

Streamlining Lawful Intercept for WiMAX Networks

- ▶ Meet stringent lawful intercept requirements for monitoring WiMAX IP-based voice, data and multimedia traffic
- ▶ Comply with lawful intercept regulations and standards securely and cost effectively, without alerting subscribers or disrupting service



THE MOBILE PERSONALIZATION COMPANY

Introduction

Communications operators across the globe must comply with a complex array of local, national, and regional lawful intercept (LI) standards and regulations. Moreover, as communication technologies and services continue to evolve, these standards and regulations evolve too, creating an increasingly heavy burden for operators, and the potential to disrupt quality of service and derail core business operations.

The advent of IP-based communications makes compliance even more challenging, as it becomes increasingly difficult to keep track of subscriber identities, as the data flow to and from a subscriber is distributed across packets that are independently routed through the network. Mobility adds yet another layer of complexity because subscribers can connect to the network from any location and, when roaming, to networks owned by other operators.

Given these challenges, WiMAX™ operators face a difficult LI compliance environment as they strive to implement LI solutions that are at once robust and cost-effective and that minimize the impact on network performance and operations.

This paper outlines the LI requirements for WiMAX and describes how WiMAX operators can meet these requirements using a Lawful Intercept solution provided by Bridgewater Systems in partnership with industry-leading lawful intercept vendors. The solution is fully integrated within the WiMAX operator's network and provides broad interoperability with network elements from other vendors.

What Is Lawful Intercept?

LI allows Law Enforcement Agencies (LEAs) to intercept voice and data traffic generated by or directed to a subscriber, regardless of the access technology used. Typically, the LEA sends a request to the operator to monitor both session data (information about the connection) and session traffic (the actual IP stream) that relate to a specific subscriber.

While the goals of LI are the same across countries, requirements and interface specifications vary. Operators need to adopt a solution that complies with local regulations. Where LI is mandatory, they have to monitor different types of traffic (e.g., voice, data, or multimedia) and services (e.g., including multicast and broadcast, where the same traffic flow is directed at multiple subscribers). Furthermore, interception has to cover traffic generated by both the operators' on-network subscribers, and subscribers visiting (roaming) from other networks.

LI operations have to be implemented in a way that does not affect network performance for intercepted subscribers to ensure that subscribers are unaware they are being targeted. All network traffic has to be accessible to LI, even though only a very small fraction of these records are sent to the LEA. As a result, it is crucial for operators to minimize the impact on the overall network performance due to LI.

Value Proposition for WiMAX Operators

- ▶ Access to subscriber communications without alerting subscribers or disrupting service in compliance with ETSI, CALEA, and local lawful intercept mandates
- ▶ Streamlined compliance with a rapidly expanding array of lawful intercept regulations and standards
- ▶ Integrated solution that leverages existing elements of WiMAX access and core networks
- ▶ Correlation of IP streams to the subscriber and support for mobility and roaming
- ▶ Support for any traffic type (voice, data, multimedia) and application
- ▶ Operators free to retain focus on revenue-generating services
- ▶ Future support of devices supporting multiple air-interfaces

What Is Special About WiMAX?

As a technology that combines a native IP core and support for mobility, WiMAX—as well as emerging fourth-generation (4G) technologies—presents significant lawful intercept challenges.

In fixed or cellular voice networks, LI is relatively straightforward as the phone number uniquely identifies the subscriber. In IP-based WiMAX networks, traffic is user agnostic and this one-to-one relationship disappears.

WiMAX subscriber traffic is linked to IP addresses that typically are set for a given session, but change over time. Subscribers may be randomly assigned a pseudo-identity during the authentication process. To ensure effective traffic monitoring, the traffic linked to this pseudo-identity has to be identified.

As a result, LI requirements are more difficult to meet within WiMAX and, more generally, IP networks. Control data and session content have to be intercepted at different locations within the network to ensure that all traffic associated with the targeted subscriber can be reliably attributed to that subscriber, regardless of application type, service type, or access location.

Bridgewater Systems Integrated Solution For WiMAX Operators

Bridgewater Systems has developed an innovative approach to LI that targets the specific requirements of WiMAX operators in cooperation with its LI partners which intercept traffic from the WiMAX operator and transmit it to the LEA. The Bridgewater solution provides robust LI for all types of traffic and applications in any IP environment that supports mobility.

Bridgewater understands the challenges that WiMAX operators face in combining affordable service with a high-quality subscriber experience. As a result, the Bridgewater solution has been developed to work seamlessly in existing networks alongside equipment from any other vendor they choose, as long as it complies with WiMAX Forum® specifications.

The solution allows operators to meet all of their LI requirements by ensuring that LEAs can intercept all IP streams—voice, data, multimedia—at a point in the network where they can be uniquely associated with the subscriber. Depending on traffic type, core network components, and regulation, the network locations where IP streams can be assigned to the subscriber may differ.

How Does It Work?

Bridgewater works in partnership with several Lawful Intercept vendors to provide an end-to-end LI solution. The Bridgewater components of the solution manage all the activities required to identify subscribers targeted by law enforcement agencies for surveillance.

Bridgewater's LI partners provide the Lawful Intercept Delivery and Collection Functions defined by the LI standards. These partner systems rely on Bridgewater to pass them the information that uniquely identifies the subscriber, which in turn enables them to deliver the content of the subscriber's intercepted communications to the appropriate law enforcement agencies.

The solution is responsible for receiving incoming LI requests, determining when a target subscriber is online, and providing the subscriber's unique identification information to the partner system responsible for the LI Delivery Function. This information includes the subscriber's IP address as well as the address of the network element to which the subscriber is connected (such as an ASN gateway or Home Agent).

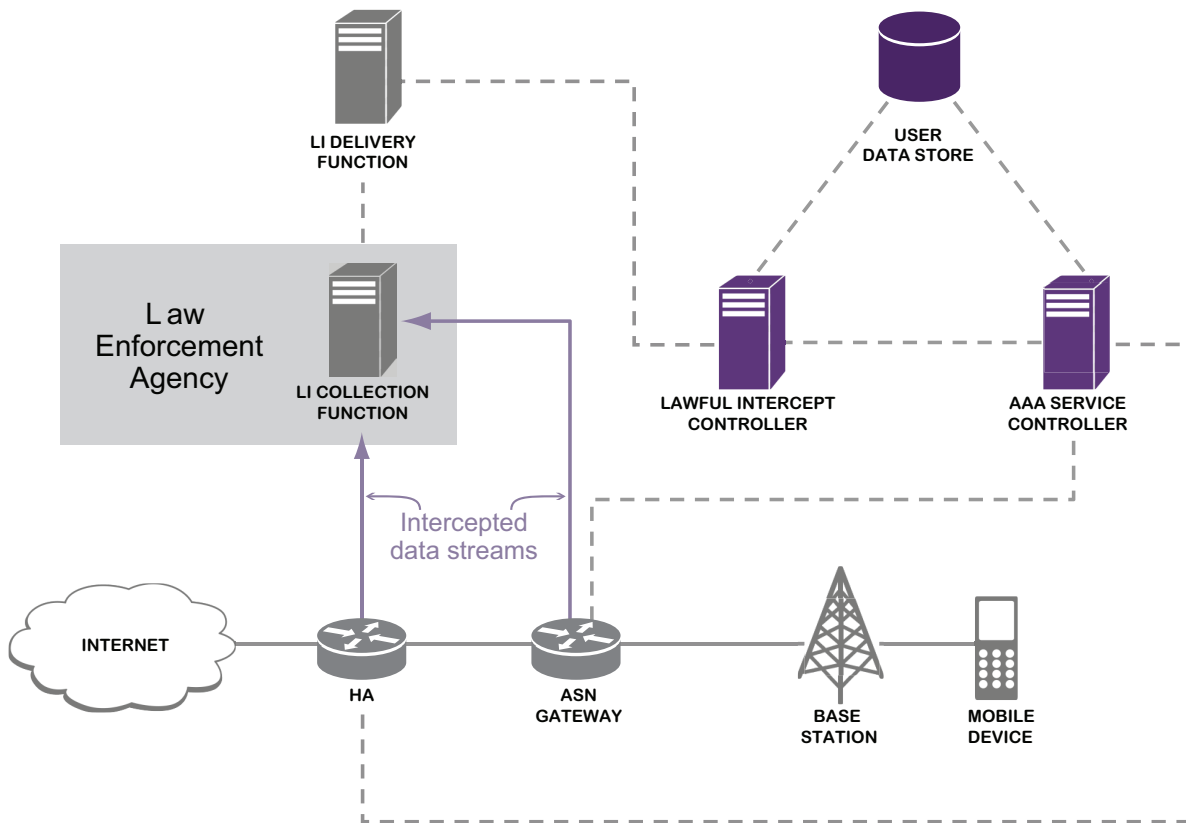


Figure 1: The Bridgewater Systems Lawful Intercept Architecture for WiMAX.

The solution employs three core product elements for performing these functions: the Bridgewater® Service Controller (AAA), the LI Controller, and Bridgewater's Subscriber Data Broker™.

The Service Controller translates the subscriber's pseudo identity, which is used by WiMAX to identify the subscriber, to the real identity of the subscriber contained in LI requests. When the Service Controller receives accounting records from the ASN gateway, it performs this translation before passing the records on to the LI Controller.

The LI Controller is a scalable and robust server that securely stores and maintains all of the information on surveillance targets for on-network subscribers and inbound roaming users. When the LI Controller is notified of a new subpoena, it first queries the Subscriber Data Broker state database to determine if the targeted subscriber is currently online. The state database keeps a record of every authenticated subscriber for the duration of the subscriber's session. If there is an entry in the database for the targeted subscriber, the LI controller sends the subscriber's IP address and the IP address of the ASN gateway and/or home agent to the Delivery Function.

If the LI Controller does not locate an entry for the subscriber in Subscriber Data Broker, it means that the subscriber is not currently online. In this case, the LI Controller continuously monitors subscriber authentications to determine when the targeted subscriber starts a new session on the network and then sends the relevant information to the Delivery Function.

Extending Lawful Intercept To Mobile And Roaming Traffic

Support for roaming and mobility adds further complexity to the interception of IP traffic. The WiMAX subscriber may connect from anywhere in the network and move across locations covered by different base stations (or base station sectors). When roaming, the subscriber will establish a connection within the area covered by another operator. In cellular networks, roaming is mostly confined to international traffic generated by subscribers traveling abroad. Roaming in WiMAX networks may become more prevalent in domestic settings if regional operators enter roaming agreements to ensure national coverage.

The Bridgewater solution enables WiMAX operators offering mobile access to correlate IP streams from multiple base stations, even if they are managed by different ASN gateways. When the subscriber connection is handed over to a base station associated with a different ASN gateway, the solution relies on actively acquired session data from the Bridgewater LI Controller to correctly track when the subscriber connects to the network.

Roaming brings a separation of network operator and service provider. The subscriber has a contract with the operator, but may also connect to networks managed by other operators. Interception typically takes place on the visited network managed by a network operator other than the subscriber's operator.

A roaming subscriber's traffic has to be intercepted within the visited network, before it leaves the ASN, because the IP traffic generated by a roaming subscriber typically reaches the Internet without passing through the home network. It is not available to the home operator, and therefore it is the visited network operator that has to submit it to the LEA.

To intercept the traffic of a roaming subscriber, the home operator forwards the LI request initially received from the LEA to the visited network operator. With the Bridgewater solution, the visited network operator can capture the subscriber traffic using the same approach used for non-roaming, on-network subscribers.

Conclusions

WiMAX enables operators to offer their subscribers true broadband connectivity in fully mobile, all-IP networks. IP traffic and mobility bring improved performance and flexibility to operators, but they also make it more challenging to comply with LI requirements, as the association between traffic flows and subscribers becomes more difficult to establish.

In selecting an LI solution, operators need to meet two equally important requirements.

- ▶ The first requirement for WiMAX operators is to select an LI solution that meets their specific regulatory requirements for all traffic types that they carry (voice, data, multimedia) and that can do so in both fixed and mobile (including roaming) usage scenarios.
- ▶ The second requirement is to ensure that the solution they have selected seamlessly integrates into their network in a cost-effective way, minimizing the impact on network performance and operations.

Bridgewater has developed a powerful integrated LI solution based on its in-depth understanding of the interworking of WiMAX core network elements, and of the LI and business model requirements of WiMAX operators.

The Bridgewater LI solution allows WiMAX operators to meet both requirements and retain their focus on revenue-generating services.

Bridgewater Systems, the mobile personalization company, enables service providers to efficiently manage and profit from mobile data services, content and commerce. The company's market leading mobile personalization portfolio provides a real-time, unified view of subscribers including entitlements, devices, networks, billing profiles, preferences and context. Anchored by Bridgewater's Subscriber Data Broker™, the portfolio of carrier-grade and standards-based products includes the Bridgewater® Service Controller (AAA), the Bridgewater® Policy Controller (PCRF) and the Bridgewater® Home Subscriber Server (HSS). More than 120 leading service providers including America Movil, Bell Canada, Clearwire, Cox, Hutchison Telecom, Iusacell, Scartel, SmartTone-Vodafone, Sprint, Tata Teleservices, Tatung, Telmex, Telstra, and Verizon Wireless use Bridgewater's solutions to rapidly deliver innovative mobile services to over 150 million subscribers. For more information, visit us at www.bridgewatersystems.com.

Bridgewater Systems

Bridgewater, Bridgewater Systems, the Bridgewater Systems logo, WideSpan, Smart Caps, myPolicy, and Subscriber Data Broker are trademarks or registered trademarks of Bridgewater Systems Corporation.

All other company, product names and any registered and unregistered trademarks mentioned are used for identification purposes only and remain the exclusive property of their respective owners.

www.bridgewatersystems.com

Company Headquarters

303 Terry Fox Drive
Suite 500
Ottawa, Ontario
Canada K2K 3J1

P: +1 613 591 6655
F: +1 613 591 6656

European Office

Albany House
324/326 Regent Street,
Suite 404, London,
United Kingdom W1B 3HH

P: 44 (0) 118 925 3298
F: 44 (0) 118 925 3299

Asia Pacific Office

Suite 211/250 Pitt Street
Sydney, NSW,
Australia 2000

P: + 61 2 9283 2313
F: + 61 2 9283 3738

U.S. Office

280 Madison Avenue,
Suite 912
New York, NY
United States 10016

P: +1 866 652 0471
F: +1 613 591 6656