White Paper

# Utimaco LIMS™

## Lawful Interception in the Digital Age: Vital Elements of an Effective Solution

# Table of contents

1 Challenges to Lawful Interception ..... 3

2 Lawful Interception in the 21st Century ..... 4

2.1 An Increasing Need for Lawful Interception ..... 4

2.2 Regulatory Environment ..... 5

2.2.1 National Laws ..... 5

2.2.2 The United States ..... 6

2.2.3 The European Union ..... 6

2.2.4 The European Telecommunications Standards Institute ..... 7

2.2.5 The 3rd Generation Partnership Project ..... 7

2.2.6 Solution Considerations for Achieving Compliance ..... 7

3 Interception Fundamentals ..... 9

3.1 Roles of Different Parties in the Interception Framework ..... 9

3.2 Key Components of a Lawful Interception Solution ..... 10

3.3 Importance of Trust and Ethical Standards in Lawful Interception ..... 11

4 Addressing the Challenge ..... 13

4.1 LIMS System Architecture ..... 13

4.2 Interception Types: Active, Passive, and Hybrid ..... 14

4.3 Functional Operation of LIMS ..... 18

4.4 Benefits of LIMS ..... 19

4.5 Summary ..... 20

5 Additional Resources ..... 21

5.1 Interception Laws ..... 21

5.2 Interception Standards ..... 23

6 Glossary and Abbreviations ..... 25

7 About Utimaco ..... 26

# 1 Challenges to Lawful Interception

With a worldwide landscape characterized by entirely new forms of electronic communication – including digital communication based on Internet technologies that have gained popularity over the last decade – the nature of lawful interception (LI) has changed substantially. Regulatory mandates implemented in many countries present a significant challenge to the telecommunications companies, network operators, and service providers tasked with meeting current requirements. Solutions that have been developed in recent years to comply with local and national regulations differ considerably from the tools of past eras when lawful interception encompassed primarily the public switched telephone network (PSTN), permitting simpler monitoring of what was essentially a closed network. In this digital era when the Internet provides multiple means of exchanging messages and voice communications – over a much more open telecommunications network than the PSTN – the onus is on companies to modify and extend their network infrastructures to accommodate the necessary framework for lawful interception and to support techniques that permit the capture and analysis of communication data in response to law enforcement requests.

The complexities of today’s communication environment heighten the need for lawful interception tools versatile enough to contend with the widest range of wired and wireless communication exchanges. These tools must also have the interoperability to integrate easily into existing network infrastructures as well as the reliability to meet real-world challenges in a proven and secure manner. Regardless of the architecture or technology employed in lawful interception activities, effective solutions need to be available on demand to respond to all lawful surveillance requests from those agencies empowered by law to obtain the information.

This document discusses the elements of a successful lawful interception solution from the perspective of those organizations looking to modify their infrastructure to meet requirements. The target audience includes network operators with fixed and mobile installations, Internet service providers, telephone companies, system integrators, and law enforcement agencies.

# 2 Lawful Interception in the 21st Century

The types of communication available to individuals in these early years of the 21st century are versatile, diverse, and based on an expanding range of technologies. Modern telecommunications networks offer access through a tremendous range of technologies, including PSTN, ISDN, xDSL, WLAN, WiMAX, GSM, GPRS, UMTS, CDMA, cable, and other technologies based on the Internet Protocol (IP).

Voice communication services have progressed from a fixed network model to encompass wireless technologies, such as cellular telephones, and Internet-based exchanges, such as voice over IP (VoIP). Data services have expanded as well, spanning video, facsimile (fax) services, Short Message Services (SMS), e-mail, image transmissions, and other services. Internet-based communications have become ubiquitous and have grown far beyond the basic capabilities of e-mail to include instant messaging, peer-to-peer (P2P) networking, chat services, and low-cost voice communication through a variety of companies and emerging technologies such as Session Initiation Protocol (SIP). The nature of the Internet also suggests that new applications and innovative tools will be developed in the future to extend communication options in unpredictable ways. Amidst this profusion of communication possibilities, national security organizations and law enforcement agencies need mechanisms and proven techniques to detect criminal activities and terrorist operations.

The need for lawful enforcement solutions is growing even while the dynamics of the market and the legal and regulatory framework continue to evolve. Network operators, ISPs, telephone companies, and others face an unprecedented public and regulatory obligation to adapt their workflow and infrastructure – selectively tapping into the vast flow of information within the telecommunications spectrum to selectively extract targeted data. For example, the interception of a single e-mail message can pose a major challenge to an Internet Service Provider because of the high volume of IP traffic handled by a typical large Internet Exchange, such as the Internet Exchange DE-CIX. This organization calculates the average throughput of the 175 Internet Service Providers it carries at 41.3 gigabits/second, and spikes in traffic range to nearly 70 Gbps.[1] Clearly, state-of-the-art technology is required to handle lawful monitoring activities that involve this level of data throughput.

## 2.1 An Increasing Need for Lawful Interception

This worldwide explosion of communication technologies creates significant challenges for law enforcement agencies and national security organizations responsible for battling various forms of crime and terrorism. The sophistication of criminal enterprises in exploiting emerging communication channels has increased with the rising popularity of these channels, posing a

[1] DE-CIX daily graph and weekly graph, www.de-cix.net/stats, June 25, 2006.

very real challenge to organizations responsible for protecting public safety and reducing the impact of crime on communities. Given the broad availability of communication options and the relative ease with which criminal networks and terrorist groups can exchange information across these channels – by both data and voice communication – the impetus to intercept illicit exchanges and track the operations of criminal enterprises is strong and compelling.

In response to rising threats and worldwide terrorist operations, individual countries and international organizations have created regulations that enable and facilitate lawful interception of communications that take place across the channels discussed earlier in this paper. Although regulations controlling the interception of communications over traditional channels, such as telephones, have been in place for a number of years, many of these regulations have been recently amended to include Internet-based communication, wireless communication, and related forms of voice and data communication. These regulations mandate compliance by telecommunication companies, ISPs, network operators, and service providers who develop or maintain the infrastructures over which the communication takes place. In such cases, solutions are critically needed that can be effectively integrated into the infrastructure and – once implemented – can support lawful interception of a wide range of communication types. To meet the ethical demands and privacy requirements at the core of lawful enforcement, these solutions must prevent any activities involving illegal interception and illegal access at all levels, including – but not limited to – access by internal employees of the service provider.

## 2.2 Regulatory Environment

An overlapping framework of international and national regulations establishes the foundation for the monitoring of telecommunications, implemented to enable law enforcement agencies to intercept messages or information being distributed for illegal purposes. This section provides an overview of the regulatory framework that prevails throughout the world.

### 2.2.1 National Laws

Throughout the world, regulations relevant to lawful interception continue to be updated and modified to contend with advances in telecommunications and evolving forms of voice and data communication. Although the regulatory environment and the nature of the solutions required for compliance vary from region to region, the overall intent in most cases is very similar and the tools that provide compliance share common characteristics. Ideally, a successful lawful interception solution must be flexible enough to adapt to varying regulations and interoperable enough to deploy easily within the diverse network infrastructures in different regions.

Countries around the world have responded to the threats of terrorism and criminal activity by enacting legislation that provides the legal basis for lawful interception. The differences from country to country essentially involve the specific requirements as defined by the legislation, including the communication services to be intercepted, the applicable data formats covered, and the mechanisms through which particular types of communication are to be handed over to law enforcement agencies (LEAs). In the United States, for example, Congress mandated that all telecommunication operators provide interception capabilities to LEAs.

In Germany, Section 11 of the Telecommunications Monitoring Order (TKÜV [14]) delineates the types of telecommunications installations for which operators must provide assistance with monitoring operations. The types include circuit-switching networks, packet-switched networks, radio-paging networks, transmission routes for direct subscriber-related Internet access, and broadband cable networks. Other countries have different requirements, and a capable lawful interception solution should be able to accommodate national variations and a wide range of service types.

### 2.2.2 The United States

Passed by the United States Congress in 1994, the Communications Assistance for Law Enforcement Act (CALEA) stipulates the conditions under which telecommunications voice providers must assist a law enforcement authority in intercepting specific subscriber calls when presented with a valid court order. The provider must also deliver a record of the intercepted communications to the requesting authority. This Act was recently extended by a Federal Communications Commission (FCC) ruling to ensure that companies that provide VoIP services meet the compliance requirements as well, with a May 14, 2007 deadline in place for making the necessary network modifications.

To comply with this regulation, providers of IP-based phone services must deploy the network equipment to facilitate monitoring of VoIP communications, including the mechanisms for tapping into calls of subscribers identified by a court order and recording calls when required.

In addition to CALEA, a number of other U.S. standards bodies establish compliance requirements that network operators must meet in respect to U.S. laws. Organizations active in this area include American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), Alliance for Telecommunications Industry Solutions (ATIS), PacketCable, and others. Section 5 provides an overview of existing standards.

### 2.2.3 The European Union

In a council resolution[2] enacted on January 17, 1995, the European Union specified requirements for national lawmakers and law enforcement agencies that establish the basis for various national telecommunication surveillance laws, as well as for many international interception standards.

[2] Official Journal of the European Communities, 96/C 329/01: "Council resolution of 17 January 1995 on the lawful interception of telecommunications."

### 2.2.4 The European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI) has been a major driver in defining lawful interception standards, not only for Europe, but worldwide. Technical standards ratified by ETSI specify a general architecture for LI that allows systematic and extensible communication between network operators and LEAs over defined interfaces. Significantly, this general architecture applies to any other kind of circuit- or packet-switched voice and data network – not just to switched-circuit voice networks and plain old telephone service (POTS).

Under the terms of the ETSI standards, compliance is achieved by meeting the requirements for all provisions of lawful interception, and, in particular, the requirements for the Handover Interfaces (HI) to the LEAs. Mandatory compliance with this ETSI standard has been enacted in a number of countries; the provisions state that following the request of a valid authority, the results of a lawful interception of a particular individual shall be delivered to the appropriate law enforcement agency. The mechanism used for the HI, as defined by the standard, must be an integral part of the network infrastructure of the service provider or network operator and it must fully meet all intercept requirements. For a listing of the standards and specifications maintained by ETSI, refer to Section 5.

### 2.2.5 The 3rd Generation Partnership Project

In addition to the ETSI specifications, a consortium of technology organizations called the 3rd Generation Partnership Project (3GPP) collaboratively defined technical specifications for lawful enforcement in 3G and future mobile networks. The initial applicable standards, 3GPP TS 33.106-108, establish a compliance framework that has been actively embraced by many industry participants (comparable to ETSI TS 101 331).

The 3GPP agreement, which was formalized near the end of 1998, includes input from ETSI, the Association of Radio Industries and Businesses/Telecommunication Technology Committee (ARIB/TTC) in Japan, CCSA China, the Alliance for Telecommunications Industry Solutions (ATIS) in North America, and the Telecommunication Technology Association (TTA) in South Korea.

### 2.2.6 Solution Considerations for Achieving Compliance

Regardless of the specific geographic location, the prevailing regulatory environment in your region is likely to include provisions so that lawful interception operations can be performed when requested by an authority. The following list highlights the capabilities of a lawful interception solution that are most relevant to regulatory mandates and legislative requirements.

- Comprehensive interception capabilities: The LI solution must be able to intercept all applicable communications of a certain target without any gaps in coverage.

- Reliability and integrity: The LI solution should ensure delivery of precise and accurate results with the highest levels of data integrity. The LI solution must be as reliable as the service to be intercepted.
- Separation of content: Intercepted communications data should be divisible into individual components; for example, the metadata included in the Interception Related Information (IRI) should be separable from the Communication Content (CC).
- Transparent surveillance: The monitoring activities performed by the solution must not be detectable by the subscriber.
- Immediate activation and real-time responsiveness: Following a request for lawful interception, a solution must be able to be immediately activated and provide real-time response in delivering intercepted data.
- Sufficient capacity: The solution must have adequate capacity to handle the scope and scale of requested surveillance activities.
- Data security and privacy: Sensitive data must be protected during transmission and the privacy of an individual's records and personal information should be safeguarded. Only authorized personnel should be able to view intercepted data.
- Decryption: Encrypted data shall be delivered in plain text format if the encryption keys are available to the service provider or network operator.
- Complete logging of events: All LI-related activities must be recorded and logged as part of a centralized record-keeping procedure.

# 3 Interception Fundamentals

Successful lawful interception activities require co-operation and collaboration among a number of different parties. It also requires physical mechanisms in place within the infrastructure to support the work processes. These topics are discussed in the following sections.

## 3.1 Roles of Different Parties in the Interception Framework

The nature of lawful interception requires cooperation and interaction among the following parties.

- Government agencies and legislative bodies: The rules and requirements that apply to lawful interception are defined and ratified into law by the legislative bodies of national governments. These requirements are enacted and enforced by responsible government agencies.
- Law enforcement agencies (LEAs): Requests for lawful interception operations typically originate from law enforcement agencies based on court orders or legal requests from a recognized authority. These requests are then presented to the service provider or network operator, who must comply with the terms of the request within a specified period.
- Service provider or network operator: Data and voice communications distributed through the network infrastructure are the responsibility of the service provider or network operator. Access must be provided to all applicable communication types as a part of a lawful interception operation requested by a valid authority.
- Interception service provider: Service providers and network operators may employ the expertise of an interception service provider to handle the management and fulfillment of lawful interception requests. These types of services can range from providing leased equipment and technical support to delivering fully outsourced, administered interception services from an off-site location.

Figure 1 illustrates the typical lawful interception process from the time the request is received to the data retrieval and termination of the request.

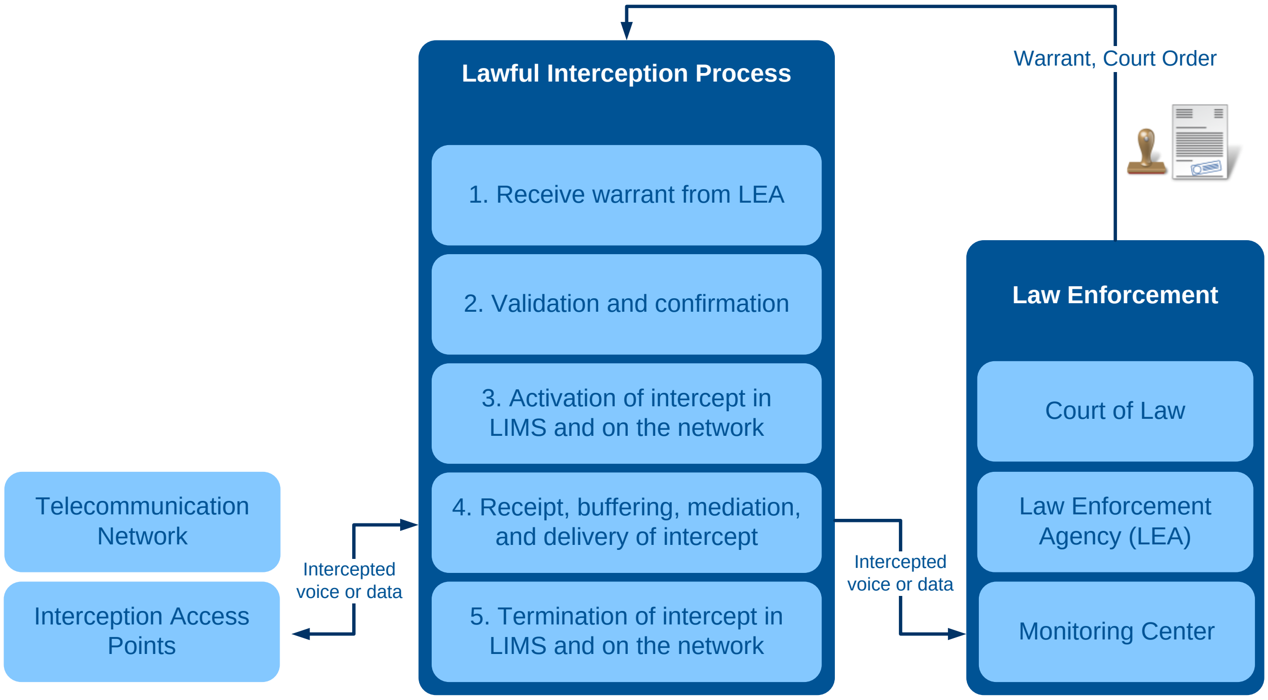
Lawful Interception Process
1. Receive warrant from LEA
2. Validation and confirmation
3. Activation of intercept in LIMS and on the network
4. Receipt, buffering, mediation, and delivery of intercept
5. Termination of intercept in LIMS and on the network
Warrant, Court Order
Law Enforcement
Court of Law
Law Enforcement Agency (LEA)
Monitoring Center
Telecommunication Network
Interception Access Points
Intercepted voice or data
Intercepted voice or data

*Figure 1: Steps in the lawful interception process*

## 3.2 Key Components of a Lawful Interception Solution

Examined at a system level, the typical LI solution includes the architecture and components shown in Figure 2. A monitoring Center, staffed by LEA personnel, relies on standardized interfaces from the governing body (whether ETSI, ANSI, or another standards body) to gain access to communications provided over fixed networks, mobile networks, and IP-related channels. As illustrated, the monitoring interface handles LI requests, the metadata (or IRI, Interception Related Information), and the actual content of the communications separately.

From the perspective of the network operator or service provider, the primary obligations and general requirements for developing and deploying a lawful interception solution are as follows.

- Maintaining cost effectiveness: The solution minimizes the time and effort involved in promptly setting up and responding to LEA representatives when LI requests are received.
- Minimizing impact to the network infrastructure: Operation of the lawful interception solution should not negatively impact the performance or behavior of the communication service or system.
- Ensuring compatibility and compliance: The solution meets the requirements of national and international standards and provides seamless operation with equipment from other vendors that provide components used within the infrastructure.

- Supporting future technologies: The solution adapts to evolving standards and specifications as they are introduced throughout the world, and can scale to accommodate the bandwidth increases and performance requirements associated with increased service levels.
- Maintaining reliability: The solution delivers accurate results and maintains data integrity at every stage of the workflow.
- Enforcing security: At all points in the LI system, data is protected against illegal or unauthorized access. Surveillance activities are not detectable in any way by users.

## 3.3 Importance of Trust and Ethical Standards in Lawful Interception

The interception of telecommunications and the surveillance of private communications produce ambivalent attitudes among legislative bodies and citizens seeking a balance between national security and privacy rights. Citizens of many countries are rightfully wary of governments and law enforcement bodies intruding on their private activities. Because of this, ethical concerns and essential privacy rights must be central considerations in any lawful interception solution.

Over the last few years, lawful interception has moved from a poorly defined and unevenly interpreted concept to a clearly established body of laws and regulations that set the limits and the framework under which LEAs and intelligence agencies must operate. This legal framework has gained recognition as an important method for prosecuting crime and detecting potential terrorist acts before they occur.

A delicate balance exists between the capabilities of the government to detect and prevent crime and terrorism – as supported by the laws and prevailing regulations in a country – and the individual rights and privacy concerns of the citizens of that country. A responsible, ethically grounded lawful interception solution recognizes that this balance can only be achieved by giving equal weight to both the legalities of the law enforcement tasks at hand and the individual rights of the citizens. Achieving this balance in a solution requires careful consideration of both the technological aspects of the challenge, as well as the legal and ethical issues that are intricately associated with the monitoring of any form of communication.

Oversight, accountability, and safeguards that protect against privacy intrusion are of paramount importance in a reputable lawful interception solution. Mechanisms to support these elements should be integral to the design of the LI product, rather than add-ons or adjuncts to the core technology. The sole purpose of an LI solution should be to obtain information within a valid and legal framework to detect criminal activities and subvert terrorist intent.

Well-engineered lawful interception solutions, such as the LI Management System from Utimaco, include built-in capabilities to prevent misuse by requiring positive authentication and authorization of all personnel initiating interception requests. Integral safeguards for auditing and recording events to ensure accountability are an essential aspect of each step in the workflow process. Another critical feature is maintaining secure storage and transfer of all intercepted data from the source to the LEAs involved in the activity. Compliance to the established matrix of accepted standards and regular certification by government bodies also bears strong consideration. Companies with a strong track record and a favourable history in the computer security field have a visible and verifiable information trail that can provide insights and evidence of their reputation and integrity. This kind of information can be a valuable metric for selecting a solution provider for a lawful interception system.

# 4 Addressing the Challenge

The Lawful Interception Management System (LIMS) from Utimaco offers an example of a system that has been successfully deployed in more than 40 countries around the world, providing a centralized solution that meets the requirements of service providers and network operators. LIMS adapts well to different geographies and varying regulatory frameworks, handling all of the major communication types relevant to lawful interception practices. This section provides an overview of the architecture and features of LIMS.

## 4.1 LIMS System Architecture

The Utimaco LIMS system architecture provides maximum flexibility and uses a modular design concept that can be adapted freely to accommodate various services, technologies, and LI standards, as well as all future developments in the lawful interception space. Utimaco Interception Access Points (IAPs) deliver specific interception capabilities with adaptability to meet future requirements. Designed to be deployed within the facility of a service provider or network operator, LIMS includes the elements shown in Figure 2.

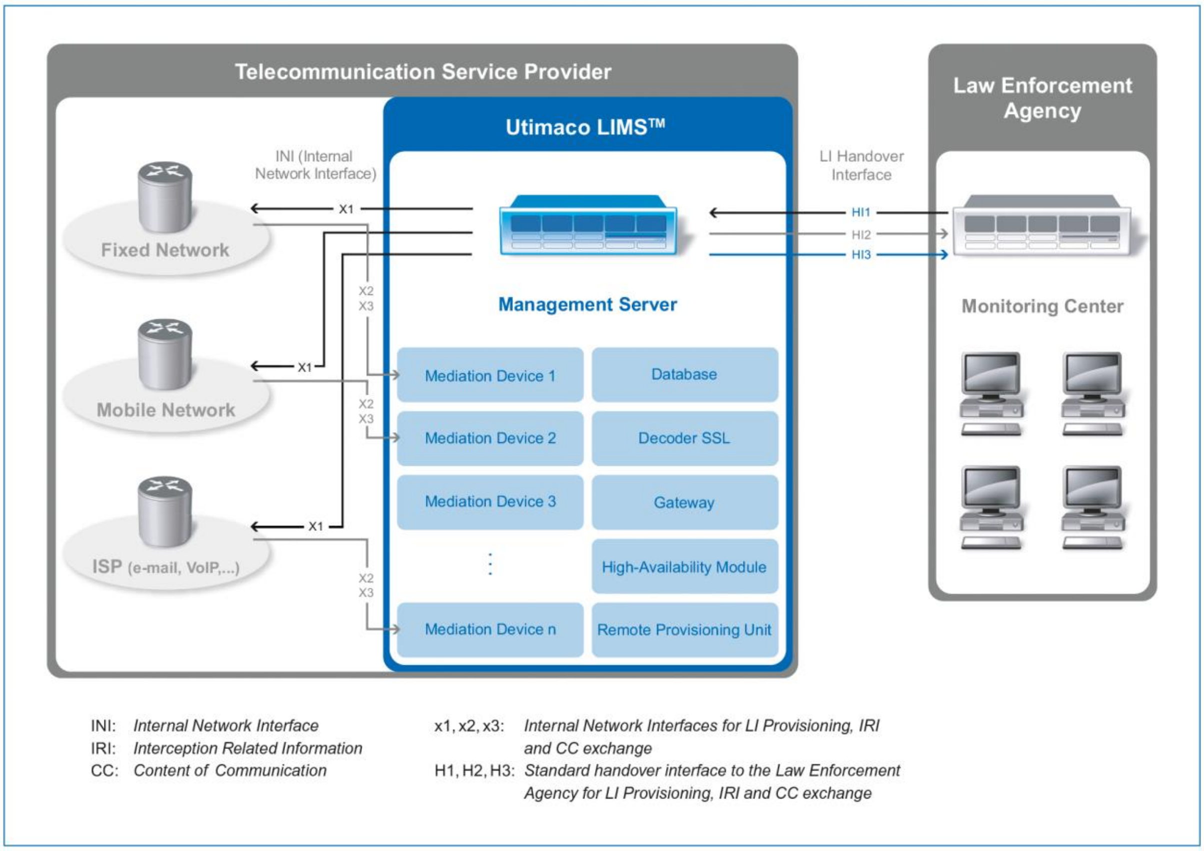
Telecommunication Service Provider
Utimaco LIMS™
Law Enforcement Agency
INI (Internal Network Interface)
LI Handover Interface
Fixed Network
Mobile Network
ISP (e-mail, VoIP,...)
X1
X2
X3
HI1
HI2
HI3
Management Server
Monitoring Center
Mediation Device 1
Mediation Device 2
Mediation Device 3
Mediation Device n
Database
Decoder SSL
Gateway
High-Availability Module
Remote Provisioning Unit
INI: Internal Network Interface
IRI: Interception Related Information
CC: Content of Communication
x1, x2, x3: Internal Network Interfaces for LI Provisioning, IRI and CC exchange
H1, H2, H3: Standard handover interface to the Law Enforcement Agency for LI Provisioning, IRI and CC exchange

*Figure 2: Elements of LIMS*

Several individual communication modules – depending on the number of network elements with monitoring capabilities – manage the data retrieval from fixed networks, mobile networks, and ISP infrastructures. Administrative tools are consolidated in a centralized, easy-to-use graphical interface that provides monitoring of system actions and collection of monitoring results. The implementation supports three different approaches to interception – active, passive, and hybrid.

For each type of network element, at least one communications module exists. This modular approach to the architecture provides a significant amount of flexibility and scalability to LIMS. Additional network elements can be added easily as required and as the monitoring network grows as the number of monitored network elements increases. As performance requirements grow, the communication modules can be distributed among multiple servers to better balance the workload. The modular architecture lets Utimaco more efficiently manage and monitor various kinds of networks and services, ranging from fixed voice and data networks to mobile networks and beyond. Utimaco LIMS currently supports over 100 different network elements and continues to develop new IAPs – those network elements that include specific interception capabilities or dedicated tap filters – to respond to emerging communications technologies.

## 4.2 Interception Types: Active, Passive, and Hybrid

When using active interception, the IAP represents a physical component of a network element, such as Serving GPRS Support Node (SGSN) in a mobile network or Broadband Remote Access Server (BRAS) in a fixed IP network. LIMS retrieves the interception data – consisting of metadata and content – directly from one or more of the network elements, as shown in Figure 3. In this case, the network element must at least support basic LI capabilities. The effectiveness of this form of interception depends on the modular design features of LIMS and the interoperability with third-party equipment vendors. Utimaco performs comprehensive testing to maximize interoperability throughout the range of vendor products.

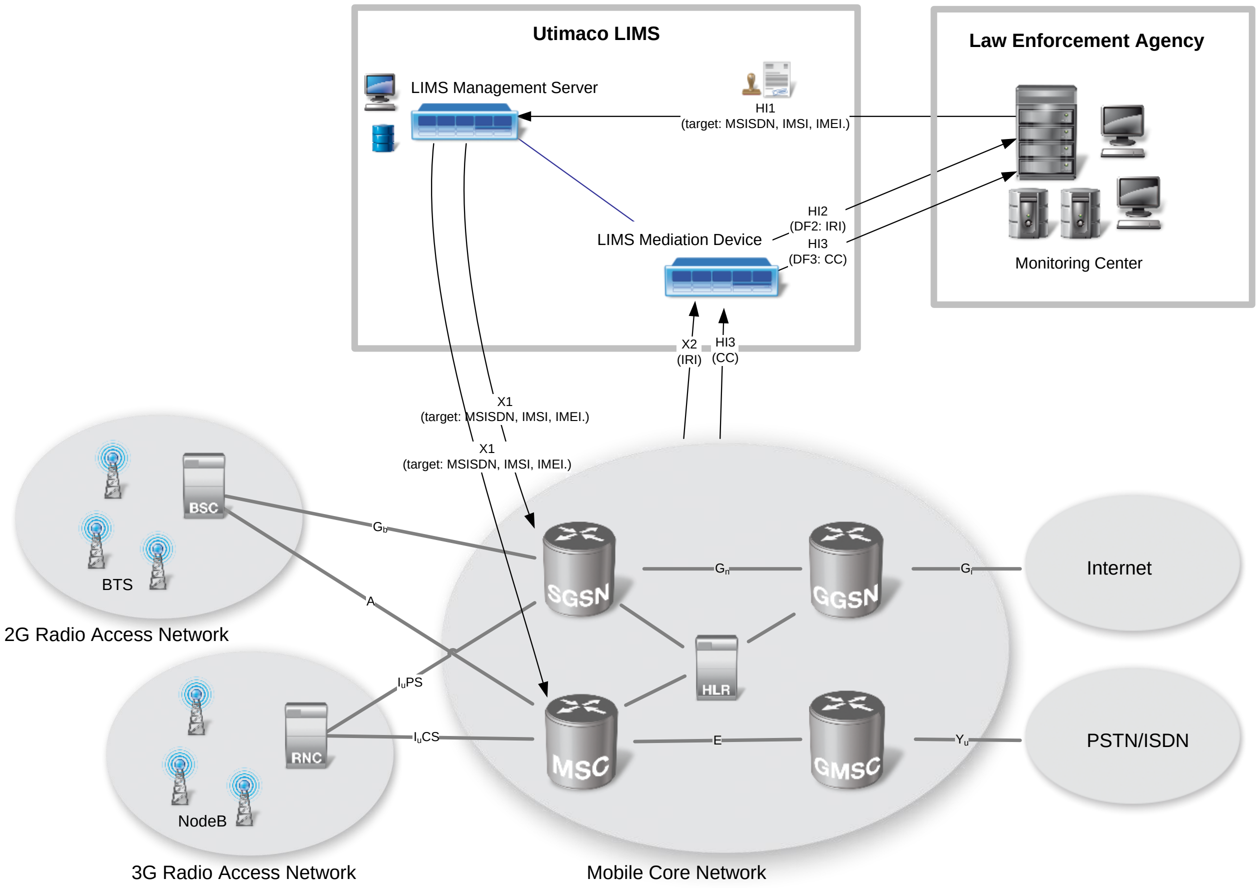

*Figure 3: Active Interception*

Active interception offers the following benefits.

- Inexpensive to implement: If the network elements have basic interception or filtering capabilities, this approach can be very cost effective.
- Minimal hardware requirements: In most instances, no additional hardware is required.
- Fast deployment: Active interception capabilities can generally be deployed very quickly.
- High availability: As a component of the operational network, availability of active interception can be easily handled.

The most significant disadvantage to active interception is that some network elements do not have interception capabilities. Furthermore:

Active interception can have a negative impact on the performance of the network element that executes the interception function.

At high throughput levels, the network element (e.g. router) can lose packets on the interception port.

When using passive interception, the IAP is a separate network element that is managed by LIMS; this is transparent to the operator network. The passive IAP filters, decodes, and delivers the intercepted metadata and content to the LIMS, as shown in Figure 4. Passive interception operates on a copy of the network traffic and it is completely transparent. This makes it impossible for the target to detect any interception activities on the service.

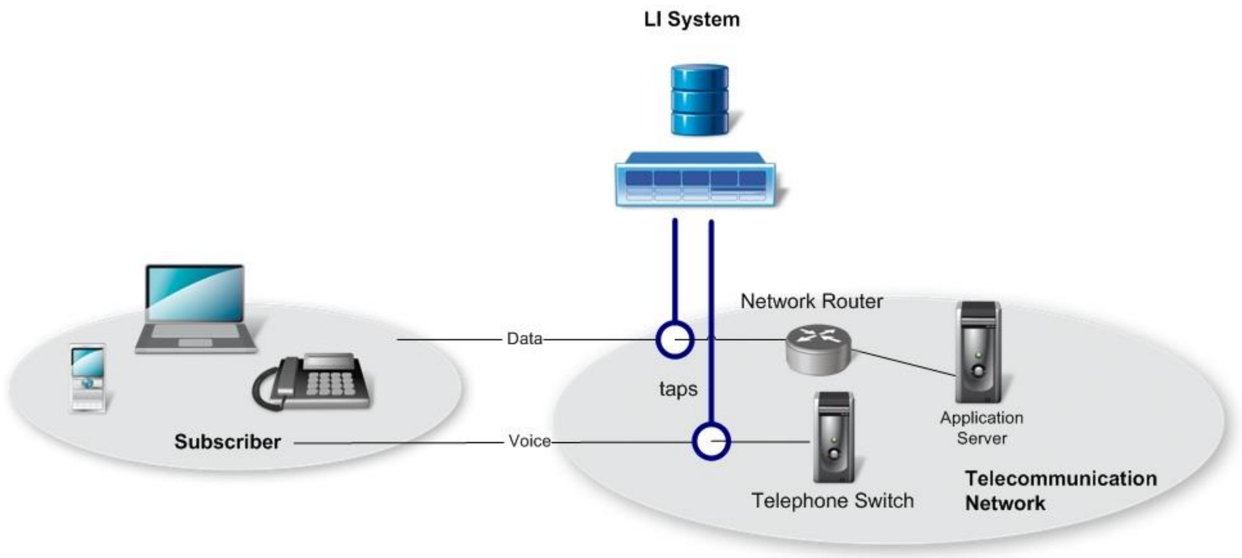

*Figure 4: Passive Interception*

Passive interception offers the following benefits.

- Flexibility: In most circumstances, passive interception can be used with any network and any service.
- Independent operation: Passive interception remains independent from the access network.
- Transparency: Operations during passive interception are completely transparent to the user and the rest of the network; all interception and filtering activities are performed on a copy of the data traffic.
- No performance impact: The passive interception model does not impact network performance in any way, nor does it intrude on the reliability or availability of network resources.
- High availability: As a component of the operational network, availability of active interception can be easily handled.

Passive interception presents these disadvantages.

- Additional cost: Because additional hardware and software are required, passive interception adds to the cost of a LI solution.
- Performance considerations: The IAP hardware has finite performance limitations that must be factored into the solution design.
- Coverage limitations: Certain types of services cannot be easily handled using filters.

Hybrid interception combines the best of both worlds, incorporating active and passive interception techniques. The hybrid approach is becoming increasingly common in today's diverse network architectures and extensive service platforms. For example, in IP networks someone can probe for user credentials to detect the IP address of a particular user. Once the user's IP address is known, an IP router can relay (respectively copy) specified traffic to or from the IP address to the interception system, where it can be directed to the monitoring Center. Depending on the nature of the network infrastructure and the type of services to be monitored, sometimes hybrid interception is the only viable solution.

As metadata (IRI) and communication content (CC) might be captured at different points in the network, LIMS assigns unique message tags to both IRI and CC. This lets a monitoring center easily correlate the information after receipt. Figure 5 illustrates the principle concept of a hybrid interception solution at an example for VoIP.

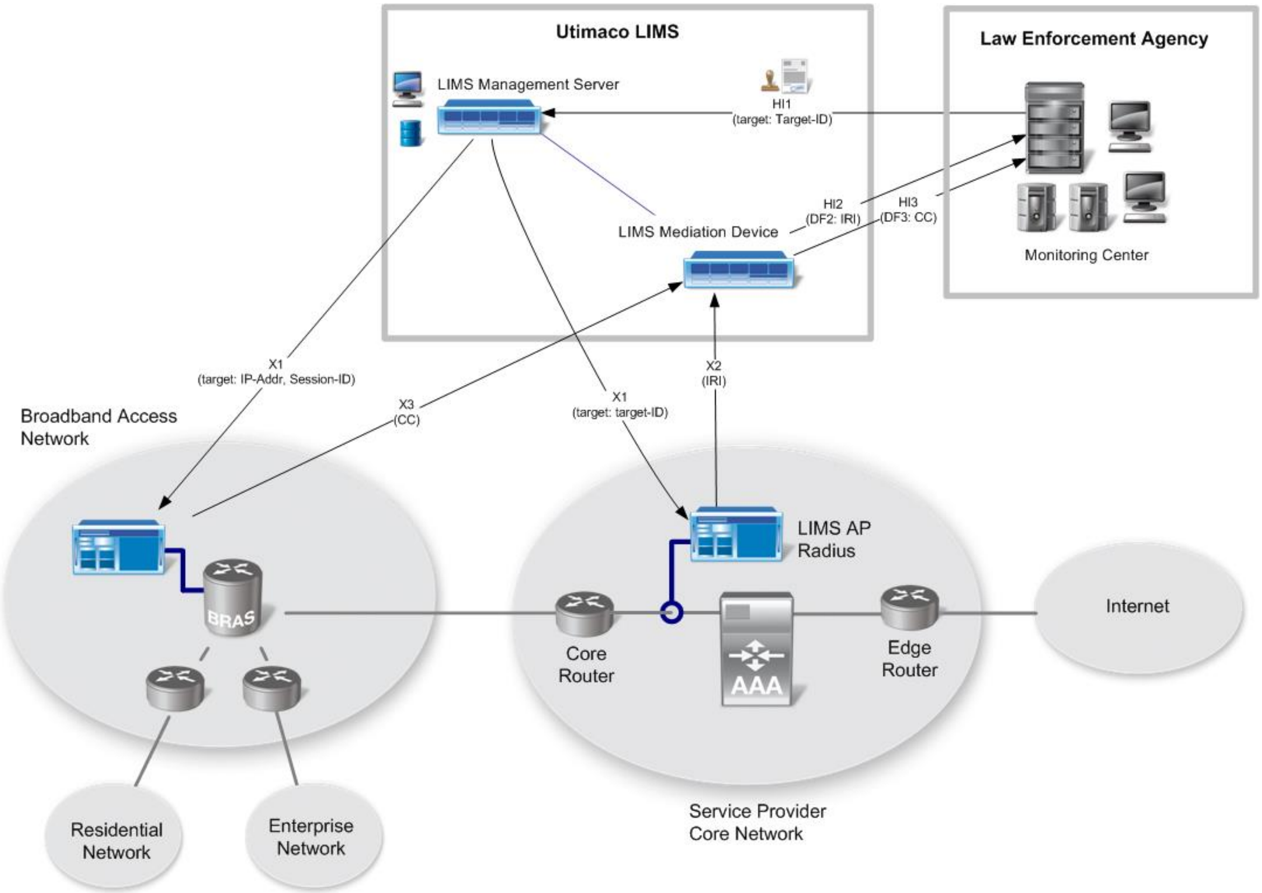

*Figure 5: Hybrid interception*

## 4.3 Functional Operation of LIMS

LIMS separates the functional elements of solutions into three fundamental areas:

- Administration
- Node management and data collection
- Mediation and delivery

Figure 6 provides an overview of the tasks that are handled in each of these functional areas.

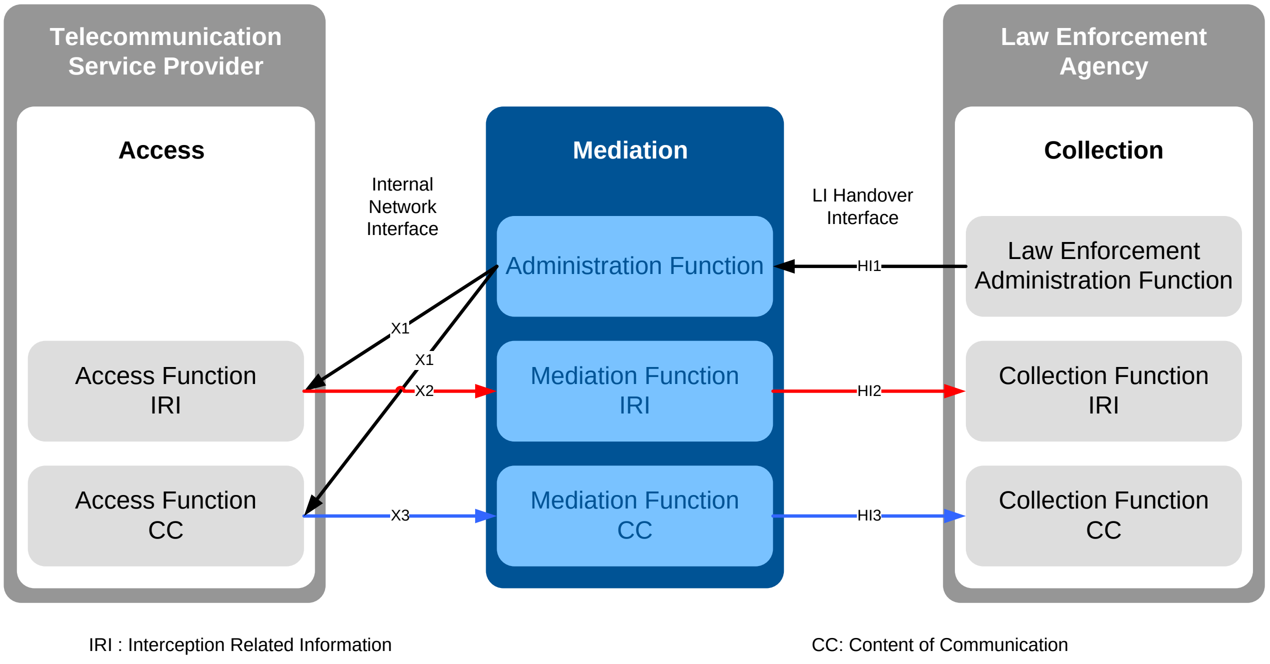

*Figure 6: LI Functions*

## 4.4 Benefits of LIMS

LIMS provides a cost-effective, comprehensive lawful interception solution that simplifies the setup and maintenance tasks for service providers and network operators while providing the security, privacy, and reliability that Utimaco customers have come to expect. LIMS provide these key benefits.

- Ease of operation: One centralized management system for all services with user-friendly administrative interface simplifies use in heterogeneous networks.
- Compliance and interoperability: The solution provides strong multi-vendor support capabilities and proven compliance with international and national laws and standards.
- Scalability: The modular architecture of LIMS scales to support complex, high-volume data surveillance operations.
- Quality support: All LIMS deployments are backed by the capable expertise of the Utimaco customer support team.
- High security and reliability: Designed for demanding applications, LIMS relies on the experience and proven technologies that Utimaco has delivered in the security realm since 1983.

## 4.5 Summary

The challenges faced by network operators and service providers are best met by LI solutions that have been developed according to the most pressing demands of the industry. The Utimaco LIMS solution addresses the predominant challenges in the industry in a number of ways. The volume of data traffic that must be monitored and filtered is growing worldwide – and the scalable LIMS architecture is well equipped to meet bandwidth requirements. As the number of telecommunications services increases and new types of services are introduced, the flexible, modular design architecture of LIMS adapts to changing technologies. Utimaco's active participation in national and international standards bodies puts the company in an excellent position to respond to the changing regulatory environment and provide cooperation to the appropriate regulatory agencies. With robust support for the full range of industry-proven interception techniques – including active, passive, and hybrid – the LIMS solution integrates easily into diverse network infrastructures with minimal deployment and maintenance requirements. The solidly established credentials of Utimaco in the security realm make it possible to effectively mediate the concerns of the network operators and ISPs against the requirements of the LEAs and regulatory agencies, providing a solution that delivers compliance while ensuring positive authentication, data protection and privacy, and exceptional accountability throughout every aspect of its operation.

# 5 Additional Resources

For more information about Utimaco and Lawful Interception solutions, visit www.utimaco.com/LIMS. The following tables give an overview of some of the most relevant interception laws and standards that apply in various countries.

Note: While the information in these tables has been carefully collected and reviewed, these tables may not be complete.

## 5.1 Interception Laws

| | |
|---|---|
| United States | Omnibus Crime Control and Safe Streets Act of 1968. |
| | Electronic Communications Privacy Act of 1986 (ECPA). |
| | USA Patriot Act, 2001. |
| | Communications Assistance for Law Enforcement Act, 1994 (CALEA). |
| | Foreign Intelligence Surveillance Act (FISA) of 1978. |
| Canada | Criminal Code (R.S. 1985, c. C-46 ). An Act respecting the Criminal<br>Law (Part VI, Invasion of Privacy; Part XV, Special Procedure and Powers). |
| Japan | "Law authorizing interceptions of telecommunications in crime investigations" (Law No. 137, 1999) (Communication Interception Act (CI-Act)). |
| | "Code of Criminal Procedure – CCP." |
| France | Loi n° 91-636 du 10 juilliet 1991 relative au secret des correspondances émises par la voie des télécommunications. |
| | Décret n° 93-119 du 28 janvier 1993, Décret relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991. |
| Italy | Intercettazioni di conversoni o communicazione, Art. 266 – 271, Code di Procedura Penale, 1988. |

| | |
|---|---|
| | Decreto del presidente della repubblica del 19 settembre 1997, n. 318: Regolamento per l'attuazione di direttive comunitarie nel settore delle telecomunicazioni. |
| United Kingdom | Regulation of Investigatory Powers Act 2000 (RIPA). |
| | The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002. |
| Russia | SORM I+II (Sistema Operativno-Rozysknykh Meropriyatii), 2000. |
| Germany | Telecommunications Act (TKG), 2004. |
| | G10 Law, 2001. |
| | Strafprozessordnung (StPO), 2002. |
| | Gesetz über das Zollkriminalamt und die Zollfahndungsämter, (Zollfahndungsdienstgesetz - ZFdG), 2002. |
| | Telekommunikationsüberwachungsverordnung (TKÜV), 2005. |
| The Netherlands | Tijdelijke regeling aftappen openbare telecommunicatienetwerken en – diensten, 1998. |
| | Telecommunications Act 1998. |

## 5.2 Interception Standards

| | |
|---|---|
| ETSI, EU | ETSI TS 101 331, Requirements of Law Enforcement Agencies |
| | ETSI ES 201 158, Requirements for Network Functions |
| | ETSI TS 101 671 / ETSI ES 201 671, Handover Interface for the Lawful Interception of Telecommunications Traffic |
| | ETSI TR 102 053, Notes on ISDN LI functionalities |
| | ETSI TR 101 943, Concepts of Interception in a Generic Network Architecture |
| | TS 102-232-1Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 1: Handover specification for IP delivery |
| | TS 102-232-2Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 2: Service-specific details for E-mail services |
| | TS 102-232-3Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 3: Service-specific details for internet access services |
| | TS 102-232-4Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 4: Service-specific details for Layer 2 services |
| | TS 102-232-5Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 5: Service-specific details for IP Multimedia Services |
| | ETSI TS 101 909-20-1/2 IP Multimedia Time Critical Services; LI for Services related to E.164 Voice Telephony, LI for streamed MM services |
| | ETSI EN 301 040, Terrestrial Trunked Radio; Lawful Interception interface (TETRA) |
| ATIS, US | T1.678 |
| ATIS | T1.724, ATIS-1000013.2007 LAES for IAS |
| ATIS-TIA, US | J-STD-025, J-STD-025-A, J-STD-025-B |
| PacketCable, US | PacketCable 1.5: Electronic Surveillance, PKT-SP-ESP1.5-I01-050128 |
| | PacketCable 2.0: Electronic Surveillance Intra-Network, Specification, PKT-SP-ES-INF-I01-060406 |

| | |
|---|---|
| 3GPP | TS 33.106, TS 33.107, TS 33.108 |
| ITU-T | IPCableCom, Project on time-critical interactive services over cable television network using IP-protocol, in particular Voice and Video over IP |

# 6 Glossary and Abbreviations

| | |
|---|---|
| 3GPP | The 3rd Generation Partnership Project (3GPP) is a co-operation between ETSI (Europe), ARIB/TTC (Japan), CCSA (China), ATIS (North America), and TTA (South Korea). www.3gpp.org |
| AAA | Authentication, Authorization, Accounting |
| ANSI | American National Standards Institute. www.ansi.org |
| BRAS | Broadband Remote Access Server aggregates the output from DSLAMs |
| BSC | Base Station Controller, a subsystem in a GSM mobile phone network |
| BTS | Base Transceiver Station, a GSM base station |
| CALEA | Communications Assistance for Law Enforcement Act (CALEA), U.S. Law |
| CC | Communication Content |
| CDMA | Code division multiple access, common 2G mobile network technology in the United States, Australia, and other countries |
| ETSI | European Telecommunications Standards Institute (ETSI). www.etsi.org |
| IAP | Interception Access Point, point in the network where the interception takes place |
| IRI | Interception Related Information, the metadata related to a communication service, e.g., call detail records, call set-up time, caller-id, e-mail address |
| LI | Lawful Interception |
| LIMS | Lawful Interception Management System |
| MSC | Mobile Switching Center, part of a GSM network |
| SGSN | Serving GPRS Support Node, part of a GSM network |
| UMTS | Universal Mobile Telecommunications System (UMTS) is one of the third-generation (3G) mobile phone technologies |

# 7 About Utimaco

Since 1994 Utimaco has been developing lawful interception and data retention systems for telecom operators and Internet service providers. Utimaco's carrier-grade systems enable real-time monitoring and long term data retention in public telecommunication networks. The systems interface with essentially all common network technologies and communications services. Utimaco is the preferred partner of many of the world's leading network equipment manufacturers. With around 250 installations in over 80 countries, Utimaco is a leading global supplier in the Lawful Interception and Data Retention market. Utimaco participates in LI standardization and supports international standardization institutes and telecom associations, such as, ETSI, 3GPP, ANSI/ATIS, and Bitkom.

Customers and partners value the reliability and long-term investment security of the Utimaco security solutions. Utimaco stands for recognized product quality, user-friendly software, excellent support, and products that effectively meet market requirements.

For more information visit www.utimaco.com

Utimaco TS GmbH
Germanusstr. 4
52080 Aachen
Germany
Phone: +49 (241) 1696-0
Fax: +49 (241) 1696-199
li-contact@utimaco.com
www.utimaco.com