Preparing for Unlicensed Mobile Access

Extending mobile access to unlicensed and untrusted networks with the Certicom Security Architecture

February 2005

certicom™

Convergence and Competition: the case for UMA

The convergence of fixed and mobile telecommunication networks has pitted mobile and fixed telephone carriers against each other in an epic battle for market share and revenue. Mobile penetration in most countries continues to grow – reaching saturation in only a few markets. Fixed line subscriber numbers and voice revenue are in decline as traditional wireline carriers lose market share to cost-effective mobile telephony.

To combat mobile operators, traditional wireline carriers are fighting back with new technologies – embracing cost-effective broadband access services such as DSL, which has evolved beyond its initial role as a broadband access technology and is fast becoming a platform for new services such as Voice over Internet Protocol (VoIP) telephony.

VoIP service can easily take revenue away from traditional fixed-line operators. On the other hand, with the right strategy, it could mean that service providers will be able to offer mobile voice services at lower costs – or receive higher margins.

Similarly, the raw per-megabit billing opportunity for "3G" mobile data is withering under the proliferation of unlicensed Bluetooth and WiFi wireless networks backed by wireline broadband Internet access. Mobile operators need services such as multimedia messaging to justify their next-generation network rollouts. They don't want their customer base to access online content from unlicensed networks.

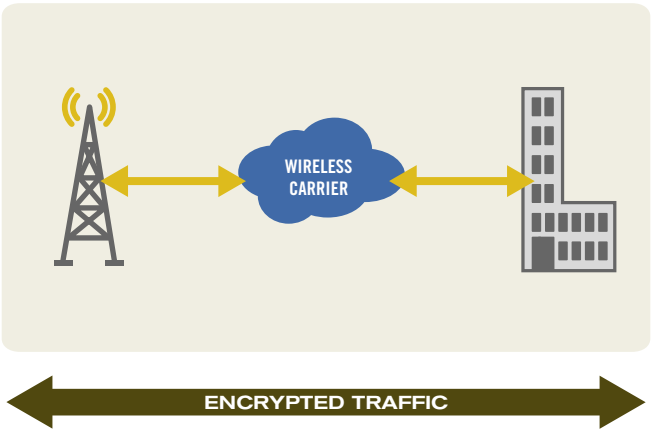

Figure 1: *Wireless Services Today: Each wireless carrier is responsible for the security of their individual networks, from their servers to the device level. This can be very costly when service is stolen or fraud is committed.*

Combine two hot new technologies – unlicensed wireless access and broadband VoIP – and things get interesting. The whole telecommunications industry is watching as companies begin to plan for this convergence. In most circles this convergence is being referred to as Unlicensed Mobile Access, or UMA. UMA technology allows wireless carriers to use cheaper connectivity options but in some cases they may not control or trust the network they are using. This creates a strong requirement for security to prevent an erosion of privacy that customers have come to expect.

This paper examines the requirements for securing UMA networks and describes how the Certicom Security Architecture is an ideal answer – offering the strong security while providing for ease of use and performance.

UMA and its Requirements

From the user perspective, consumers must trust their telephone networks to be inherently secure – otherwise they aren't interested. From the operator perspective, if you can't secure a service, you can't bill it. If you can't bill it, it's not a service. Providing billable services across untrusted networks requires strong, efficient, interoperable security protocols.

Ease of use, interoperability and security are critical to mainstream adoption. Case in point is Bluetooth. Although off to a slow start, Bluetooth is now being built into 20% of the world's mobile handsets, putting deployment of Bluetooth enabled phones at almost 100M devices. WiFi, too, has suddenly taken off, surpassing even Bluetooth in hype and expectation – after growing security concerns were addressed. Handled properly, UMA also stands to experience the same type of adoption.

An unlicensed network uses "license exempt" or "license free" radio spectrum for connectivity, using technology such as WiFi or Bluetooth for network access. When combined with mobile handset technology this is termed "unlicensed mobile access".

Consumers and business users will ultimately benefit from this revolution in telecommunications. First, however, the industry needs to solve the challenge crucial to every network operator– creating secure, billable, user friendly services.

The burden of the new specifications will fall especially to handset vendors, who need to quickly develop new dual-mode (UMA/traditional wireless) devices that are user friendly, support rigorous security requirements, and meet industry interoperability requirements.

UMA technology establishes a standard for seamless hand-off and roaming between a cellular network and fixed IP-based wireless networks, such as Wi-Fi or Bluetooth. This is applicable for data, but the important application is voice. Potentially, this means that specially equipped mobile handsets could transparently connect to Bluetooth wireless access points in the home. Wireline networks transport calls using VoIP rather than using a traditional cellular network. This is true

fixed/mobile convergence, where one handset is all you need at home, in the office, or on the road. It's an ideal solution for a company like British Telecom (BT) with customers in its traditional fixed line telephony (BT Retail), broadband VoIP (BT Broadband) and mobile virtual network operator (BT Mobile) customers.

VoIP in traditional IP networks currently lacks full-featured security support. Signaling can be secured by running SIP protocols over an SSL connection but SSL can't encryption the voice channel, which contains the actual conversation. The UMA requirements for mobile handoff and roaming are more complex, because it must be able to securely traverse an untrusted network.

The easiest approach to accomplish this is to create an encrypted tunnel. UMA (www.umatechnology.org) and 3GPP (3GPP – 3rd Generation Partnership Project) have chosen IPSec, one of the oldest and most proven IETF security protocols. IPSec has proven to be an extremely versatile protocol and has evolved from a network layer protocol to a common remote access protocol.

Typically a remote access IPSec tunnel is established by authenticating the user to a VPN gateway. This is accomplished with a password, a SecurID token or a digital certificate. For a voice connection this level of authentication is not practical and the UMA group is proposing to use the SIM authentication.

SIM authentication can authenticate the device and allow the wireless service provide to re-use their investment in existing authentication, authorization and accounting (AAA) services. All GSM and GPRS networks use a SIM to provide authentication today and the SIM is a key component to their accounting process.

Additionally, in order to use the proven security of IPSec in mobile handsets it had to be extended with new authentication schemes specific to the 3GSM and GPRS services. As a result, both UMA and 3GPP have proposed extensions to the IETF for IPSec. These are being handled as part of the 3GPP 33.234 working group and the IETF IKEv2 draft (draft-ietf-ipsec-ikev2-11.txt).

IKE, or the Internet Key Exchange, provides the initial negotiation of the IPSec and sets all the required parameters for the tunnel (i.e. encryption type, authentication type, etc). It's been several years since IKE was developed and it's been extended by various vendors using proprietary systems. The IKEv2 RFC provides a more common standard for companies to interoperate and includes support for a number of new features. One of these new features is support for EAP (Extensible Authentication Protocol), which replaces the aging XAUTH (Extended Authentication) protocol.

EAP provides similar functionality to XAUTH, in that passwords and SecurID tokens can be authenticated as part of the IPSec tunnel negotiation. But EAP provides a much more standardized

approach to handling this authentication and provides a number of security enhancements including the encryption of the authentication exchange.

For the UMA and 3GPP, the key component to EAP is the ability to extend it to provide support for new authentication systems. As a result EAP-SIM authentication is a key requirement and provides a mechanism to authenticate the SIM in a similar process to GSM and GPRS authentication that happens today on wireless networks. This allows wireless services providers to integrate UMA-based systems into their existing accounting systems with minimal impact.

The Challenge: Choosing the Right Solution

Even with the complexity of UMA, the opportunity is to valuable to pass up. Operators and mobile handheld manufacturers are being forced to integrate it into their already busy development schedules. This is pushing them to either re-evaluate their project plans or look for a solution from a trusted vendor.

Operators are expanding their networks to allow for UMA deployments and pushing mobile handheld manufacturers to include the necessary UMA functionality. The implementation of UMA mainly involves the selection and integration of products from a variety of vendors. The operator must take care select a UMA-compliant VPN solution and integrate it into their existing authentication and accounting systems.

For mobile handset manufacturers, UMA technology must be integrated into their products with minimal impact for the user. In many cases this means creating a virtual radio stack and hiding much of the enhanced security that is provided as part of the UMA. One of the key components in this process is the selection and inclusion of an IPSec toolkit capable of handling the UMA specifications. The toolkit must be small and efficient to maximize the resources of the phone and not substantially increase the cost of the device.

IPSec toolkits are available from a variety of sources today but many include a number of hidden costs. IPSec is a complex protocol and an all-purpose implementation may not include support for commercial gateways. Many of the general IPSec implementations assume you will be developing both the client and the gateway. As a result they provide no specific compatibility or interoperability with other commercial implementations. General IPSec implementations may not support new protocols or extensions on the same schedule as the device release. This can leave mobile handheld manufacturers struggling to implement complex security extensions, which are outside of their core competency.

Higher performance can also be achieved by focusing on the client-side IPSec implementation

and using very efficient cryptography like AES and Elliptic Curve Cryptography (ECC). The AES protocol provides the bulk encryption and ECDH or ECMQV does the key exchange. The combination allows a relatively slow processor to encrypt data at high rates.

Certicom Products for UMA

The Certicom Security Architecture for Mobility can provide an ideal solution for UMA.

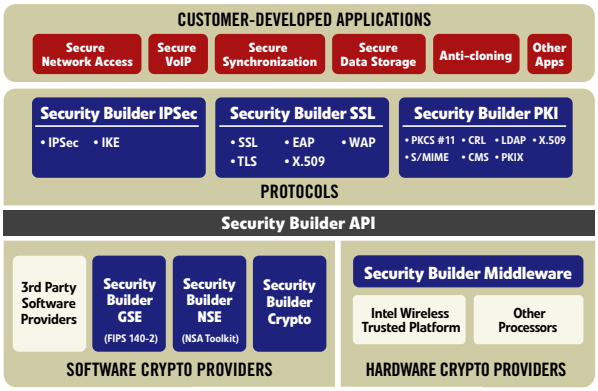

Figure 2: *The Certicom Security Architecture*

The Certicom Security Architecture for Mobility is a comprehensive, cross-platform security solution for developers designed to address the challenges of embedding security in mobile handsets. It allows handset manufacturers to build secure applications that can be quickly and cost-effectively embedded across multiple families and generations of devices, and rounds out the ability of mobile processor vendors to deliver designs that are optimized for strong, high performance handset security.

The Certicom Security Architecture for Mobility consists of a modular set of security protocol toolkits, software cryptographic providers, and middleware required to integrate complete security that leverages both software and hardware.

In short, this platform provides complete security that can be embedded in a timely, cost-effective manner.

The Certicom Security Architecture for Mobility includes:

- **a modular set of security protocol toolkits**
  - **Security Builder® IPSec™: client-side virtual private network toolkit**
  - **Security Builder® PKI™: digital certificate management toolkit**
  - **Security Builder® SSL™ complete Secure Sockets Layer security protocol toolkit**

- **software cryptographic providers**
  - **Security Builder® Crypto™: cross-platform cryptographic toolkit**
  - **Security Builder® GSE™: FIPS 140-2 Validated cryptographic toolkit**
  - **Security Builder® NSE™: cryptographic toolkit for national security information**

- **a hardware abstraction layer that has been optimized for a specific chipset**
  - **Security Builder® Middleware™**

All components of the Certicom Security Architecture for Mobility are pulled together by a single common API, Security Builder® API™, that sits between the protocols and cryptographic providers, and enables access to the fastest and/or strongest security on the device, whether it resides in hardware on the chipset or in the software cryptographic provider.

The API acts as a common cryptographic interface that reduces the security learning curve for developers while providing access to a wide variety of cryptographic and security solutions.

Protocols

Security Builder IPSec

Security Builder IPSec is the key product of the Certicom Security Architecture for UMA designs. Certicom developed Security Builder IPSec for mobile handheld manufacturers that require a very efficient implementation for their products. Security Builder IPSec has been extended to provide support for the UMA and 3GPP specifications and allow device vendors to quickly integrate into their devices. It maintains preconfigured compatibility with leading VPN vendors and is available on a number of different platforms.

The intuitive interface and API allow vendors to add IPSec security to a variety of platforms (including Windows Mobile, Linux and Palm), with a total code size between 150 KB and 600 KB.

Security Builder IPSec supports the following algorithms:

- AES (128,192 & 256 bit) 3DES and DES
- ECDH163 & ECDH 283 (Group 7 & 9)
- DH768, DH1024, DH1536 (Group 1, 2 and 5)
- SHA-1, MD5

Security Builder SSL

Security Builder SSL is a complete Secure Sockets Layer protocol toolkit for enabling secure and efficient SSL/TLS transmission of data. The toolkit provides security support for public and symmetric key algorithms including ECC and supports the following protocols: SSL 2.0, SSL 3.0, TLS 1.0, WAP 2.0, EAP-TLS, EAP-TTLS, EAP-PEAP.

Security Builder PKI

Security Builder PKI is a comprehensive digital certificate management toolkit that can be used to add additional support for digital certificates or public key infrastructure. It supports CMS for the development of S/MIME applications, interoperates with third-party PKIs and CAs, and complies with the following industry-standards: IETF-PKIX, PKCS, ANSI, and ISO.

Cryptographic Providers

UMA security can also be enhanced with support from the addition of the following cryptographic providers.

Security Builder Crypto

Security Builder Crypto can augment the security provided by the hardware cryptographic provider by offering highly efficient implementations of the most widely used cryptographic operations. It is available on more than 30 different platforms (operating systems and chipsets). It provides a complete suite of cryptographic algorithms for developers to easily integrate encryption, digital signatures, and other security mechanisms into applications.

Security Builder GSE

For developers who need to meet the stringent security requirements of government customers, Certicom offers Security Builder GSE, which allows you to incorporate a complete FIPS 140-2 Validated cryptographic module or individual FIPS-approved algorithms into your products without having to submit your application through the lengthy and costly FIPS approval process.

Security Builder NSE

Security Builder NSE enables organizations to quickly build applications that meet the field-of-use guidelines set out by the National Security Agency (NSA) to protect mission-critical national security information. The Security Builder NSE toolkit covers the technology that was part of the 26 patents licensed by the NSA from Certicom plus optimized implementations. It also includes support for ECC-based algorithms such as ECDSA, ECMQV and EC support for S/MIME, TLS and IKE.

Security Builder Middleware

Security Builder Middleware is a hardware abstraction layer that links Security Builder API, and thereby all security services, to a specific hardware cryptographic provider. It wraps the cryptographic features given by the hardware cryptographic provider in a series of registration functions. Applications call one or more registration functions in Security Builder Middleware to link in the cryptographic features from the cryptographic provider.

The advantage of using Security Builder Middleware and Security Builder API together is that the differences among hardware cryptographic providers are abstracted away. For example, if your application accesses features enabled by one Certicom-supported provider, but you now wish to use an implementation from another Certicom-supported provider, all you have to do is “plug-in” or register Security Builder Middleware for the new provider.

The UMA Network: Secured

Using UMA, carriers can now provide their customers with wider access at less cost to them. A mobile handset can now securely access two types of networks: the traditional 3G wireless carrier network that uses its own encryption, and an open and previously “untrusted network”. IPSec provides the protocols needed to securely communicate using a VoIP gateway (se Figure 3).

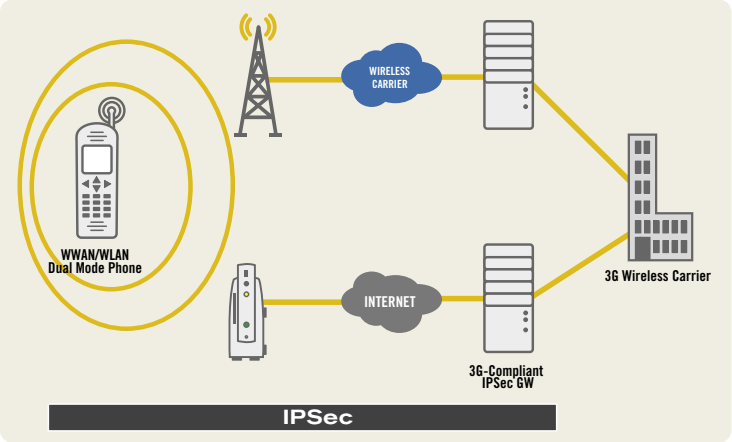

Figure 3: *The UMA Network*

Whether at home, in the office, or on the road, users always expect to be able to use the fastest Internet connection available. UMA provides a means for them to use these connections for voice traffic in a security and reliable environment. By preparing for UMA now mobile operators and mobile handheld manufacturers can be well position to leverage a new customer growth segment.

certicom™

About Certicom

Certicom Corp. (TSX: CIC) is the authority for strong, efficient cryptography required by software vendors and device manufacturers to embed security in their products. Adopted by the US Government's National Security Agency (NSA), Certicom technologies for Elliptic Curve Cryptography (ECC) provide the most security per bit of any known public key scheme, making it ideal for constrained environments. Certicom products and services are currently licensed to more than 300 customers including Motorola, Oracle, Research In Motion, Terayon, Texas Instruments and XM Radio. Founded in 1985, Certicom is headquartered in Mississauga, ON, Canada, with offices in Ottawa, ON; Reston, VA; San Mateo, CA; and London, England.

certicom™

Certicom White Papers

To read other Certicom white papers, visit www.certicom.com/whitepapers.

The Inside Story

Many Happy Returns: The ROI of Embedded Security

Wireless Security Inside Out (authored by Texas Instruments and Certicom)

Welcome to the Real World: Embedded Security in Action

Sum Total: Determining the True Cost of Security

The Elliptic Curve Cryptosystem for Smart Cards

Elliptic Curve DSA (ECDSA): An Enhanced DSA

Formal Security Proofs for a Signature Scheme with Partial Message Recovery

Postal Revenue Collection in the Digital Age

An Elliptic Curve Cryptography Primer

ECC in Action: Real World Applications of Elliptic Curve Cryptography

Using ECC for Enhanced Embedded Security: Financial Advantages of ECC over RSA or Diffie-Hellman

Good Things Come in Small Packages: Certicom Security Architecture for Mobility

certicom™

Contact Certicom

Corporate Headquarters

5520 Explorer Drive
Mississauga, Ontario
L4W 5L1
Tel: +1-905-507-4220
Fax: +1-905-507-4230
E-mail: info@certicom.com

Sales Offices

Canada

5520 Explorer Drive
Mississauga, Ontario
L4W 5L1
Tel: 905-507-4220
Fax: 905-507-4230
E-mail: info@certicom.com

Ottawa

84 Hines Road
Ottawa, Ontario
K2K 3G3
Tel: 613-254-9270
Fax: 613-254-9275

U.S. Western Regional Office

1810 Gateway Drive, Suite 220
San Mateo, CA 94404
Tel: 650-655-3950
Fax: 650-655-3951
E-mail: sales@certicom.com

U.S. Eastern Regional Office

1800 Alexander Bell Dr., Suite 400
Herndon, Virginia 20190
Tel: 703-234-2357
Fax: 703-234-2356
E-mail: sales@certicom.com

Europe

Golden Cross House
8 Duncannon Street
London WC2N 4JF UK
Tel: +44 20 7484 5025
Fax: +44 (0)870 7606778

www.certicom.com