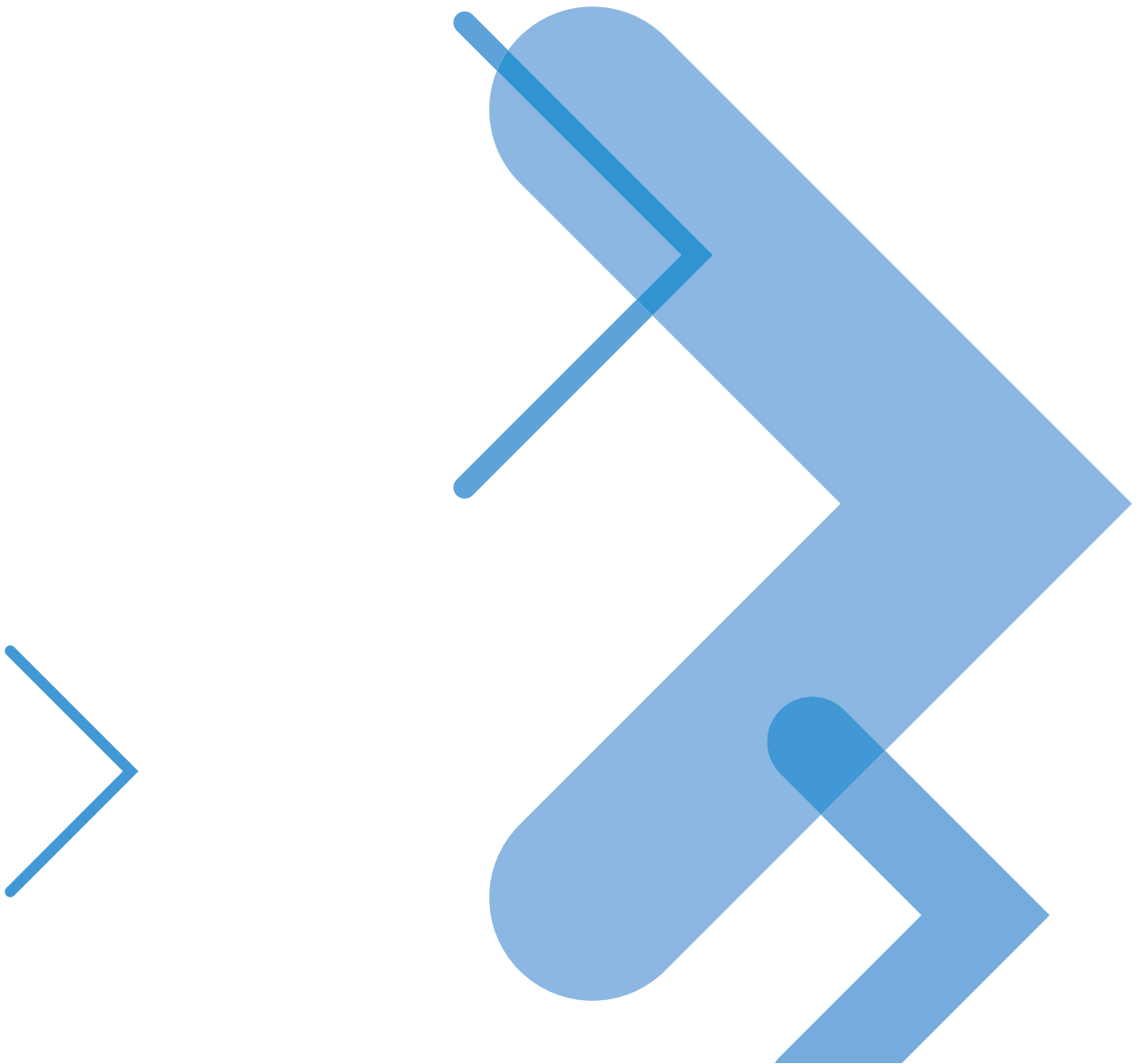




WiMAX Security for Real-World Network Service Provider Deployments



Executive Summary

For network service providers in search of next-generation subscriber services and new revenue streams, WiMAX represents a path towards seamless mobile access that is similar to wide-area cellular services (UMTS/CDMA) but with higher throughput rates (up to 70Mbps) and LAN-like connections that are similar to Wi-Fi. WiMAX could well represent the future of service provider infrastructure, but how secure is it?

WiMAX security standards from IEEE specify some powerful standards-based security controls, including PKMv2 EAP-based authentication and over-the-air AES-based encryption. But secure technology does not, in itself, constitute a secure end-to-end network, and, consequently, WiMAX presents a range of security design and integration challenges.

As discussed throughout this paper, service providers need to ensure that deployment efforts address and prioritize WiMAX security initiatives within the context of potential business impacts from identified threats. Beyond the technology aspects of security, WiMAX design and integration must also add a number of key security best practices into existing operational processes and policies.

For many WiMAX providers, the cost of operating a security program is often not considered with the same rigor as other operational areas—a situation that can lead to creeping security OPEX costs. To control downstream costs, providers should carefully consider the longer-term implications of operational expenses, in general, and in the security area, in particular. If security is to be fully addressed, WiMAX providers need an implementation process based on advanced security design and operational best practices that can leverage the standards-based security controls available in WiMAX. This approach can potentially enable very effective security OPEX management.

Why WiMAX?

WiMAX (Worldwide Interoperability for Microwave Access) is designed to deliver next-generation, high-speed mobile voice and data services and wireless “last-mile” backhaul connections that could potentially displace a great deal of existing radio air network (RAN) infrastructure. For network providers, this will enable an expansive array of multimedia and real-time subscriber services that go well beyond current 2.5/3G applications, including mobile streaming media services, mobile TV, Unified Communications, and Voice over IP (VoIP), which, for the first time, becomes practical and viable on a metro-wide scale through WiMAX. Network service providers can’t take full advantage of mobile voice and multimedia over IP unless

there is the potential to manage Quality of Service (QoS). With this in mind, five distinct classes of service quality have been built into WiMAX, allowing a more robust and resilient connection for users who require time-sensitive applications and service level agreements (SLAs).

WiMAX can offer a large wireless access network footprint to subscribers (similar to data-enabled cellular services such as UMTS/CDMA), while at the same time providing higher throughputs that are similar to WLAN networks. With its large footprint, high access speeds, built-in QoS and SLA capabilities, WiMAX is an ideal access network for next-generation converged voice and data services and streaming wireless multimedia.

Figure 1. WiMAX architectural components

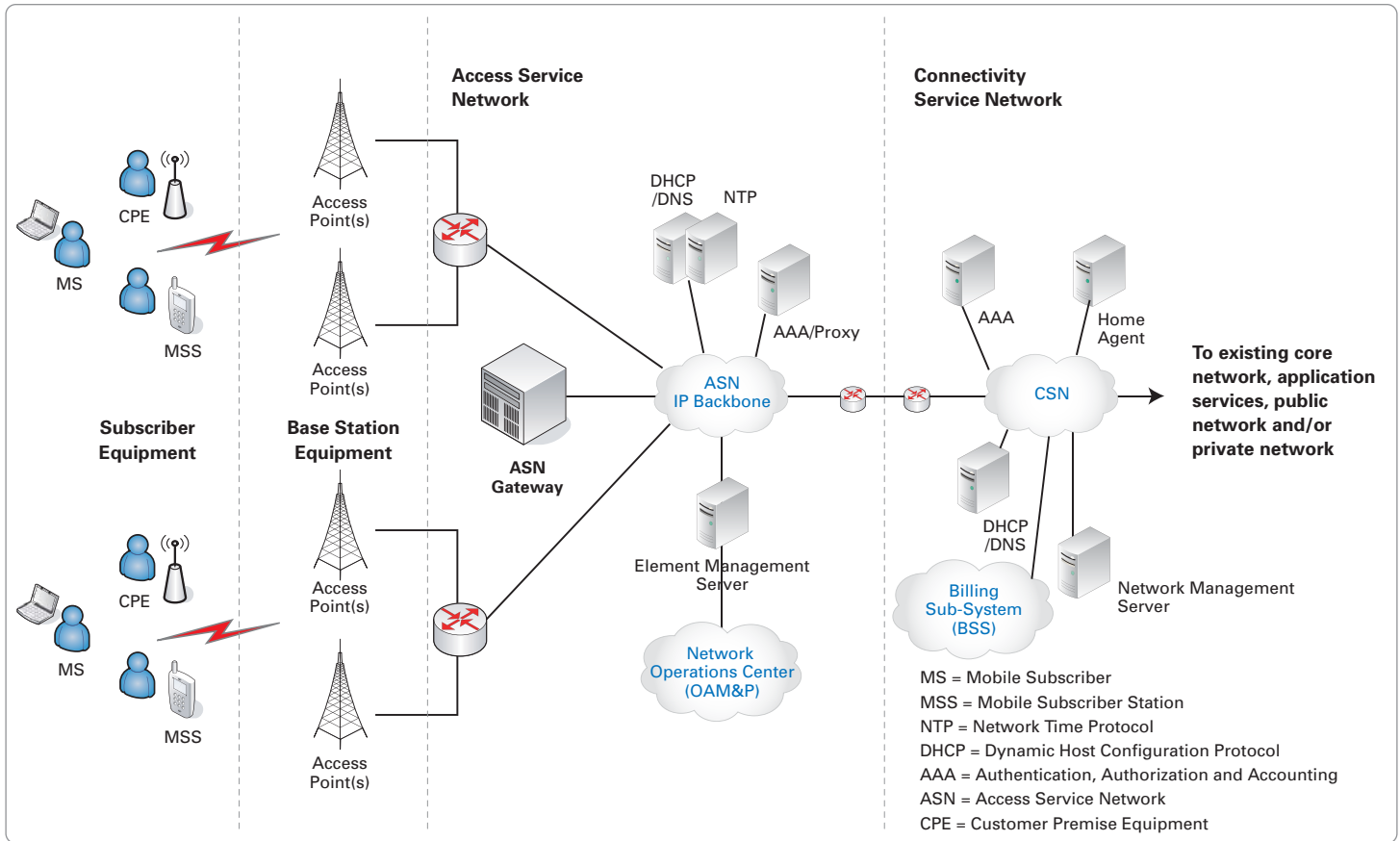


Figure 1 shows the main architectural components of a WiMAX network, including:

- **WiMAX Mobility Subscriber Station.** On the far left of Figure 1, mobile subscribers (MS) use mobile subscriber stations (MSS)—generalized mobile equipment that provides connectivity between subscriber equipment and base station equipment.
- **WiMAX Access Service Network.** Access Service Network (ASN) is defined as a complete set of network functions that provide radio access to a WiMAX subscriber, including a proxy AAA server, DHCP addressing function, and other IP-based resources, including network management.
- **WiMAX Connectivity Service Network.** Connectivity Service Network (CSN) is defined as a set of network functions that provide IP connectivity services to the WiMAX subscribers through the ASN.

WiMAX Security: A Multifaceted Challenge

Since WiMAX utilizes IP (Internet Protocol) as its core transport mechanism for handling control/signaling, subscriber and management traffic, network service providers need to be concerned about the IP-related security threats and the implications of security for end client devices, the core network, application servers, and everywhere in between.

Anticipating the need for strong security, IEEE 802.16 working groups incorporated a substantial amount of advanced security thinking into the WiMAX standards. Their philosophy has been to “build in” security instead of having to “bolt on” security at a later time. The WiMAX standard includes specifications and guidelines for security enhancements in these areas: 1) the authentication of the subscriber device, 2) higher-level (user) authentication, 3) advanced over-the-air data encryption, and 4) options for securing control/signaling data within the core network, which all converge on an IP-based, service-orientated core backbone network.

Although security has been more stringently architected into WiMAX, due to the complexities involved in various deployment models of WiMAX networks, it’s the responsibility of the network service providers to develop comprehensive security strategies for the design of secure network, policy, integration and operational security practices. Otherwise, the network and users can be left vulnerable to service abuses, malware and hacker exploits, which exposes the network service provider to heightened operational and business risk. Table 1 presents the key security concerns for service providers.

Too often, it is assumed that security devices alone can ensure a secure end-to-end network. But it’s only by looking at all aspects of the WiMAX security

Table 1. Key WiMAX security concerns for network service providers

Requirement	Type of attack	Attack description
Confidentiality	Man-in-the-Middle	Impersonation of base station to subscriber, or a two-way impersonation between subscriber and base station
Integrity	Privacy Compromise	User and/or management traffic traveling over wireless/wireline links is detected (via real-time packet capture or offline analysis)
	Theft of Service	Subscribers access services without proper authorization and without online or offline auditing, and consequently do not pay for services (includes cloning exploits)
Availability	Physical Denial of Service	Degraded network performance (and its services) by perturbing the physical medium (jamming, etc.)
	Protocol Denial of Service	Exhausted network and system resources or performance (by injecting new or modifying existing user and control traffic)
	Replay	Injection of previously valid messages so as to exhaust resources on network or to lock out valid subscriber

challenge that a truly effective security posture can be achieved across the entire end-to-end WiMAX environment. Consequently, it is critical to the successful operation of WiMAX deployments that implementers address all the people, process, policy and technology aspects of security mitigation. The first step down the path towards this holistic, real-world approach is to understand the primary protection methods of WiMAX security. The following sections explain how WiMAX solutions address various types of attacks.

WiMAX Security Aspects

The WiMAX 802.16e standards effort specifies a number of advanced security protections including: mutual device/user authentication, flexible key management protocol, strong traffic encryption, control/ management message protection, and security protocol optimizations for fast handovers when users switch between different networks. The IEEE approach to standards-based security relies on Privacy and Key Management Protocol Version 2 (PKMv2) as a key management protocol that enables crypto key exchange for authentication, encryption and protection of multicast and broadcast traffic.

Device and User Authentication: The PKMv2-based WiMAX standards address both device and user authentication using the Internet Engineering Task Force EAP (Extensible Authentication Protocol).

Mobile Traffic Encryption: The Advanced Encryption Standard (AES) CCM is the cipher used for encrypting subscriber traffic Over the Air (OTA) Mobile WiMAX MAC interface. The WiMAX approach to AES encryption uses Counter Mode with Cipher Block Chaining Message (CCM) Authentication Code. With AES CCM, the sending party generates a unique per-packet value and communicates this value to the receiver—a technique that can mitigate man-in-the-middle attacks because attacks will have difficulty substituting traffic. As further protection, a Traffic Encryption State machine uses a periodic key refresh mechanism to enable sustained transition of keys.

To optimize the re-authentication mechanisms for supporting fast handovers in Mobile WiMAX, a 3-way handshake scheme is supported. This method is useful to prevent any man-in-the-middle attacks.

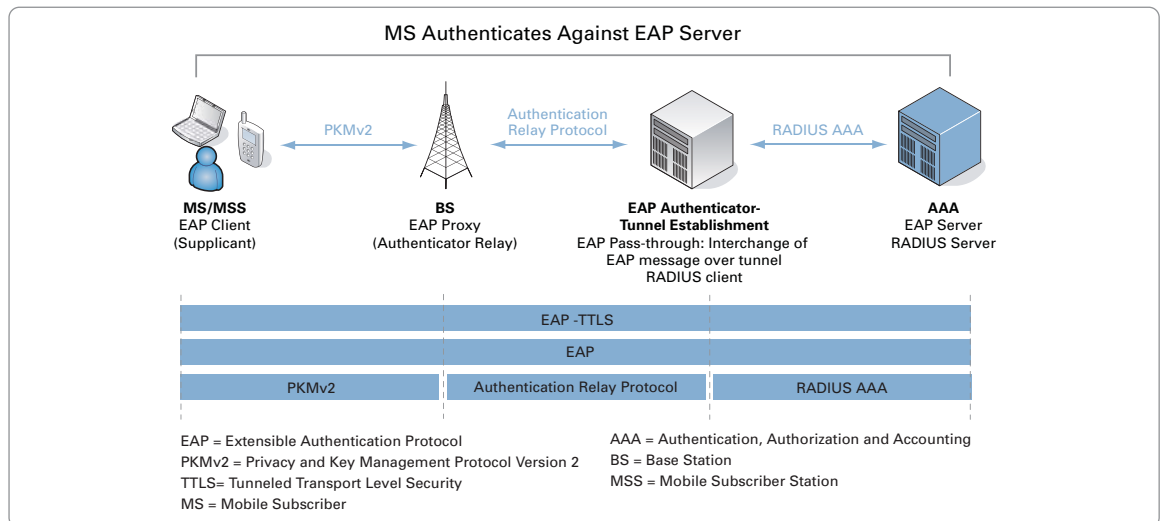
Authentication is an area that has received considerable attention within WiMAX standards and technology efforts. Authentication is the ability of the network to ensure that end-user and subscriber end devices (MSS) are legitimate consumers of network services. Network entry authentication in this system relies on EAP to provide a flexible and scalable framework for the authentication of MS/MSS. As shown in Figure 2, the PKMv2 protocol uses EAP key management for the trusted distribution of authentication and encryption keys

from the base station to the subscriber handset, thereby providing authentication of the user by the network. The EAP authentication framework allows the use of a variety of authentication methods appropriate for different types of devices and capabilities, which all exist within a common framework for end-to-end authentication.

Although these advanced authentication techniques are defined in the WiMAX security specifications, the uniform public key infrastructure and mutual authentication aspects of security need to be addressed in the real-world architecture design by implementers who take into account all the processes and policies associated with strong two-way authentication and key management.

- **Scenario # 1 – Common billing and customer care:** In this case, the WiMAX and 3GPP networks are not fully integrated, but subscribers can get integrated billing and customer care for the two services in a unified way.
- **Scenario # 2 – Direct IP access via WiMAX:** Subscribers can get Internet access via WiMAX, but authentication and accounting are handled by the 3GPP billing system.
- **Scenario # 3 – WiMAX 3GPP IP access:** Subscribers can access 3GPP packet switched services via the WiMAX Access Network, which requires that the WiMAX Access Network have interworking with the 3GPP PLMN. [1]

Figure 2. End-to-end view of the WiMAX authentication and key exchange methods



In this end-to-end view of WiMAX authentication and key exchange methods, EAP running over carrier protocols (PKMv2, RADIUS, etc.) is used as an authentication framework mechanism between entities. TLS (Transport Level Security) provides for mutual authentication between two endpoints. TTLS (Tunneled Transport Level Security) extends TLS mechanisms to perform AAA Server authentication for subscribers or subscriber devices.

WiMAX Integration Challenges

What are the real-world implications for integration of WiMAX into actual 2G and 3G networks operating under the 3GPP and 3GPP2 frameworks? Within current working group thinking, the 3GPP committees consider WiMAX as an untrusted network (as of August, 2006). Consequently, it is the responsibility of network providers and network designers to ensure the same level of security within WiMAX IP access as is provided by 3GPP IP services under regular mobile network operations. According to WiMAX Forum documentation of 3GPP/WiMAX interworking, 3GPP operators can grant authenticated subscribers access to services in the 3GPP Packet Switched (PS) domain through a WiMAX Access Network. The WiMAX Access Network architecture can be integrated into the 3GPP core network environment using different configurations and integration options.

Some example scenarios for WiMAX/3GPP interworking include:

Given all the options and scenarios possible with WiMAX/3GPP (and WiMAX/3GPP2) integration, network service providers need to carefully consider the security issues associated with the convergence of this access mechanism with the existing IP core network infrastructure. The WiMAX standard introduces substantial improvements in the way of security and RF innovation, but lack of proper architecture design, implementation and integration strategies can produce a precarious environment for the service provider and the subscriber.

Below are two primary issues for planning security of WiMAX network integration:

- **AAA Traffic:** To allow secure exchange of security, authorization and accounting material, an appropriate security and trust relationship should exist between the 3GPP AAA server and the WiMAX Access Network.

- **Data Traffic:** Appropriate security devices and tunnels should be deployed between the WiMAX Access Network and the 3GPP Gateway located on the border of 3GPP PS.

WiMAX Security Reference Architecture

To address the full spectrum of security factors for WiMAX in real-world wireless provider networks, Motorola Security Services (MSS) has designed a holistic *WiMAX Security Reference Architecture* that provides a comprehensive view of vulnerabilities, identified threats and mitigations. This Security Reference Architecture is the result of a thorough security analysis of the WiMAX network environment, including:

- A security risk assessment from an operational network and customer requirements perspective
- Comprehensive WiMAX threat identification and analysis
- The impact of vulnerabilities within the network environment
- Suggested mitigations and recommendations for network design, network devices, procedures, policies, and related human factor issues

The MSS WiMAX Security Reference Architecture is a unique guideline for network service providers that are planning countermeasures and security enhancements to mitigate/reduce threats to an acceptable risk level. At key points in the WiMAX network, appropriate security controls are selected based on defense-in-depth layering, along with people, process, policy and technology enforcement. The recommendations are visualized within a security overlay diagram detailing the points of security integration.

The WiMAX Security Reference Architecture is based on extensive study of industry knowledge on WiMAX and the IP network environment, including these security standards and best practices: NSA-IAM, ETR 332, ITU-T X.805, NIST and ISO 17799. The architecture analyzes WiMAX threats and protections using these logical and functional network areas:

- **WiMAX User Plane:** The end-user security plane addresses security of access and use of the service provider's network by customers, including actual end-user data flows.
- **WiMAX Control/Signaling Plane:** The signaling and control data across WiMAX networks are transferred by ASN Gateway, BTS, FA/Router, Switches and AAA using protocols according to the type of signaling messages and network elements involved.
- **WiMAX Management Plane (Operation, Administration, Maintenance and Provisioning OAM&P):** This plane addresses security of management data across the WiMAX network and the elements that perform OAM&P, such as network management systems and network elements that have visibility on the management plane, radius servers, base stations, routers, etc.

Table 2 shows examples of threats and countermeasures that exist within the WiMAX User Plane. The MSS WiMAX Security Reference Architecture includes similar threat information for the other planes and layers as well. The architecture also includes extensive mitigation and policy guidelines, as well as best practices for the end-to-end WiMAX infrastructure.

In addition to WiMAX, MSS has created Security

Table 2. Example of WiMAX threats and countermeasures

Layers	Threats	Countermeasures	Examples/Comments
Application	Worms, Trojans, Viruses	Antivirus, FW, IDP	Voice, instant messaging, e-mail, enterprise network access, custom application, video, Web browsing, etc.
Service	SIP (Session Initiation Protocol), E-mail, Denial of Service, DNS Attacks	DMZ, FW, ACL Policy	SIP, SMPT/POP, HTTP, etc.
Infrastructure	EAP Throttling, Spoofing, DoS	EAP MAX Session Counter, Security Association, Secure Perimeter, FW, IDP	Air interface and mobile core network interface carrying end-user data
	Flooding MS, RF Flooding	Over-the-Air Encryptions, SSL VPN Tunneling	

Reference Architectures for CDMA, GPRS, WLAN, IMS, UMA, and other key network environments.

Conclusion

WiMAX is a powerful wireless services access platform that will increasingly support a wide range of revenue-generating voice and data applications for network service providers around the globe. The mission-critical nature of WiMAX applications demands high levels of network security, but this is not possible unless security standards, technologies, processes and policies are all united in a holistic, real-world security architecture that can protect the WiMAX infrastructure from end to end and top to bottom.

Motorola Security Services has a unique set of "holistic" security planning, design and integration capabilities that can help cellular network service providers achieve their WiMAX deployment and revenue goals. MSS provides a specialized security service focused on understanding and satisfying the unique business and technical needs of leading network service providers. MSS can benefit providers in the deployment stages of WiMAX, as well as in cases where WiMAX has already been implemented.

Hacking, fraud, virus attacks, identity theft, Denial of Service attacks and data pirating can lead to WiMAX service interruption and revenue loss. The more a service provider relies on data services and data-driven applications, the more it needs to have an advanced network security design. MSS security design and integration services are uniquely able to protect WiMAX networks against criminal and malicious exploitation of network infrastructure. MSS helps service providers proactively manage their WiMAX networks, reducing vulnerabilities and safeguarding performance while security OPEX is efficiently controlled.

About Motorola Security Services

- Proven expertise in voice and data security for service providers, governments and enterprises
- Established track record of delivering design and implementation of complex infrastructure networks that are supported by a full range of professional and managed security services
- Holistic security framework that operationalizes security across the people, process, policy and technology foundations of each organization
- Practical hands-on experience with vulnerability assessment and mitigation, as they relate to threats associated with converged networks
- Onsite Security Assessments: Two-Way Radio Network, WLAN, WWAN, UMA, IMS, CDMA, GSM/GPRS, wi4 WiMAX, UMTS, Physical and Facilities
- Defense-in-Depth Threat Management (Design, Managed Service, Integration) expertise
- Policy Design and Related Services (Incident Response Planning, Risk Management, Compliance)

About Motorola Services

Motorola Services, based on innovative technologies, delivers optimal solutions and managed services for service providers, governments and businesses. Motorola offers a comprehensive portfolio of cost-effective, high-performance services and applications that are robust and operational in critical multi-vendor, multi-technology environments. We leverage deep expertise in mobility, security and systems integration to deliver seamless communications. Motorola Services collaborates with customers to understand their needs and help them achieve their organizational objectives.

References:

[1] WiMAX End-to-End Network Systems Architecture - 3GPP/ WiMAX Interworking, Release 1; 2006; WiMAX Forum

[Please contact your Motorola representative to learn more about real-world WiMAX security architectures that can help your organization achieve its wireless connectivity goals.](#)



MOTOROLA

Motorola, Inc.
www.motorola.com

The information presented herein is to the best of our knowledge true and accurate. No warranty or guarantee expressed or implied is made regarding the capacity, performance or suitability of any product. MOTOROLA and the stylized M logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

© Motorola, Inc. 2007
0807MSSWiMAX