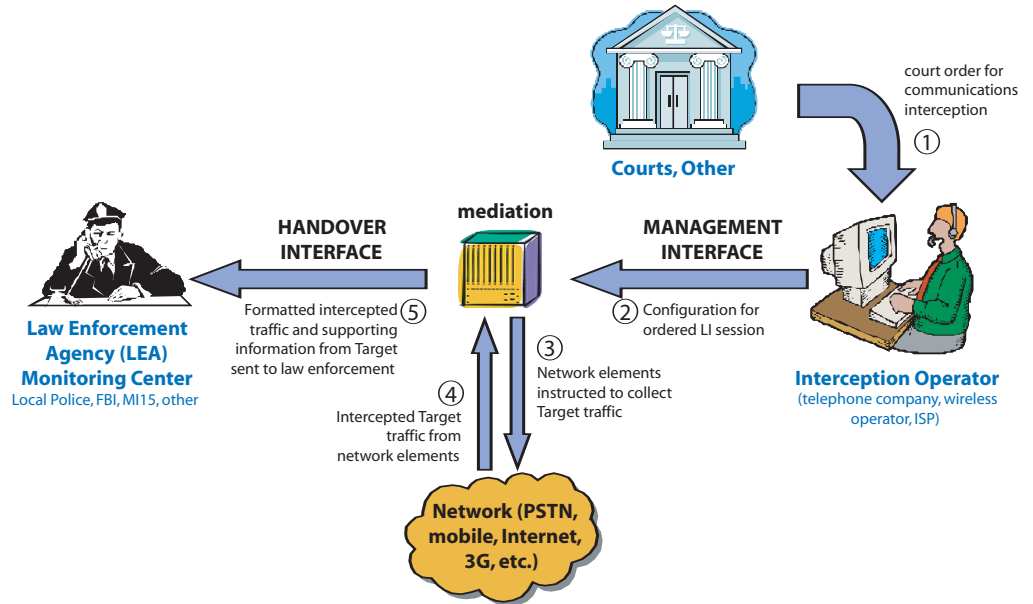


## STANDARDS-BASED LAWFUL INTERCEPTION FROM AQSACOM

Lawful Interception (LI) throughout the Western World is characterized by the process depicted in the following figure. The standards-based LI process involves an interplay between the **Courts**, who authorize the interception; the **Network Operator**, who performs the interception under highly secure conditions; and the **Law Enforcement Agency (LEA)**, who monitors the interception and gathers the interception data as evidence to be used in a legal action.



Aqsacom plays a vital role in the standards-based LI process by providing the mediation management platform to facilitate the LI procedures. Mediation performs a multi-fold purpose. In particular, Aqsacom's standards-based mediation management system:

- configures key equipment within the public communications network to intercept the telephone or internet traffic of the target subject(s);
- provides a common interface between the LEA and network operator, regardless of the types of equipment in the network and for a wide range of supported services (fixed line telephone, mobile telephone, internet and internet applications, mobile data, 3G, etc.) – this greatly simplifies the work of the LEA in monitoring interception traffic;
- enables the network operator to invoke the interception through an easy-to-use, common user interface that interoperates with the diversity of services that the operator might offer;
- future-proofs both the network operator and LEA as new services come on line in response to market demand.

Aqsacom's comprehensive approach to LI adheres to established LI standards and many other requirements, as presented in the following diagram. We now discuss the parts of this diagram in more detail.

On the standards front, the European Telecommunications Standards Institute (ETSI), 3GPP, and other organizations worldwide propose three *handover interfaces* for managing the interception data between the network operator and law enforcement agencies. Here the interception instructions are conveyed to the Aqsacom system through Handover Interface Hi1; Hi2 and Hi3, respectively, convey the data describing the interception (e.g., number dialed, email address sent to, time of call, etc.) and content of the call / message from the network operator to the LEA via the Aqsacom system.

Alarms from equipment and services			Access & Transmission Security By equipment	Fault Tolerance By equipment	Disaster Recovery By solution
Statistics by equipment and services; LEA invoicing					
Enhanced Hi1 By service	Enhanced Hi2 By service	Enhanced Hi3 By service			
ETSI/3GPP specifications					





AQSACOM develops and markets real time Lawful Interception, Mobility Tracking and Surveillance solutions. With its core business focused on lawful interception and related applications for over eleven years, AQSACOM provides end-to-end turnkey solutions for fulfilling lawful interception requirements anywhere in the world, especially over highly heterogeneous networking and services environments. AQSACOM's diversified customer portfolio includes clients from more than 30 countries, covering geographical areas as diverse as Central and Eastern Europe, Asia-Pacific, North America, Africa and the Middle-East.



## Enhanced Lawful Interception:

As the deployment and market acceptance of communications services evolve, the interception requirements of traffic originating from these services must also evolve. Such is especially the case with the many applications based on Internet Protocol (IP), including Voice-over-IP, email, instant messaging, etc. Comprehensive LI needs to account for the interception of critical information generated by these applications. Examples of such LI information include identification of parties that communicate through instant messaging, precise location of the different phases of a mobile call, identification of what users downloaded what streaming files from an illicit source, where a subject using a Web-based email application sent an email, etc. Aqsacom refers to these data as Enhanced Interception Related Information (IRI), to be distinguished from the standards-based IRI.

## Security, Confidentiality, Integrity, Authentication, Non-Repudiation:

Due to the nature of LI, security must be taken very seriously to preserve the privacy of the target and the confidentiality of the investigation. Aqsacom therefore adheres to secure standards at the:

- **Access and delivery level** in the conveyance of interception data and content to the LEA. Here secure information flow is assured through standards-based strong authentication, confidentiality, integrity, and non-repudiation. These standards are applied over private dedicated circuits, switched data circuits (ISDN), and secure VPNs through the use of IPSec and TSL. In addition, secure information flow must be assured between the mediation system, the interception operator, and network elements by using strong authentication for access to any part of the network.
- **Equipment level.** Aqsacom assures tight control of all data on the hard disk through encryption of all log and buffered interception data. Access to the mediation management system is controlled through strong password protection and optional biometric means. All hardware conforms to standards-compliant, tamper-proof design.
- **Maintenance level.** Aqsacom applies very strict intervention procedures to guarantee that no confidential information can be extracted from the mediation management platform or its components. Furthermore, operational maintenance procedures must not allow administrators to access any interception of confidential data. Even the mediation system's vendor cannot access the interception data during debugging, repair or upgrade – in short, no "back door" access to the interception data is permitted.

All actions and events that take place within the mediation platform must be logged to conform to traceability requirements. Finally, the mediation software should be certified virus-free and delivered to the network operator in an authenticated format (e.g., with a secure hash).

## Fault Tolerance:

Aqsacom assures continuous interception operations regardless of equipment, network, or system fault. Equipment fault tolerance is assured through duplicated platform components (e.g, RAID arrays for the disk storage, RAM redundancy, back-up CPUs that reside on-line, and hot swappable hardware components). Network faults are mitigated through ample hard disk buffering of intercepted data and content. System-level fault tolerance is assured through Aqsacom's replicated system approach, where multiple mediation platforms can operate simultaneously on line to share the interception process loading and support one another in the event of the failure of any one system.

## Disaster Recovery:

Aqsacom supports a comprehensive solution for disaster recovery to ensure continuous interception operations in the event that a complete interception facility becomes incapacitated due to a catastrophic event (war, terrorism, natural disaster) or more mundane causes (electric and/or communications line breaks, local fire). The solution calls for a rapid transition to a fully functioning interception facility with replicated interception capabilities. In local disaster recovery, downed mediation systems can be restored or rebuilt through a step-by-step process that implements a recovery CD.

## Statistics Collection and Alarms:

Information is continuously gathered to keep network operators and the LEA apprised of the demands on the interception system and to ensure that load factors are in conformance with expected service. In the event of equipment or network failure, the network operator and LEA are immediately notified by the Aqsacom system through alarms locally and remotely.

[www.aqsacom.com](http://www.aqsacom.com)

email: [sales@aqsa.com](mailto:sales@aqsa.com)

AQSACOM Americas  
Washington, DC  
Tel: +1 202 315 3943

AQSACOM Europe  
Paris  
Tel: +33 1 6929 8400

AQSACOM Asia  
Melbourne, Australia  
Tel: +61 3 9909 72 80