



# **Wireless Security: from the inside out**

building security into the OMAP™ platform

**A Technology and Business Review from Certicom and Texas Instruments**

January 2003

Over the next few years,

more than 50 percent of enterprises will deploy

PDA's and smart phones for communication,

coordination, planning and

other corporate activities.

*Source: META Group, 2002*

Within a relatively short time, wireless communication has evolved from a novelty to a part of everyday life. The question now for consumer and corporate users is: "What are the possibilities?"

The pursuit of answers to that question has generated a growing demand for new, increasingly sophisticated wireless services; a demand that's being met aggressively by service providers and device manufacturers.

Yet as wireless services become more complex, enabling the exchange of personal, sensitive and proprietary information, the associated security risks intensify. This presents device manufacturers with a considerable challenge: to build in powerful, flexible and scalable mechanisms for protecting user data without compromising performance.

Certicom and Texas Instruments have worked together to address this challenge, integrating security functionality directly into a sophisticated, high-performance mobile-applications platform.

## The wireless world

While both consumers and enterprises contribute to the rising demand for new wireless services, their needs and expectations are not identical. Consumers are principally interested in messaging (SMS and MMS), personalization and accessing the web. Their reasons are many: to stay in touch, to download ring tones, view weather reports or stock prices, check email, buy products or play games.

Enterprise requirements are more complex, often involving the extension of internal applications to wireless users. These can range from calendar and email programs to customer relationship management, sales force automation and inventory applications.

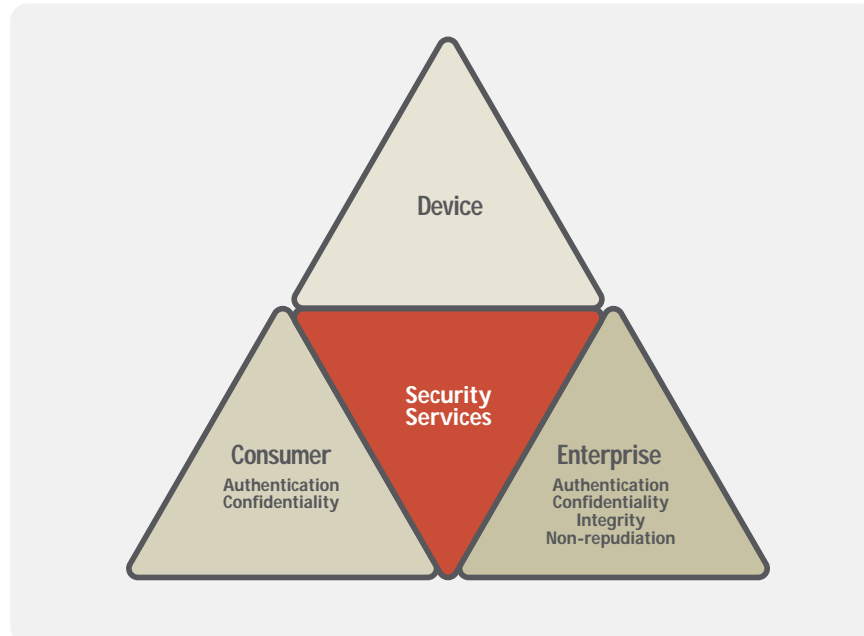
Consequently, the wireless security needs of the two groups vary considerably. Consumers may be sufficiently protected by firewalls, secure http connections and anti-virus software. Authentication—a key element of any security solution—may be handled adequately by a user's service provider alone.

Enterprise security is more intensive, demanding stronger methods of encryption (such as AES, which is required for any U.S. government security solution), access control and authentication. Virtual private networks (VPNs) allow an organization to extend the protective reach of its existing security infrastructures. That infrastructure may have its own authentication function built in, in the form of a RADIUS server, for example, or Public Key Infrastructure(PKI).

Need	Consumer	Enterprise
Confidentiality	X	X
Integrity		X
Availability	X	X
Compliance		X
Identification	X	X
Authentication	X	X
Authorization		X
Accountability		X
Affordability	X	X
Non-repudiation		X
Disaster recovery		X
Flexibility	X	X

What does all of this amount to? A recognition that the same device in the hands of different users may be required to deliver widely varying levels of security—making it necessary for manufacturers to include a rich, flexible and interoperable set of underlying security components.

Before discussing those components, it is important to understand the nature of the security threats that wireless technologies face.



*Enterprises, consumers and devices all need their own forms of protection.*

## Device risks

There are over 20 million handheld PDAs and one billion mobile phones in use today: all employed for a vast range of personal and professional purposes; all boasting increasingly sophisticated capabilities. Much of the information stored on those devices would be considered—if you asked the users—to be confidential, such as PIN numbers, corporate passwords, customer data and contact information, bank account numbers, credit card numbers, appointments and contacts. Yet few corporations today have security policies in place to govern the use and protection of this portable information.

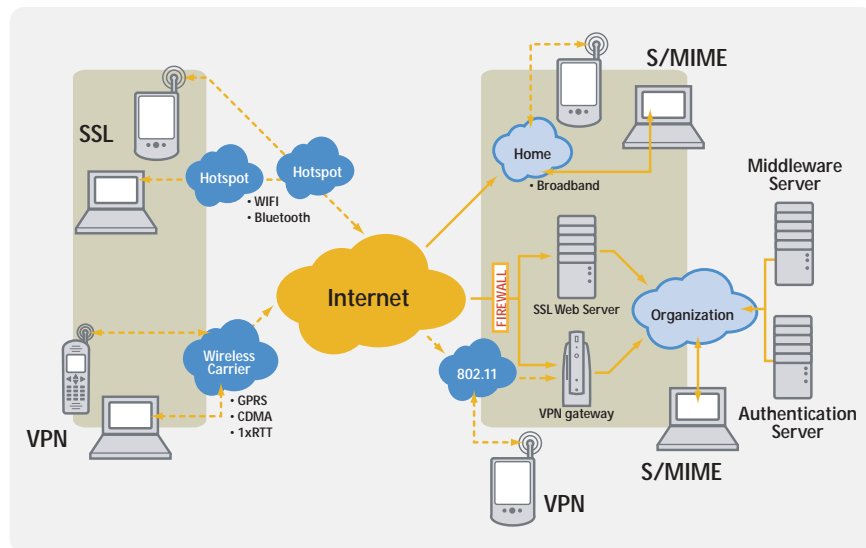
That is a somewhat unnerving thought in light of the fact that approximately six percent of all PDA owners have reported losing their devices, with the unsecured contents becoming accessible to whomever happens along.

## Connectivity risks

In addition to protecting the information stored on a device, there is an equally pressing need to protect data in transmission between wireless devices and their networks. This latter requirement is made particularly complex by the growing variety of connectivity options available to wireless users.

Today's handheld devices have the ability to access wireless wide-area network (WAN) services based on GSM/GPRS and CDMA/1xRTT infrastructures. IEEE 802.11b-standard wireless 'hot spots'—i.e. wireless access points—allow users to take advantage of local fast-access services where available. Switching from WAN to LAN in this way is desirable because wireless WAN services are usually billed on a per-use basis and can quickly become costly. Wireless LANs also afford much greater bandwidth at dramatically lower cost.

The same security technologies and standards in the wired world can and are being deployed in the wireless world. Remote users today can get web mail through a web browser interface secured by SSL; they can get general enterprise access through a secure IPSec VPN and have end-to-end secure messaging through an S/MIME plug-in for a mail client. These security technologies operate independently of the wireless infrastructure and work with existing enterprise security architectures. How—and where—devices connect to networks affects their security vulnerabilities.



*How—and where—devices connect to networks affects their security vulnerabilities.*

Short-range standards such as Bluetooth make it possible for users to synchronize their wireless devices locally without having to establish any kind of physical connection via a cradle.

Each technology has its own attendant vulnerabilities. Standards groups are working with great determination to overcome these, however they've not been successful thus far. For example, Wired Equivalency Privacy (WEP), which was designed for 802.11b applications, has been comprehensively broken. Potential solutions for WAN users have not fared much better.

Multiple security technologies work well on PC platforms where memory, power and bandwidth is almost unlimited. On a constrained device, however, you cannot afford to have a number of independent implementations where much of the underlying security is essentially replicated. Not only does this use valuable memory but it is much slower and potentially susceptible to many security threats.

The conclusion, then, is that security is best embedded within the architecture of the device itself as a common, robust Cryptographic Service Provider (CSP), rather than delivered externally via an add-on component or cumbersome extension. The embedded security components can take advantage of a number of "on-chip" facilities from hardware acceleration to a secure execution environment. The embedded CSP enables application developers to deploy lightweight, standard security applications that are found today in the wired world.

Finally, any security solution adopted must be transparent to the user and exert minimal impact on device performance.

A manufacturer's first crucial choice is between adopting a third-party security add-on or an integrated solution.

## The challenge to manufacturers

Adding new core functionality to a wireless device presents a number of challenges, especially when that functionality is as sophisticated and potentially resource-intensive as security. Those challenges, listed below, apply more or less equally to manufacturers with a cost-of-goods-sold philosophy—whose roots are typically in the cell phone world—and those with a computing philosophy who depend on Moore's law to drive price performance into an acceptable range for customers.

### Development time

Time to market is a key success factor for device manufacturers; getting products onto shelves ahead of the competition and in time to capitalize on calendar-based opportunities such as the Christmas shopping window. Consequently, any new functionality must be added and integrated easily and rapidly.

## Performance

No one feature is so appealing to users that they're willing to sacrifice the overall performance of a wireless device—or, for that matter, its battery life. Manufacturers, then, must constantly strive for an optimal balance between what a device can do, and how well it can do it.

## Interoperability

Because, as has already been discussed, wireless users are presented with ever-increasing options for connectivity, it is essential that devices maintain compatibility with established and emerging open standards.

## Reliability

If a new feature introduced to a wireless device proves to be unreliable, it can become a significant—even fatal—liability. Much of the security technologies required operate at the core of the operating system. Imagine downloading a secure application into a smartphone that disrupts voice communication. A “secure computing environment” where code is digitally signed by the manufacture is necessary. This is perhaps most pointedly true of security. A hacker's exploitation of a security weakness could kill sales into many vertical markets.

## Cost

Unlike the PC environment where memory, power and bandwidth is assumed almost unlimited, the handheld can only do so much before costs force a device to be uncompetitive. Code duplication must be eliminated and optimizations must be performed to stay competitive.

Given these five considerations, a manufacturer's first crucial choice is between adopting a third-party security add-on or an integrated solution. The former requires a greater amount of integration work and can be complex and unwieldy. The latter is therefore preferable but, to be truly satisfactory, must come tightly integrated and include all core security functionality—a tall order, to be sure. Working together, however, it's an order that Certicom and Texas Instruments have successfully filled.

The OMAP platform is designed for real-time, multimedia-rich products such as 2.5G and 3G wireless handsets and PDAs.

## The OMAP platform integrated security solution

The combination of Certicom's wireless-security expertise and Texas Instruments' proven OMAP processors have produced a complete, fully integrated and trusted platform for the development of next-generation wireless devices—one that answers all of the manufacturer challenges outlined in the previous section.

TI's OMAP platform is comprised of high-performance, power efficient processors, a robust software infrastructure and comprehensive support network for the rapid development of

## Power + performance

Simple API allows developers to focus on system-level issues; eliminates hardware security-integration process.

Interoperates with proven standards and protocols, including SSL, IPSec, PKI and authentication standards.

Cryptographic acceleration, secure key-storage and true random-number generation operations are all done on the chip.

Offloading public-key to DSP increase speed of operations.

Achieves all of the above with extreme code efficiency and minimal footprint.

differentiated internet appliances, 2.5G and 3G wireless handsets and PDAs, and other multimedia-enhanced devices. The capabilities of these processors are harnessed by an open, easy-to-develop software infrastructure that supports the industry's most prevalent operating systems.

Certicom has worked in partnership with Texas Instruments to integrate sophisticated security capabilities into the latest OMAP wireless processors, the OMAP730 and OMAP1610 devices. This core cryptographic module includes cryptographic functions, communications protocols and PKI functionality.

These new OMAP processors are also distinguished from their predecessors by the addition of hardware accelerators (provided in association with a third party), which are capable of supporting DES, Triple DES and other key standards-based security operations. The added hardware and associated firmware enable advanced functionality such as a secure execution environment, accelerated crypto algorithms, and low-power security protocols.

### OMAP730 device

A single-chip solution, the OMAP730 device combines a Texas Instruments digital signal processor (DSP)-based GSM/GPRS modem baseband subsystem with a TI-enhanced ARM microprocessor for real-time voice and wireless data applications—making it the most thoroughly integrated smartphone processor available on the market today.

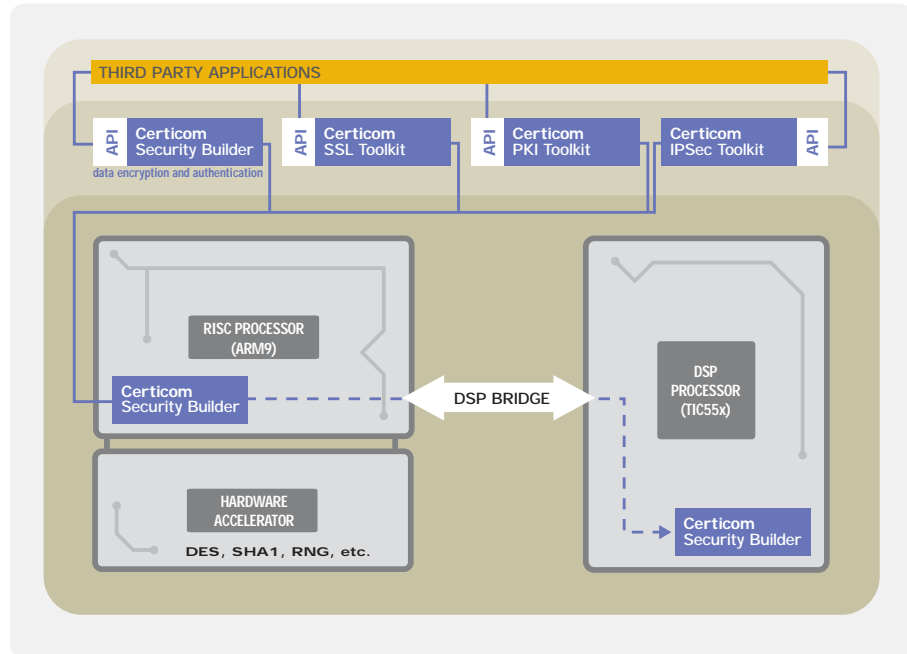
### OMAP1610 device

This dual-core processor features a Texas Instruments-enhanced ARM microprocessor plus a high-performance, low-power DSP with the express purpose of accelerating security and multimedia applications. By shifting processor-intensive cryptographic functions off the main processor and onto the DSP, the 1610 device frees up much-needed headroom. Its open software architecture renders the activity of the dual-core processor transparent to users, and at the same time simplifies programming and integration for developers.

A high-end, enterprise-class processor, the OMAP730 and OMAP1610 devices provide:

- true hardware-based random-number generation;
- crypto hardware accelerators supporting DES, Triple DES, AES, SHA-1 and other standards-based security operations;
- a secure bootloader for device-code integrity including code signing; and
- a secure-execution mode, enabling secure key storage and runtime authentication.

Both the OMAP730 and OMAP1610 devices are supported by familiar and easy-to-use toolkits and APIs.



*With Security Builder embedded, and a range of APIs available, developers can create exactly the security solutions they need.*

## Building security

Certicom wireless security solutions are optimized for precisely this kind of embedded functionality. Ultra-secure and capable of carrying out high-performance cryptography, they are designed for maximum scalability and openness, supporting virtually every wireless standard.

Certicom’s cryptography suite eliminates the need to integrate multiple security toolkits; its intuitive API reduces the need for device manufacturers to maintain extensive cryptographic expertise. This is because all toolkits are built on the foundation of Certicom Security Builder using a single API. As a result, making changes or additions (for example, adding SSL) is a simple and efficient process, as the base cryptographic functionality does not have to be re-created.

The functionality available for the OMAP platform includes:

### Security Builder®

A core, standards-based cryptographic software-development kit that, within a small footprint, enables strong, efficient security for any application and offers comprehensive algorithm support. It offers a complete suite of algorithms for developers to easily integrate encryption, digital signatures and other security mechanisms into applications.

### **SSL Plus™**

This widely deployed commercial SSL toolkit enables rapid integration of standard network security, working with all major implementations and browsers, and with certificates from major certificate authorities. It supports a wide range of encryption algorithms and authentication protocols to provide the ultimate security with high performance in a small size.

### **PKI Toolkits**

This flexible platform enables developers to build and deploy any trust model across mobile devices, desktops and servers, both wired and wireless. It allows developers to add robust PKI security and offers wide cryptographic support.

Perhaps the most important characteristic of Certicom's security technology is its minimal code base. Designed specifically for the performance and bandwidth requirements of resource-constrained devices, its code size ranges between 4K and 200K, depending on the functionality in use. In contrast similar PC-based application code sizes are in the megabytes.

Taking advantage of every available economy, it occupies a small, unobtrusive footprint—leaving considerable space free for other programming elements. And unused algorithms can be compiled out easily, allowing developers to pare down further to exactly the features their particular applications require.

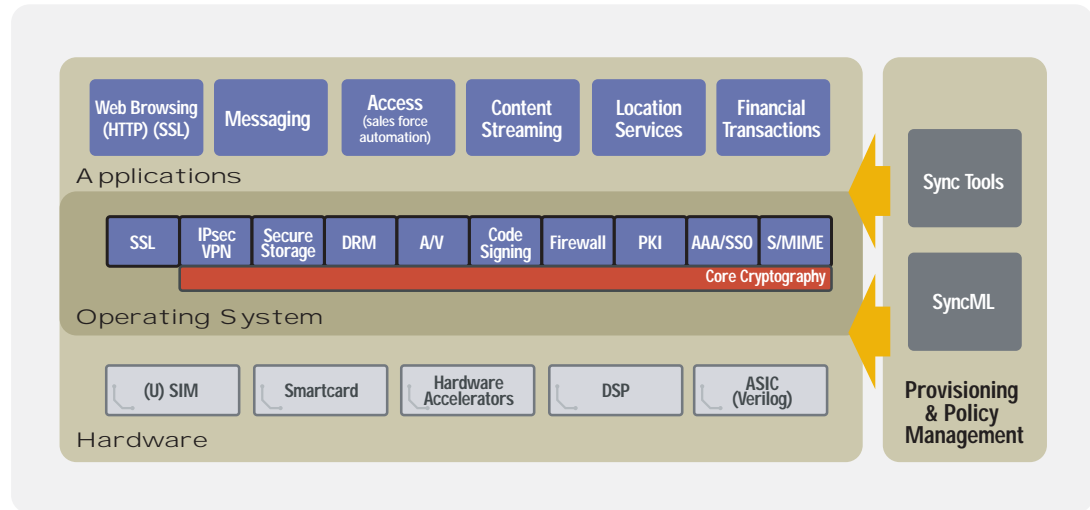
As well, Security Builder is the only embedded toolkit to provide efficient elliptic curve cryptography (ECC) to accelerate processing speeds, prolong battery life and improve bandwidth utilization by a factor of 10x over RSA.

ECC is now gaining significant attention now because unlike RSA, its key sizes scale linearly with the new encryption standard AES for the equivalent amount of security. This means highly secure and fast security for the foreseeable future. All the major standards bodies have adopted ECC-based protocols such as ECDSA digital certificates and MQV key agreement.

## **From a system perspective**

The diagram which follows illustrates a network security architecture for the future of wireless handhelds. In order to deliver a rich set of applications, a number of standards-based security protocols are required. These are built on a common cryptographic service provider that had direct access to hardware facilities and is optimized to run on the target processor.

In other words, the solution can act as the device's cryptographic service provider (CSP). Security components in the operating system—algorithms, SSL, IPsec, PKI, etc.—execute natively on the OMAP platform at the hardware level and take advantage of the many resources available there, from acceleration to security-object storage.



OMAP platform enables seamless interoperation between applications, operating systems and device hardware.

What's perfectly clear is that wireless security is a necessity, and that need will only continue to grow over time.

## Meeting the need

Securing today's—and tomorrow's—wireless devices is complicated by the fact that so much varies depending on who the users are, what kind of information they're dealing with, their mode of network access, and the nature of the existing security infrastructures they may be interacting with.

What's perfectly clear is that wireless security is a necessity, and that need will only continue to grow over time. While standards and protocols wrestle with liabilities at the network level, manufacturers have an opportunity to provide their customers devices that offer a full range of built-in security capabilities.

Of course, this must be done in a way that allows manufacturers to meet a number of key requirements. The integrated security solution from Certicom and Texas Instruments for the OMAP platform does exactly that.

### Time to market

This solution provides a simple API and suite of toolkits for ease of development; all underlying security functions—from basic algorithms to full protocols—have been completely integrated. As a direct result, development and product-integration times are accelerated, making security-related initiatives entirely feasible.

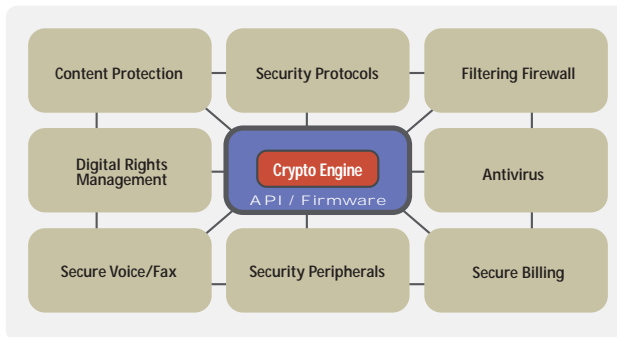
### Performance

Certicom and Texas Instruments have worked together to optimize performance on each OMAP

processor, the 730 and the 1610 devices—building on an understanding of resource limitations faced by wireless devices. Because of this optimization, battery life is preserved along with processing power. The economical code base of Certicom’s proven security technology introduces a remarkable degree of scalability and flexibility, allowing developers to start small and to compile out any elements unnecessary to their particular applications.

### Single-vendor simplicity

By offering a fully integrated solution, Certicom and Texas Instruments eliminate a host of requirements for integration and testing that would be necessary with the use of an add-on third-party security solution. Interoperability is not a concern; Certicom’s technology has proven its successful compliance with open standards.



*The OMAP platform helps manufacturers build security into their devices—enabling protection on multiple fronts according to user requirements*

movian by Certicom applications can be built to further enhance device performance by capitalizing on the integrated cryptography of the OMAP platform. This adds the final element to a complete offering that meets all the requirements for true, trusted wireless security.

Ultimately, what Certicom and Texas Instruments provide is a trusted platform for developing simple or sophisticated security applications for next-generation wireless devices, giving manufacturers the tools they need to meet market expectations and, at the same time, their own business requirements.

## Other Whitepapers from Certicom

*Advances in Cryptography -ECC,Future Resiliency,and High Security Systems*

*The Elliptic Curve Cryptosystem for Smart Cards*

*An Introduction to Information Security*

*Current Public-Key Cryptographic Systems*

*Remarks on the Security of the Elliptic Curve Cryptosystem*

*Elliptic Curve DSA (ECDSA):An Enhanced DSA*

*Enabling wireless security -extending the benefits of mobility to government*

*Extending the benefits -enabling wireless security in the enterprise*

These whitepapers are all available from [www.certicom.com/resources](http://www.certicom.com/resources)

## About Certicom

Certicom is a leading provider of wireless security solutions, enabling developers, government and enterprises to add strong security to their devices, networks and applications. Designed for constrained devices, Certicom's patented technologies are unsurpassed in delivering the strongest cryptography with the smallest impact on performance and usability.

## About Texas Instruments

Texas Instruments Incorporated, the market leader in wireless technology, offers the most complete portfolio of chipset solutions, hardware and software reference designs and OMAP application and modem processors that enable voice and multimedia enhanced applications for 2.5 and 3G wireless phones, PDAs and mobile Internet appliances. Adopted by leading wireless manufacturers including Nokia, Fujitsu, Palm, Sendo, HTC, Panasonic and others, TI wireless technology delivers the optimal combination of high-performance and low power consumption and is scalable to address any market segment. In addition, the OMAP platform offers support for leading operating systems, a broad network of OMAP Developers creating exciting applications and services for mobile devices and worldwide integration services offered by independent OMAP Technology Centers. For more information visit <http://www.ti.com/sc/wireless/>