

Is your AAA up to the WiMAX challenge?

- ▶ Key Authentication, Authorization, and Accounting (AAA) Capabilities Required to Support WiMAX Deployments



THE MOBILE PERSONALIZATION COMPANY

Introduction

World Interoperability for Microwave Access (WiMAX™) is intended to reduce the barriers to widespread broadband access deployment with standards-compliant wireless solutions engineered to deliver ubiquitous fixed and mobile services such as high speed Internet access, Voice over IP (VoIP), messaging, streaming media, and other IP traffic.

WiMAX—a 4G technology—enables delivery of last-mile broadband access without the need for direct line of sight (LOS). Its ease of installation, wide coverage, and flexibility make it suitable for a range of deployments over long-distance and regional networks, in addition to rural or underdeveloped areas where wired and other wireless solutions are not easily deployed and LOS coverage is not possible.

Commercial launch of WiMAX is well underway around the globe—Sprint launched its XOHM service in the fall of 2008. Scartel introduced YOTA WiMAX services in Russia in late 2008—and trials continue in most markets. According to the WiMAX Forum®, WiMAX operators now offer networks covering 430 million people globally and are on a path to nearly double to 800 million people by the end of 2010. In addition, global WiMAX network deployments are approaching 460 in more than 135 countries for fixed, portable, and mobile networks.

According to Infonetics Research, year-over-year, worldwide sales of 802.16e mobile WiMAX equipment (ASN gateways, BTS, CPE) grew 188% in 2008. While WiMAX infrastructure revenue is somewhat subdued by the current global economic climate, strong CPE sales will drive overall mobile WiMAX market growth in 2009, as more services launch and new subscribers adopt WiMAX services for the first time.

The importance of authentication, authorization, and accounting (AAA) servers in mobile, fixed, and nomadic WiMAX networks is becoming increasingly evident. Standards support for AAA in mobile WiMAX is based on WiMAX Forum Network Working Group (NWG) specifications, and now this working group is incorporating standards support for AAA in fixed/nomadic deployments in Release 1.5 of the NWG standard.

As operators plan their network rollouts, they typically focus on the radio access infrastructure. In many cases, they leave AAA service control and subscriber data management to a later stage, only to find out that they have quickly become major issues as they get ready for commercial launch. Operators deploying WiMAX are realizing that the decisions they make now regarding AAA service control, which supports provisioning, mobility and quality of service (QoS) management, and service and charging models, can have a significant impact on their WiMAX business and commercial roll out plans.

Operators need to work with a market leader with experience in commercial WiMAX launch, as well as the standards insight and technical vision to help navigate a successful implementation, and enable innovative new services.

This paper will be of interest to network planners involved in evaluating connectivity service network (CSN) infrastructure for WiMAX deployments. It examines core requirements for AAA service control in WiMAX and will help those trying to understand if their AAA server has what it takes to support fixed, nomadic and mobile WiMAX. It also provides guidance on what to look for in a solution to ensure that it will accommodate WiMAX growth and service innovation.

► **In Wi-Fi, the AAA server plays a straightforward role in authenticating and authorizing users. In contrast, the AAA is much more involved in WiMAX in the core of the network—managing authentication, authorization, and accounting as well as other key service control functions such as provisioning, mobility management, and QoS management.**

The Role of AAA Service Control in WiMAX

Similar to other networks, the AAA server provides the following core functions in WiMAX:

- ▶ Authentication—confirmation that a user requesting a network service is entitled to do so. It involves presentation of an identity and credentials such as a user name, password, and/or digital certificate. It also requires support for device authentication.
- ▶ Authorization—granting of specific types of service (or “no service”) to a user based on his/her authentication, the services requested, and the current system state.
- ▶ Accounting—tracking of network resource consumption by users.

Using Wi-Fi as an example, the AAA server plays a straightforward role in authenticating and authorizing users. In contrast, the AAA server is much more involved in WiMAX at the core of the network managing authentication, authorization, accounting services as well as other key service control functions such as provisioning, mobility management, QoS management.

In the WiMAX Forum’s NWG Stage 3 Release 1.5 specification, the AAA server is specified as a fundamental building block. It also includes some functions that are not typically supported in other AAA deployments, such as Wi-Fi. Earlier versions of the standard were focused on the use of AAA in Mobile WiMAX, including support for mobile IP. Release 1.5, the upcoming version of the NWG Specification, provides support for Simple IP and Fixed/Nomadic WiMAX.

- ▶ Simple IP—For operators that do not require support for mobility, Release 1.5 introduces standards support for Simple IP, which helps reduce system complexity and the overall cost of the system.
- ▶ Fixed and Nomadic support—within fixed WiMAX, the subscriber is confined to operating within a known and limited area for example, their home location. In nomadic WiMAX, a subscriber can use their device in many locations, but there are no handoffs, so they must disconnect from one location before establishing a connection in the next.

However, given that the AAA server is now a standards-based building block for any WiMAX deployment—fixed, nomadic, simple IP or mobile—WiMAX operators need to ensure that when choosing or evaluating a AAA server for WiMAX, the vendor is offering standards support based on the WiMAX Forum NWG standard.

EAP Authentication Support

A WiMAX compatible AAA server must support the following authentication modes:

- ▶ Device-only authentication using device certificates installed in every WiMAX device during manufacturing. This mode of authentication is typically used to support the first time provisioning of open retail devices. Once the devices are authenticated, a subscription is created and one of the other authentication modes is typically used. This mode uses EAP-Transport Layer Security (EAP-TLS).
- ▶ User-only authentication using a shared credential. This mode of authentication is the most commonly used mode where the subscriber is authenticated using a pre-shared secret established during account setup. This mode uses EAP for Universal Mobile Telecommunication Systems Authentication and Key Agreement (EAP-AKA).
- ▶ Device and user authentication using a single EAP authentication. This mode of authentication is a hybrid mode where first, the device and the network are mutually authenticated using WiMAX assigned certificates, and then, the subscriber is authenticated using a pre-shared secret established during subscription creation. The mode of authentication uses EAP Tunneled Transport Layer Security (EAP-TTLS) with MSCHAPv2 as the inner authentication method.

When comparing a Wi-Fi AAA deployment to a WiMAX AAA deployment, the authentication procedures are common, in that both use EAP and employ similar EAP methods, but that is where the similarity ends. A WiMAX AAA deployment needs more robust support for Remote Authentication Dial-In User

Service (RADIUS) and Diameter protocol support, QoS, and accounting scalability as described in this paper. It also needs to be able to support different WiMAX services such as Simple and Mobile IP.

Multi-Protocol Support

Release 1.5 of the standard includes support for both RADIUS and Diameter protocols, with both targeted specifically at Mobile WiMAX. The AAA server should ideally include simultaneous support for both RADIUS and Diameter protocols allowing operators to protect their investment in legacy applications and services and leverage new SIP-based services supported by Diameter. In addition, many infrastructure vendors have standardized on one protocol or another. Multi-protocol support ensures the operator has flexibility in their choice of infrastructure vendor—as some infrastructure vendors have chosen Diameter versus RADIUS—and avoids vendor lock-in in the future.

Quality of Service Support

Unlike the simplistic QoS support in Wi-Fi—for example, related only to pure bandwidth with maximum rates specified—the AAA server in WiMAX must be able to provide QoS parameters to the network elements. These parameters are provisioned as part of the user profile during network authentication and authorization.

WiMAX also supports multiple traffic flows, each of which can have specific QoS characteristics assigned to it. This enables efficient traffic management and segregation, which will allow WiMAX to support service tiers and services such as VoIP and video calling that may require QoS assurance for a superior user experience.

Accounting

WiMAX supports both IP/Ethernet Session-based and IP/Ethernet flow-based accounting. In IP/Ethernet Session-based accounting, the accounting of all user data are accumulated into a single set of accounting records and reported back to the AAA accounting server.

In IP/Ethernet flow-based accounting, each flow,—which is typically related to a VoIP call, or a video conference—, is reported using its own set of accounting records. As a result, a user session could have a number of accounting records, each related to a specific flow or services used during the course of a session.

In WiMAX, many accounting records can be generated because of mobility, where each handover event may generate multiple accounting records, as well as the use of flow-based accounting. The AAA server must be able to deal with a large volume of accounting messages. It must also support a complex accounting correlation strategy to identify usable records from the raw accounting message it receives, and synthesize those records into formats that can be used by a billing system. An additional benefit is the ability to leverage new charging models. Without this capability, it is likely that a new mediation system will be needed. At the very least, a significant upgrade to the existing mediation system would be required.

Fixed vs. Mobile WiMAX standards

WiMAX/IEEE 802.16 is the global standard for broadband wireless access, equivalent to the IEEE 802.11 for Wi-Fi. It features two variants related to the radio access network:

- ▶ Fixed WiMAX, based on 802.16-2004, supports fixed or nomadic models. With fixed WiMAX, the user equipment does not move between locations while connected to the network as it would in a mobility scenario. This fixed WiMAX deployment model is well suited to home or office use. In nomadic WiMAX, the user terminal can change location (e.g., the user connects at a coffee shop and then moves to an airport), but the IP session or connectivity is not maintained and the user must obtain a new connection at each location.
- ▶ Mobile WiMAX™, based on the 802.16E-2005 standard, introduces support for mobility. Mobile WiMAX allows the user terminal to maintain connectivity while moving from location to location—for example, a user driving from a coffee shop to the airport can hold a VoIP conversation over the WiMAX network. As the terminal moves, the connection is handed off between base stations (BS) and, from time to time, the mobile may even hand off from one operator's BS to another operator's BS, assuming a suitable roaming agreement is in place. Mobile IP (MIPv4 or MIPv6) is the technology used to maintain the IP session during the handoffs.

Scalability

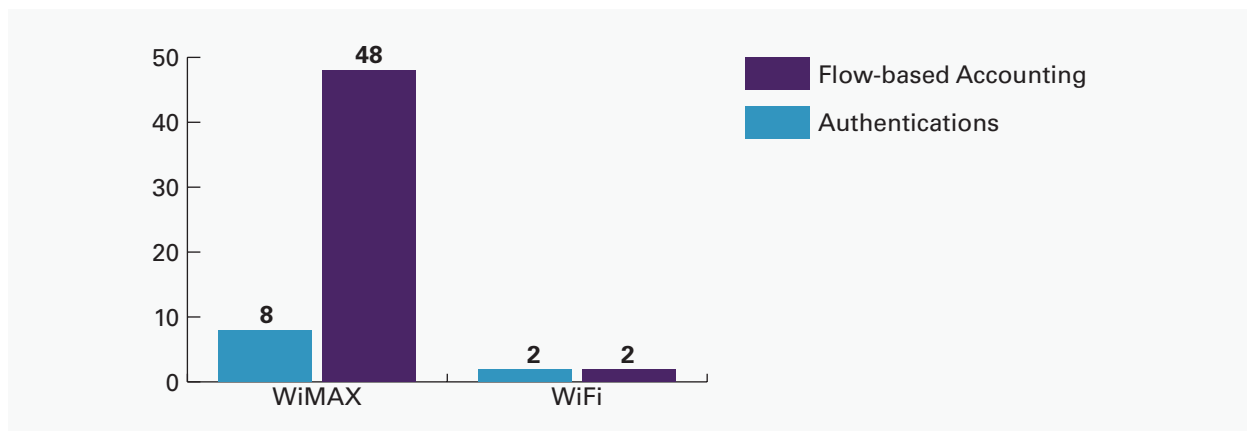
WiMAX and Wi-Fi deployments differ in how the AAA server is used. In Wi-Fi, AAA servers are typically used for authentication once per session. In WiMAX, call models are significantly “chattier” than in Wi-Fi and in 3G networks, due to the “always on” nature of a truly mobile service. AAA servers may perform the authentication function and computationally expensive key derivations many times per session. As a result, the transaction load placed on the AAA server by a WiMAX subscriber is substantially higher than that placed by a Wi-Fi or 3G subscriber.

AAA servers serving Wi-Fi or even today’s 3G networks may not be able to perform at acceptable levels when scaled up to handle the volume of messages generated in a WiMAX network.

Figure 1 compares comparable WiMAX and WiFi call models based on the following assumptions:

- ▶ 3 hour hold time
- ▶ 15 minute accounting interims
- ▶ 4 different accounting flows during the course of the session
- ▶ EAPTLS is used for authentication in WiMAX

In examining authentication messages generated, it shows a 4 fold increase when comparing WiMAX to WiFi. However, when flow-based accounting is applied, there is a significantly higher number of accounting messages generated (48) in WiMAX vs a single accounting record in WiFi comprising a start message and stop message. This comparison helps highlight the scalability and performance challenges that the AAA needs to be able to address through sheer volume of authentication and accounting messages generated in WiMAX.



Mobility puts additional scalability demands on the AAA server due to the volume of accounting records generated during a mobile session. For example, each session initiated by the mobile user will generate its own accounting messages. If session-based accounting is used, there will be accounting messages (start, interims, and stop) for each session the user establishes. If flow-based accounting is used, there will be a set of accounting records generated for each flow established in the session.

In comparison, since Wi-Fi is not a mobile network, a single accounting record is typically generated—if one is generated at all—because most Wi-Fi networks work on a “fixed price for a fixed time” model. Operators will need a carrier-grade AAA solution that can scale to support the increased accounting demands of Mobile WiMAX.

Mobile IP Characteristics Required for Mobile WiMAX

Mobile IP Key Derivation

Legacy AAA servers do not typically support mobile IP (MIP). The following examples of MIP key derivation functions are required to support mobile WiMAX deployments:

- ▶ Key derivation—Key derivation for mobile IP is much more sophisticated than that required by Wi-Fi AAA applications. Upon successful EAP authentication, the AAA server derives mobility keys and other keys from the EAP key material and distributes them to the access serving node gateway (ASN Gateway).
- ▶ Key distribution—The AAA server needs to distribute the mobility keys to the home agent (HA). The mobile IP key recovery procedure with the HA happens after the keys are distributed to the device; therefore, the AAA server must be able to store the keys and distribute them to the HA.
- ▶ Knowledge of state—The AAA server for mobile WiMAX must be able to remember key sequence numbers and previously generated keys. A typical AAA server does not need to maintain state knowledge.

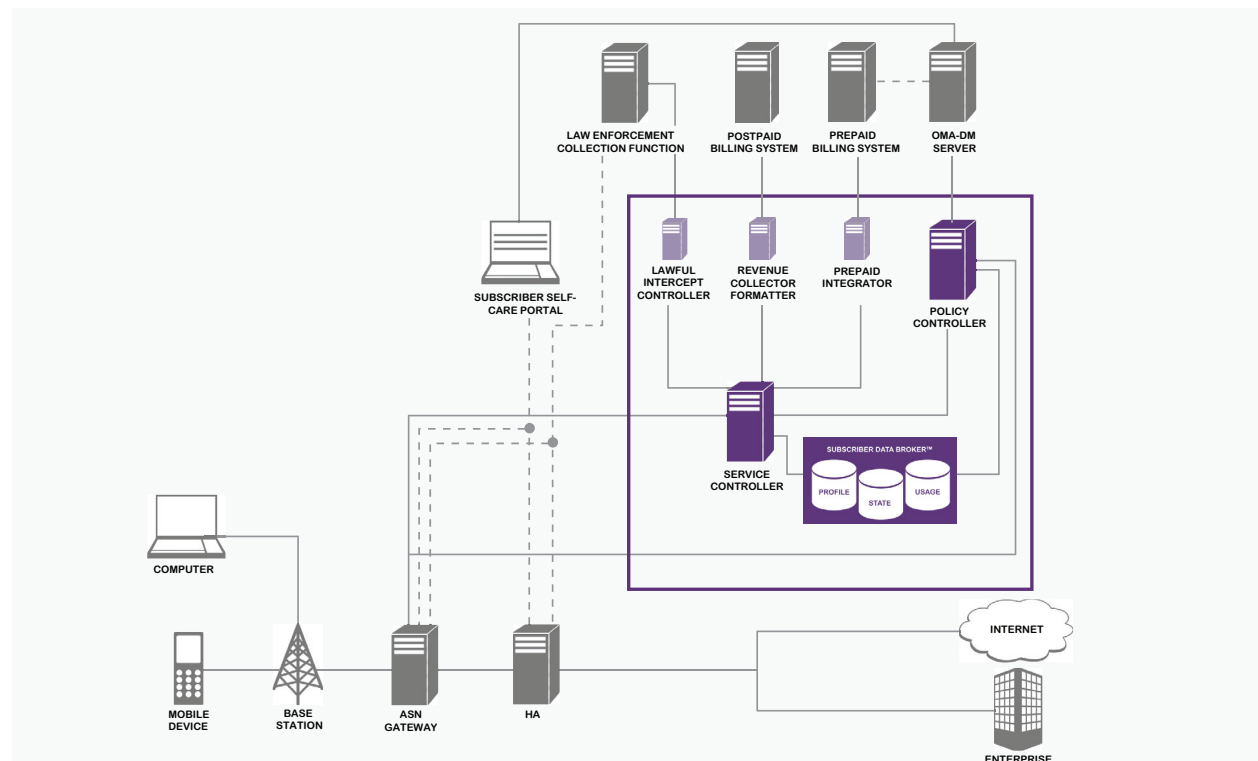


Figure 1: In a mobile WiMAX deployment, the Bridgewater® Service Controller provides core authentication, authorization, and accounting functions to manage a consistent subscriber experience across both visited and home networks.

Support for Mobility Clients

Mobile WiMAX requires support for proxy and client-based MIPv4 and proxy and client-based MIPv6 mobility clients. In Wi-Fi models, the AAA server does not need to support MIP and, consequently, could lack these important capabilities needed to support mobile WiMAX.

The AAA server should also have the ability to determine the optimum HA to which a subscriber's session should be assigned. This allows for least-cost routing to the home network and enables wholesale providers to send subscriber traffic to the proper retailer's HA. In addition, if the allocation algorithm is sufficiently intelligent, it can avoid overloaded or failed HAs, thereby increasing the subscriber's chance of a successful session and a positive network experience.

Service Control Functionality Required to Support WiMAX Services

Beyond the core support required for AAA services in WiMAX discussed in the previous sections, operators must ensure that their AAA server has sufficiently robust functionality to support subscriber growth, transaction volumes, service model innovation and extensibility in WiMAX deployments.

Integrated Policy Support

- ▶ Integrated policy engine and database that supports flexible network, service, and user policies defined at many levels of granularity. This includes domains, user groups, individual users, and wholesale and retail subscriber bases as well as new business models that allow for flexible service creation and reduced overhead.

Scalability and Performance

- ▶ Able to support both subscriber and transaction growth as a result of the chatty WiMAX call models and the increased load of multi-fold increases in accounting records through mobility and session and flow based accounting.
- ▶ Support of high performance RADIUS proxy to enable control in both home network and roaming scenarios, including failover and lockout policy control to ensure a positive subscriber experience.

Subscriber Management

- ▶ Centralized, integrated subscriber management that gives operators providers the ability to centrally manage all subscribers, create comprehensive profiles that define access entitlements across all available services and networks, and avoid re-provisioning subscribers into multiple databases as new network types are integrated. A unified subscriber view also enables fast, flexible service creation that leads to more revenue opportunities.
- ▶ Support for hotlining or subscriber redirection to reduce revenue leakage and create new revenues from top-up services. The ability to divert subscribers from their desired destination to one controlled by the operator is particularly useful when requiring prepayment for services or delinquent postpaid accounts or even for advertising during account updates or other administrative activities.

Interoperability and Extensibility

- ▶ Extensive and proven interoperability with a broad range of network elements, including OSS/BSS and other application platforms, to minimize the need for custom integration and development and accelerate time to market.
- ▶ Vendor neutral pedigree to enable multi-vendor interoperability in mixed vendor and network environments, avoid the hidden cost of vendor lock-in, and achieve a future-proof solution.
- ▶ Support for migration from fixed to mobile WiMAX to eliminate the need to re-provision subscribers and to provide a seamless transition with no disruption to existing subscriber management systems.

Lawful Intercept

- ▶ Satisfy wiretapping lawful intercept (LI) requirements, which add an unavoidable complexity to IP networks like WiMAX. In many markets, LI provisions must be in place to launch service. Support for lawful intercept for compliance with such legislation as the Communications Assistance for Law Enforcement Act (CALEA), requires that the AAA can derive and store stateful information such as IP address, device type, and other relevant data about a specific subscriber session and map an IP address to a subscriber identity in real-time.

Service and Business Model Innovation

- ▶ Accounting mediation support to collect, store, correlate, and format IP/Ethernet session-based accounting records, with tight integration to pre-paid and post-paid billing systems to allow the operator to accurately bill for services and avoid revenue leakage. Avoids the cost of custom mediation solutions.
- ▶ Pre-paid and post-paid charging model support including the ability to integrate with existing pre-paid and post-paid billing systems and meter a subscriber's session to improve revenue capture, and eliminate the need for costly upgrades to existing billing systems or custom mediation solutions.
- ▶ Increasingly, operators want the flexibility to introduce casual user 'Day Pass' services to accelerate subscriber acquisition and drive up revenues from users who do not want to sign up for service contracts.
- ▶ The ability to provide support for multiple business models, including simultaneous support for wholesale and retail services from a common subscriber management and service control AAA infrastructure

Conclusion

To effectively capitalize on WiMAX services, operators need to closely examine the capabilities of AAA servers. Given the pace at which WiMAX services are being launched, now is the time for operators to consider the business benefits of a robust, full-featured system that provides all the functionality required to grow their business and remain competitive with innovative 4G services.

They should also weigh the advantages of working with a proven vendor that has been actively involved in supporting commercial launch of WiMAX in numerous markets, and therefore able to help operators navigate through the applicable standards, so they can make the right choices that will give them flexibility in launching new services.

About Bridgewater Systems and WiMAX

As a principal member of the WiMAX Forum, Bridgewater Systems is actively involved in contributing to the development of WiMAX standards, in particular the WiMAX Forum Network Working Group (NWG) standard as it relates to authentication, accounting, and policy management. Bridgewater has been chosen by more than 25 WiMAX operators around the globe, including Sprint XOHM, Scartel and Tatung.

Does Your AAA Have What it Takes for WiMAX?

	WiMAX Requirements	Business Value
Mobile IP	<ul style="list-style-type: none"> ▶ Stateful mobile IP Session Key derivation and delivery 	<ul style="list-style-type: none"> ▶ Real-time management of the subscriber's mobile experience in WiMAX
Authentication	<ul style="list-style-type: none"> ▶ Broad EAP Authentication Support ▶ Device and Subscriber Authentication 	<ul style="list-style-type: none"> ▶ Ensure seamless subscriber experience with support of multiple EAP methods simultaneously. ▶ Broad security controls required for WiMAX
Dual Stack Protocol Support	<ul style="list-style-type: none"> ▶ Ability to support RADIUS and Diameter protocols simultaneously 	<ul style="list-style-type: none"> ▶ Protect investment in legacy applications and enable migration to next-generation networks.
Subscriber Management and Quality of Experience	<ul style="list-style-type: none"> ▶ Centralized, pre-integrated Subscriber Management System ▶ Quality of Service (QoS) Support ▶ Hotlining or Subscriber Redirection 	<ul style="list-style-type: none"> ▶ Manage subscribers across all services and networks simultaneously. ▶ Improve subscriber experience with QoS associated with subscriber session or application. ▶ Avoid revenue leakage. Manage subscriber experience in real time.
Lawful Intercept	<ul style="list-style-type: none"> ▶ Map encrypted pseudo-identity to a subscriber to enable lawful intercept 	<ul style="list-style-type: none"> ▶ Comply with commercial launch requirements for LI compliance
Service and business model Innovation	<ul style="list-style-type: none"> ▶ Post-paid Support ▶ Pre-paid Support ▶ Casual User Services ▶ Session-based accounting and flow-based accounting support ▶ Support of Multiple Business Models; e.g., Wholesale, Retail 	<ul style="list-style-type: none"> ▶ Eliminate the need for custom mediation solution or costly enhancements to existing BSS. ▶ Accelerate subscriber acquisition with flexible prepaid plans. ▶ Appeal to users who may not want to sign up to prepaid services or postpaid contracts ▶ Differentiate services and appeal to a broader base of subscribers who may want to manage data services consumption in different ways. Enable flexible billing models. ▶ Leverage new business models with common policy management infrastructure.
Scalability and Performance	<ul style="list-style-type: none"> ▶ Scalability to support transaction heavy call models ▶ Support greenfield deployments with the ability to scale in line with subscriber growth ▶ Intelligent Radius Proxy 	<ul style="list-style-type: none"> ▶ Support for increased transaction volumes due to accounting messages and subscriber authentications. Sustain future growth. ▶ Future proof solution ▶ Minimize operational impact of non-performing proxy targets.
Extensibility and Future-Proof Requirements	<ul style="list-style-type: none"> ▶ Migration Path from Fixed to Mobile WiMAX ▶ Integrated policy engine ▶ Vendor and Network Agnosticism ▶ Extensive and Proven Interoperability 	<ul style="list-style-type: none"> ▶ Future-proof solution. ▶ Create and manage flexible network, service, and subscriber policies from single platform. ▶ Ease of integration in mixed networks. ▶ Accelerate time to market. Avoid expensive custom integration
Standards Support	<ul style="list-style-type: none"> ▶ NWG standards support for fixed, nomadic and mobile WiMAX 	<ul style="list-style-type: none"> ▶ Reduce costs of custom integration

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