circuit-switched networking. Such evolutionary approaches were described in the previous section; recall they are LTE Via Generic Access (VoLGA), Circuit Switched Fall Back (CSFB), Single Radio Voice Call Continuity (SRVCC), and Simultaneous Voice LTE (SVLTE). In summary, voice interception of such networks is carried out via the lawful interception methodologies that have been in place for the legacy circuit switched voice networks.

Figure 6-1. Interception of voice over legacy circuit switched 2G/3G network infrastructure. (From Figure 1a of ref. [1].) IRI and CC interception products are delivered to the LEA’s Law Enforcement Monitoring Facility (LEMF) via the HI2 and HI3 handover interfaces, respectively.

Figure 6-1 provides a generic overview of how the voice interception is carried out, where it is assumed that the underlying voice and messaging transport is based on a circuit-switched network architecture. Here Intercept Related Information (IRI) is obtained from the Mobile Switching Center Server (MSC) or Gateway Mobile Switching Center Server in response to requests from the Administrative Mediation Function (ADMF) and conveyed over the X1_1 Administrative interface. Raw IRI is then delivered from the MSC/GSMC over the X2 interface to the Signaling Delivery Function. The IRI is formatted into a standards-compliant data flow by the Mediation Function, then delivered via the HI-2 Handover Interface to the Law Enforcement Monitoring Facility (LEMF). Intercepted Content of Communication (CC; i.e., the content of the voice calls) can be obtained either from the MSC/GSMC or Media Gateway (MGW). CC is then delivered to Law Enforcement via the Bearer Delivery Function. Note interception of SMS messages is normally
handled at the level of the MSC/GSMC as is the case for SMS interception over legacy systems, with the message contents delivered over HI2 to the LEA.

6.1.2 Target Identities for Transitional LTE Networks

The target identities for 2G and 3G interception at the GSN (xGSN/xGW) can be one of the following: IMSI, MSISDN or IMEI.

6.1.3 Implementation with AQSACOM ALIS

Figure 6-2 describes the interconnection of the ALIS Lawful Interception mediation systems with the legacy 2G/3G network. Parts of the LTE core network are included in the diagram to emphasize that they are isolated from the ALIS connectivity when circuit-switched voice interception is required. For wireless broadband networks that still support legacy circuit-switched 2G and 3G infrastructure, ALIS mediation systems may be placed at the level of the Mobile Switching Center (MSC) for voice interception. 3G data interception may also be supported by ALIS through communication with a Gateway GPRS Support Node (G-GSN), which is not shown. The latter would be useful in SRVCC implementations where the data services connectivity switches between LTE and 3G data networking.

Figure 6-2. Interception of legacy circuit-switched voice by ALIS when wireless carriers offer circuit-switched voice in conjunction with LTE-based services.
6.2 Interception of Voice over LTE (VoLTE)

6.2.1 Overview

Interception of Voice over LTE assumes that the wireless services provider has deployed VoLTE with packetized voice services. The interception of Intercept Related Information (IRI) is handled at the level of the IMS Proxy or Serving Call Session Control Function (P-CSCF and S-CSCF, respectively). The P-CSCF applies to roaming subscribers, whereas the S-CSCF applies to subscribers situated at their home network. As Figure 6-3 shows, the interception order’s provisioning is presented to the P-CSCF or S-CSCF via the X1_1 interface from the ADMF. Raw IRI is then presented to the Delivery Function, formatted, and sent to the LEA via the HI2 handover interface.

In IMS-based VoLTE, provisioning the interception of CC is performed at the Serving Gateway (SGW) or Packet Data Gateway (PDN-GW) – see Figure 6-4. Note CC interception does not apply to the IMS core network nodes. Furthermore, interception only applies to basic calls; interception for forwarded and transferred calls is the subject of further study [1, Paragraph 7A.1].

In the case of roaming, the wireless services carrier must provide detailed roamer information during the interception provisioning. Care must be taken to provision the correct service node based on the roaming information available in the target identification to prevent loss of any interception data.

![Figure 6-3. Interception of voice from LTE networks where voice is supported by IMS. This figure describes the collection and delivery of IRI for interception of networks that are configured for true VoLTE. (From Figure 1d of ref. [1].)
Figure 6-4. Interception of voice from LTE networks where voice is supported by IMS. This figure describes the collection and delivery of CC for interception of networks that are configured for true VoLTE. (From Figure 12.1.3 of ref. [1].) Generally, IRI is not handled at this level although this figure shows such capability.

6.2.2 Target Identities for VoLTE

IMS provisioning of interceptions for obtaining IRI is performed at the level of the CSCF, where the IRI is extracted from the SIP messages. As described in the previous section, the P-CSCF and the S-CSCF are the points of interception for gathering IRI from the target user. The P-CSCF (Proxy CSCF) is a SIP Proxy server that sits as the first point of contact to the IMS terminal. The S-CSCF (serving CSCF) is a central node of the signalling plane located in the IMS home network. Note VoIP IMS interception should be considered a “work in progress” within 3GPP and therefore is not complete, as will be indicated below.

Based upon network configuration, the ADMF provisions the P-CSCFs, or S-CSCFs, or both with SIP URI or TEL URL target identifiers. According to 3GPP TS 33.107, clause 7A.3 ‘Multimedia events’:

- All SIP messages to or from a targeted subscriber, and all SIP messages executed on behalf of a targeted subscriber for multi-media session control are intercepted by the S-CSCF, and optionally P-CSCF, and sent to Delivery Function 2 (see Figure 6-3). The target identifier used to trigger the intercept will also be sent with the SIP message.
• P-CSCF event reports may be redundant with S-CSCF event reports when the P-CSCF and S-CSCF reside in the same network; however, this standard does not require nor prohibit redundant information from being reported to the Delivery Function 2.
• The IRI should be sent to Delivery Function 2 with a reliable transport mechanism.
• Correlation for SIP to bearer shall be supported within the domain of one provider.
• An intercepted SIP event sent to the Delivery Function 2 is shown as follows:
  - Observed SIP URI
  - Observed TEL URL
  - Event Time and Date
  - Network element identifier
  - SIP Message Header
  - SIP Message Payload

The target identities for 3G interception at the GSN (xGSN/xGW) can be one of the following: IMEI or MSISDN. IMSI is under consideration by the 3GPP.

The target identities for multi-media at the CSCF of the IMS core can be one or more of the following: SIP URI or TEL URL.

The general format of SIP URI is defined in RFC 3261 Section 19.1.1. Its generic syntax is as follows:

\[
\text{sip:} \text{user:password@host:port;uri-parameters?headers}
\]

(refer to RFC 3261 for the details of each component in the syntax scheme).

Examples:

\[
\begin{align*}
sip:joe.bloggs@212.123.1.213 \\
sip:support@phonesystem.3cx.com \\
sip:+612015550123@phonesystem.3cx.com
\end{align*}
\]

The general format of TEL URL is defined in RFC 2806. Its generic syntax is shown as follows:

\[
\text{telephone-scheme ":" telephone-subscriber}
\]

Where telephone-scheme is ‘tel’; telephone-subscriber is an E.164 number.

Example: \[
tel:+61-201-555-0123
\]

The IMS carrier provides the network numbering scheme to ALIS during X1 provisioning.
6.2.3 *Interception of VoLTE by ALIS*

The implementation of ALIS for VoLTE is shown in Figure 6-5. As described in Section 6.2.1, provisioning of the network for IRI interception is at the level of the CSCF and PSCF functions; CC provisioning and interception takes place at the Serving or PDN Gateway.

![Figure 6-5 Implementation of ALIS in IMS-based VoLTE network.](image)

Remember, for wireless broadband networks that still support legacy 2G and 3G infrastructure, ALIS mediation systems may be placed at the level of the Mobile Switching Center (MSC) for voice interception. 3G interception may also be supported by ALIS through communication with a Gateway GPRS Support Node (G-GSN), which is not shown.

Figure 6-6 emphasizes that a common ALIS system can manage the interceptions of both the newer VoLTE IMS and legacy switch circuit voice networking environments. In this implementation (one of many), an ALIS-D mediation platform is assigned to the legacy circuit switched network, and another ALIS-D is assigned to handle the LTE VoLTE networking. Both are controlled by a common ALIS-M administrative platform. In effect, *one ALIS system can handle evolution of the network as it migrates from circuit-switched...*
voice services to purely packet networking. As the network expands geographically, additional ALIS-D mediation platforms can be deployed to following the growth of the network (see next section).

7 Solution Scaling

As carriers build out their LTE networks, the Lawful Interception architecture and support must scale with the network build-out. ALIS readily handles the scaling simply through the addition of ALIS-D servers, all controlled from a single ALIS-M management server. This scaling is illustrated in Figure 7-1. As sub-networks within a carrier’s network are built out or converted to LTE, ALIS can be brought on line in stages by the assignment of new ALIS-D servers to each new sub-network. Of course, if traffic loading permits, one ALIS-D system can handle multiple sub-networks. Figure 7-2 illustrates ALIS scaling at a regional level. Here a larger wireless operator may have multiple networks covering different geographical regions. In that case, one ALIS-D platform is assigned to each regional network. Additional ALIS-D servers for each region can be brought on line if additional interception capacity or redundancy is needed. Note this example of regional coverage of lawful interception by ALIS should be viewed as conceptual in that the physical location of the ALIS-D servers can be geographically dispersed by region or collocated at a central data center.

Figure 6-6. Implementation of ALIS for true VoLTE (IMS-based) voice interception along with legacy 2G/3G voice interception.
ALIS also supports *broadcast areas*. This allows the provisioning of only those ALIS-D servers in large wireless networks that are associated with a given target. For example, if a target resides in a certain country or state, provisioning would be restricted to ALIS-D servers in that country or state. This restriction could be overridden depending on how the warrant’s requirements progress during the course of an interception.

**Figure 7-1.** Scaling of an LTE network through the addition of ALIS-D servers all controlled by a common ALIS-M platform.

**Figure 7-2.** Regional support of an LTE through ALIS-D platforms assigned to each region of a wireless operator’s network.
8 Summary

This White Paper has presented an overview of the ways in which wireless cellular network operators are supporting voice services as they build out network infrastructure based on LTE. The incorporation of voice into LTE presents many technical challenges to the lawful interception of voice calls given the myriads of approaches to supporting voice on or in conjunction with LTE networks.

AQSACOM’s ALIS mediation platform offers a comprehensive solution to such 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 independence from equipment vendors 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 the newest networking infrastructure supporting true Voice over LTE, while also supporting legacy UMTS, CDMA2000, and 2G voice networks that will operate in tandem with LTE for the foreseeable future. Thus, AQSACOM provides a clear migration path for the support of lawful interception as network operators adapt new voice networking technologies while maintaining their existing voice infrastructure. Equally important, the operation of the ALIS platform is essentially identical over the types of network services implemented. For example, a common platform and operator interface can handle the interception of subscribers who make use of a Network Operator’s wireline, Internet access, GSM, 3G or 4G services. This allows the operators of the interception system to quickly adapt to new services thereby reducing training costs.

**No Detection by the Mobile Subscriber**

Subscribers are completely unaware of whether or not they are being intercepted, thanks to AQSACOM’s use of signalling information that is inherently processed within mobile networks.

**Intact LEA Investment**

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 functionalities**

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 points of view.

Thanks to AQSACOM’s strong international presence and technical know-how in lawful interception, ALIS constitutes a forward-oriented yet transparent solution to lawful interception as wireless network operators evolve to incorporate new services and underlying technologies to their networks. Through ALIS, network operators are able to readily meet the national requirements of lawful interception while minimizing investment, training, and overall operational costs.
9 References


ANNEX A. Description of IMS

IMS enables the network operator to offer value-added, media rich services. It also enables the network operator to charge subscribers by the duration of the service, the type of service offered, bandwidth consumed, etc.

Where LTE defines the core network used to carry packets, IMS is used to provide the services over the packet network. The call-centric model and hooks to the PSTN further support the appeal of IMS for the delivery of carrier-offered voice services. A parallel path for the implementation of IMS over fixed broadband networks presents an important aspect of IMS, particularly towards the convergence of wireless and fixed broadband services. Whether the network operators, in the long run, will be willing to continue to offer traditional voice services over packet wireless or broadband fixed networks remains to be seen. Right now this is the trend given the high margins that are still generated by voice services.

Key networking elements of IMS are shown in the green boxes of Figure A-1. This diagram was derived from the 3GPP IMS specification [10,11]. The network components, especially those which pertain to lawful interception, are briefly described as follows:

**AS** (Application Server). Application Servers handle the signaling that supports the application offered by the network operator. Such signaling operates over IP networking. For example, in the case of VOIP, the AS will control the call set-up, tear-down, forwarding, etc. via Session Initiation Protocol (SIP). In general, application operation conforms to IETF recommendations when appropriate.

**CSCF** (Call Session Control Function). This handles call control within the IMS core network by registering the call endpoints and signal routing between them, as well as manages the quality of service. CSCF is managed by the following functions:

**S-CSCF** (Serving CSCF). This manages the call sessions placed by the subscriber, including maintenance of session state between the endpoints and passing of call information to the Application Servers or to external networks (such as the PSTN).

**P-CSCF** (Proxy-CSCF). This is the signaling connection point to the subscriber handset. It determines if the call is to be controlled by the local I-CSCF or by a home CSCF if the subscriber is roaming. Signaling is handled via SIP.

**I-CSCF** (Interrogating CSCF). The I-CSCF coordinates all call sessions and session states within the network’s IMS environment.

**HSS** (Home Subscriber Register). Includes the functions of the Home Location Register (HLR) as well as other functions for managing user mobility and multimedia applications over IP networks. It contains information about the subscriber and the services subscribed to. Upon registering onto an IMS network, information about the subscriber is polled from the HSS by the I-CSCF.

---

6 ETSI TISPAN has dealt with lawful interception for fixed broadband networks supporting IMS; see [12].
**BGCF** (Breakout Gateway Control Function). Selects the network which will provide connectivity to the PSTN. In some cases, one BGCF may select another if multiple networks are involved; alternatively, the BGCF will connect to the MGCF (below) for direct PSTN connectivity.

Media services are managed within the IMS environment through:

**MGCF** (Media Gateway Control Function). Controls the Media Gateway to circuit switched PSTN networks. This control is through SIP.

**IM-MGW** (IP Multimedia - Media Gateway). Handles the media processing for transporting calls between circuit switched and packet networks.

**MRFC** (Multimedia Resource Function Controller). Coordinates control of the MRFP (below) via SIP messaging with the Application Servers.

**MRFP** (Multimedia Resource Function Processor). Carries out packet processing in support of the Application Servers.

---

For details on the signal flows and interactions between the above elements, the reader is referred to numerous tutorial articles on IMS as well as the full specification [10,11]. Figure A-2 provides a simplified view of IMS in terms of a layered conceptualization. The AS and HSS operate at the Application Layer. Systems responsible for managing call session control are associated with the Control Layer. Systems responsible for routing the calls through the appropriate networks operate at the Media and Access Layer.
Figure A-2. Simplified view of IMS.

End of document