

# Enterprise UMA - the Carrier Standard for Enterprise Mobility

July 2006

## The Carrier Standard for Enterprise Mobility

Unlicensed Mobile Access is a standardized method to extend the cellular infrastructure via the Internet and WiFi. Using dual-mode phones, consumers use UMA to make calls from their homes and hotspots, and seamlessly rove between the WiFi and cellular domains. Worldwide, a few carriers already offer UMA-based residential services, and many more are in various stages of trial.

Does the **Mobile** in Unlicensed Mobile Access describe the **device** or **action**? Is UMA just a mechanism for a cell phone to access to the cellular network from residential WiFi?

### WHY IS UMA ONLY A RESIDENTIAL SOLUTION?

Regardless of what the analysts say, the Mobile in Unlicensed Mobile Access defines more than the device for residential service - much more. Envision a solution wherein a carrier can provide secure, authenticated, single access mobility services to an Enterprise -- a solution that delivers:

- Integration with the Enterprise PBX and the carrier voice service,
- Ubiquitous services from the carrier, Enterprise, and Internet available to laptops, cell phones, and PDAs.
- Enterprise WiFi communications that are carrier-class secure and authenticated
- Improved indoor coverage
- Seamless Enterprise WiFi to cellular handover
- Carrier-offer bundled services for Enterprise voice, data and mobility without IMS' cost or complexity

UMA is the only standards-based technology available that can deliver these Enterprise services.

Technically, UMA is an Access Method; but to date, UMA is seen as little more than a delivery mechanism - just a piece of required technology to extend cellular telephony via residential Internet. All that is about to change...

As an Access Method, UMA has the ability to:

- Converge the carrier and Enterprise networks;
- Provide a single access method to both Enterprise and carrier voice and data services;
- Provide carrier-class authentication and security to the Enterprise;
- Extend *carrier and Enterprise* voice and data *mobility* ubiquitously to all mobile devices - laptops, cell phones and PDAs;
- And do it all within the residential UMA infrastructure.

UMA is not a limited-life residential roving service. At NET, we see UMA extending far beyond residential boundary. Employed within an Enterprise, UMA becomes a cornerstone solution, establishing a new category of carrier-offered total Enterprise Mobility - voice and data, carrier and Enterprise. Using UMA to its fullest potential as an Access Method, it is possible for a carrier to provide cost-effective bundled mobility service to the Enterprise in a completely unique way. Never has a single technology been positioned to provide ubiquitous access and service across the Enterprise, Internet and cellular networks. Enterprise UMA fundamentally changes the philosophical and conceptual principles on which the UMA technology was originally created - UMA is extended so far that it requires redefinition.

### THE MOBILE IN UMA IS THE ACTION - IT IS MOBILITY.

The missing link to opening UMA's potential is the Enterprise UMA Mobility Controller. The Enterprise UMA Mobility Controller uses UMA to deliver bundled voice and data mobility services, carrier and Enterprise, using simple, standards-based technology that is available today.

### ENTERPRISE UMA DELIVERS

*One access control point, one access method, one authentication scheme, one security method, and one converged network with ubiquitously available services from anywhere.*

*Enterprise UMA revolutionizes the way carriers deliver services to the Enterprise.*

### 1 & 2. SINGLE ACCESS CONTROL POINT AND ACCESS METHOD

Traditionally, the enterprise network is constructed with two access locations: intranet and Internet. Internal access is supported by locally switched Ethernet, and Internet connectivity is comprised of router and firewall, VPN appliance and client. Enterprise mobility is a function mainly of cellular voice and VPN-protected data.

With the advent of VoIP and WiFi, traditional mobility solutions are inadequate. With VoIP, integration of the cellular network and corporate telephony infrastructure is required to provide seamless mobility. For Wifi, mobility is dependent upon the access network and device - different devices require various types of security and authentication based upon their location and the desired services. At present, an enterprise must install several devices, and associated authentication and security, in order to obtain both voice and data mobility:

- VPN appliance and clients support extranet data mobility.
- Session Border Controllers, or other specialized enterprise mobility server, support WiFi extranet voice.
- Enterprise-installed WiFi Access Points support intranet mobility; access must be protected by WEP or WPA security associated with the wireless access point.
- A VoIP gateway connects VoIP and PBX services.

These solutions represent completely different methodologies, disciplines, and architectures, and significantly increase the Enterprise IT burden.

The Enterprise UMA Controller replaces all of these devices and institutes a single access method. With UMA, all enterprise wireless devices connect to the Enterprise UMA Controller. As the controller accesses both enterprise and cellular networks, the UMA Controller is the single access point for all devices to reach all services.

*One access control point, one access method.*

### 3. STRONG AUTHENTICATION SCHEME

The Enterprise UMA Controller accesses carrier AAA services via the existing carrier UMA infrastructure. SIM-loaded laptops and phones attached to the Enterprise UMA Controller are authenticated just as any normal UMA phone; authentication permits devices to access both carrier and enterprise networks and services.

UMA's carrier-class mutual authentication protects both the Enterprise and carrier networks; Enterprise UMA Access Control ensures that only Enterprise-permitted devices can access the converged network. Cellular's SIM-based authentication has been in use successfully for years - it's simple, extremely effective, and when employed within the enterprise, vastly reduces IT burden while simultaneously providing exceptionally high, carrier-class authentication.

*One access control point, one access method, one authentication scheme.*

### 4. SECURITY METHOD

The need for enterprise security has never been greater. Internet and intranet wireless access points are a paramount security concern for IT departments. Unsecured Wireless Access Points and WEP attacks are real, but seemingly unaddressable concerns.

UMA is inherently secure. With Enterprise UMA, both intranet and Internet

communications converge at the Enterprise UMA Controller, creating carrier-class secure IPsec tunnels. WiFi data within UMA tunnels are 100% secure, even if the access point employs no security of its own! With Enterprise UMA, data security is automatically guaranteed regardless of the WiFi infrastructure or location.

This security extends to laptops, phones and PDAs! The need to have a separate WiFi security (WEP WPA) and Internet security (VPN) is replaced with a single, secure UMA infrastructure.

*One access control point, one access method, one authentication scheme, one security method.*

## 5. CONVERGED NETWORKS

As carriers begin to offer Internet-based telephony and hosted application services, the traditional demarcation between the carrier and enterprise networks begins to blur. The firewall function employed to wall the enterprise from the outside world is no longer useful for the purpose; an enterprise-carrier network federation is required in order to deliver Internet-based services - the future is a converged network.

IMS is touted as the answer for converging both carrier and enterprise networks - a heterogeneous framework that joins all services in all networks. The truth of IMS is far from its promise. IMS' base protocol, SIP, is still undergoing massive change as it winds its way towards being as interoperable as IP. Then IMS, under development for years, is still being defined and changed. It is for these reasons that we are unlikely to see a true, native IMS phone on the market any time soon. One day IMS may fulfill its potential, but for the foreseeable future, the ever-shifting IMS framework is based upon a protocol that has yet to reach maturity. The result is massively expensive, homogenous networks with which only carriers can afford to experiment. Enterprises require a different convergence solution.

Enterprise UMA cost-effectively converges enterprise and carrier networks to deliver revenue-generating telephony and data services, as well as future IMS services when they become available. Using mature, standards-based UMA, a carrier can extend the cellular infrastructure to the enterprise while maintaining the carrier-enterprise demarcation point. For businesses, Enterprise UMA is affordable. The required equipment's ROI is recovered in months as the carrier cost-effectively offers bundled voice, cellular, data-converged, and Total Mobility services. Best of all, carrier-offered Enterprise UMA services effectively eliminates customer churn.

*One access control point, one access method, one authentication scheme, one security method, and one converged network.*

## SERVICES AND AVAILABILITY

NET's patent-pending Enterprise UMA Controller accesses both enterprise and carrier networks. Carrier voice, data, and future IMS services, as well as enterprise voice and data, are available from the cellular macro, Internet, and Enterprise networks.

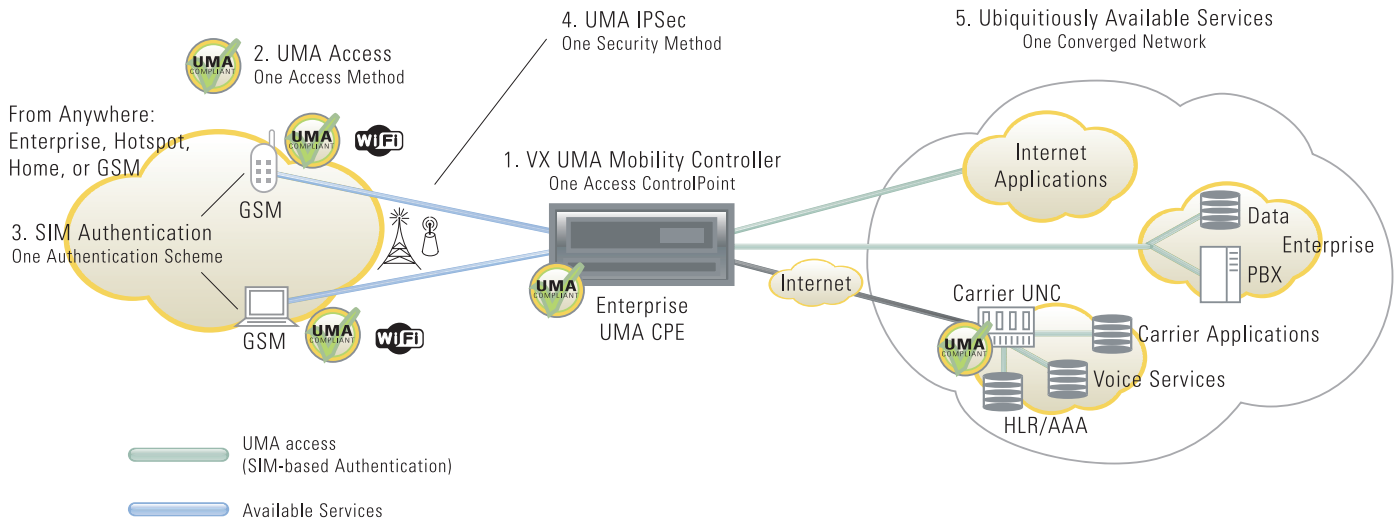
Enterprise UMA fuses the corporate WiFi and network infrastructure together with the cellular core to create a seamless, location-independent service experience. A dual-band UMA/GSM phone provides a single device, and phone number, for each user. SIM-loaded laptops and phones securely access enterprise and carrier services from any network. NET's Enterprise UMA Controller seamlessly integrates the corporate PBX to the carrier UMA service; corporate users can 4-digit dial UMA phones. Carriers can offer enterprise voice services without the SIP and thereby maintain control over telephony services and operation. Data mobility offered by UMA exceeds IMS' SIP-based capabilities; laptops and phones can securely access enterprise data servers from cellular, Internet or enterprise networks. And of course, all carrier services are available too.

*Enterprise Mobility: One access point, one access method, one authentication, one security, and one converged network with ubiquitously available services from anywhere.*

NET's Enterprise UMA breaks ground on new technology and explodes UMA's presence beyond the residential frontier allowing carriers to offer compelling, revenue-generating Enterprise voice, data, and mobility services using a standards-based, cost-effective UMA infrastructure.

NET has been a technology innovator for over 20 years. Talk with us. Let NET show you the future of Enterprise Mobility.

**Figure 1:** The VX UMA Mobility Controller permits devices from GSM, Internet, and Enterprise networks to seamlessly access services on the Internet, Enterprise, or Carrier networks. UMA unifies access method, security, and authentication into a single, carrier-class solution.



**Corporate Headquarters**  
 6900 Paseo Padre Parkway  
 Fremont, CA 94555 U.S.A.  
 T 510.713.7300  
 F 510.574.4000  
 E info@net.com  
**www.net.com**

**N.E.T. Federal**  
 21660 Ridgetop Circle, Suite 100  
 Dulles, VA 20166 U.S.A.  
 T 703.948.1800  
 F 703.948.1850  
 E net\_federal@net.com

This document does not create any express or implied warranty by NET or about its products or services. NET's sole warranty is contained in the written product warranty for each product. The end-user documentation shipped with NET products constitutes the sole specifications referred to in the product warranty. The customer is solely responsible for verifying the suitability of NET products for use in its network. Specifications are subject to change without notice.

© 2006 Network Equipment Technologies, Inc. All rights reserved. NET, the NET logo are trademarks of Network Equipment Technologies, Inc., and its subsidiary, N.E.T. Federal, Inc. All other trademarks are the sole property of their respective companies.

UMA-WP-0806