certicom™

# Good Things Come in Small Packages

## An Overview of the Certicom Security Architecture for Mobility

September 2004

# Comprehensive Security: A Mobile Market Opportunity

In the mobility ecosystem, increased consumer market penetration combined with growing competitive pressures are forcing product and service providers to differentiate their offerings with rich new capabilities to drive revenues and replacement rates. To protect these new revenue streams as well as private user information, comprehensive security is quickly becoming mandatory for mobile environments. Fraud, theft and design portability issues have shown that security is best embedded within a mobile device, rather than adding security late in the design process. Certicom has leveraged over 15 years experience to deliver the most comprehensive security platform available to mobile developers – the *Certicom Security Architecture for Mobility*.

The *Certicom Security Architecture for Mobility* allows device manufacturers to quickly and cost-effectively build comprehensive, optimized security into their devices in order to differentiate their phone, drive replacement rates, and satisfy the security requirements of operators, enterprises and end users. It allows handset manufacturers to embed security across multiple families and generations of devices, and rounds out the ability of mobile processor vendors to deliver whole security solutions to their handset manufacturer customers.

This paper describes the business and technical challenges of security facing both groups and how the *Certicom Security Architecture for Mobility* addresses each of them. To put the market situation in perspective, it discusses the overall need for security in the mobile ecosystem and how these needs trickle down to – and create an opportunity for – mobile handset manufacturers and mobile processor vendors.

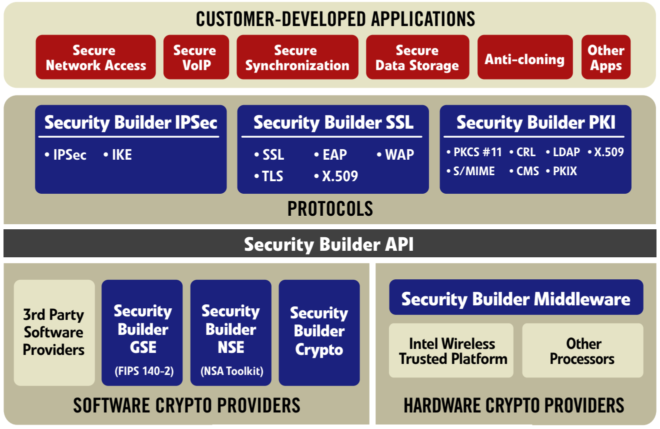


***Figure 1:*** *The Certicom Security Architecture*

# Mobile Market Drivers

## The Mobility Ecosystem

The mobility ecosystem contains several members with cumulative wants and needs. At one end are users – consumers and enterprises – who ultimately drive business for all other members: mobile operators, content providers and finally, mobile handset manufacturers and mobile processor vendors. These last two share many of the same challenges in serving their markets. The diagram below shows the needs of each member, and how these requirements are passed down to the vendors of mobile handsets and mobile processors.

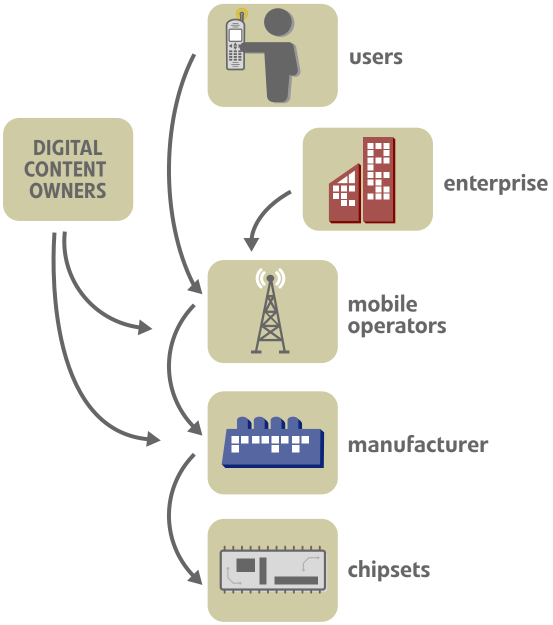


***Figure 1:*** *The Mobility Ecosystem*

New services such as banking, digital media, and networked gaming encourage end user handset upgrades but security risks and poor usability act as barriers to adoption. Replacement business will inevitably flow to the mobile handset manufacturers that can supply these services securely and transparently. In turn, mobile operators will carry the devices of handset vendors that provide the technology required to accomplish these goals.

Enterprises are attracted to wireless devices by the benefits of a mobile work force. To reduce support headaches, IT departments typically standardize on one or two handsets. But prior to deployment, enterprises demand protection for their assets as well as flexible integration with their existing IT security policies. For these reasons, enterprises will be top consumers of secured handsets and applications. The volumes involved in enterprise-wide rollouts make this a very lucrative market for mobile operators.

Digital content owners are also eager to reach users with media like digital video or audio files. A typical content distribution agreement would see a content owner, either directly or through an aggregator, license the mobile operator to offer audio files to the end users. Profits from these services may be split between the mobile operator and the digital content owner. This business model requires strong security to ensure appropriate digital rights management (DRM) for the sake of subscription-based revenue. DRM capabilities define and control the use of licensed content. For example, content use could be locked to a specific device and activities like reproduction and printing could be limited. Thus, content owners will do business with the mobile operators and manufacturers that can guarantee the security of their content.

For their part, mobile operators need to differentiate their products and services from their competition, maintain or grow average revenue per user, reduce subscriber attrition rates, and attract new subscribers. With the maturation of the voice services market, they look to new data services as the solution. To capture this market, a mobile operator must satisfy content owners that their handsets and network are secure. This is also important for limiting their exposure to liability for any illicit use of products or services. To remain competitive, operators need to achieve this while complying with changing mobile regulations, and controlling costs. For mobile operators, the future relies heavily on the revenues that strong security make possible. Mobile operators will only purchase handsets that include the comprehensive security that protects both voice and data services.

Each of these groups: end users, enterprises, content owners and mobile operators, pass their requirements down the mobile handset ecosystem. Ultimately, satisfying these demands is the task of the mobile handset vendors and mobile processor vendors.

**In Q4 2003, the industry wide average selling price for handsets stood at US$171. The previous quarter was US$139. The ASP for the entire market in 2003 was $163, with the ASP for Smartphones at $360, and the ASP for Connected PDAs at $450.**

– (ABI Research, 2004)

## Mobile Handset Vendors: The Business Challenge

To maintain or grow market share, mobile handset vendors must differentiate—and the key to differentiation is innovation. Just as today's PC market maintains relatively static prices and encourages upgrades by continually introducing new features, so too will handset vendors stabilize average selling prices and replacement rates through innovation. Handset vendors face an extremely competitive market where they must balance innovation costs against profit margins. Increasingly this competition is coming from low cost offshore manufacturers as well as large networking vendors who enter the market via their expertise in voice over IP (VoIP) technology.

Differentiating through embedded security allows mobile handset manufacturers to help their customers address the growing problem of theft and fraud in the industry. The US Secret Service estimates losses from telecommunication fraud at more than a billion dollars each year with cell phone cloning representing a large part of this figure.[1] Handset vendors that help operators reduce losses through security will be well positioned to become the handset supplier of choice.

Security is also vital for lucrative markets such as the US government. According to a US Department of Defense directive issued in March 2003, US government departments are required to use solutions that are FIPS 140-2 Validated for sensitive data communications. FIPS 140-2 Validated solutions are also increasingly recognized by other industries that require guaranteed security: including financial and healthcare. While these markets are attractive, the validation process represents a significant barrier to entry. Embedding a previously validated cryptographic module can further differentiate a handset and provide quick access to these markets.

The need to innovate adds to development costs in an environment where time-to-market is exceedingly important. Using embedded security as a means of differentiating handsets can be a complex addition to development schedules. It demands specialized skill sets that can lie outside the core expertise of mobile handset vendors and integration which must be repeated with each new handset design. Today, mobile handset vendors race against accelerated six month development cycles and lengthy security integration is not an option. Embedded handset security must therefore be reusable and portable across product families and generations to avoid hindering release schedules. The Certicom Security Architecture enables this.

**For 2003, the average replacement rate for handsets is estimated to be about 22% worldwide and is expected to rise to about 34% by 2009. Replacement sales accounted for 40% of global sales in 2003, and are expected to rise as high as 87% in 2009.**

– (ABI Research, 2004)

## Mobile Handset Vendors: The Technical Challenge

One of the key lessons learned to date is that security is best embedded. Otherwise, developers add security patches to address specific vulnerabilities within individual applications. These additions may or may not be interoperable and lead to uncertainty regarding the overall security of the platform.

Without a system-wide approach to security, latent vulnerabilities may only be recognized after a successful attack. If the original patch was added on, these weaknesses can be difficult to address. This is also true when trying to extend patchwork security to cover the new features of an evolving mobile handset design.

Embedding security from the ground up adds measurable value. In addition to limiting vulnerabilities by design, new threats can be addressed as they appear. A ground-up approach also allows developers to facilitate the migration of security information by users from one platform to another when they upgrade.

Beyond traditional security integration challenges, there is a significant range of processing power and bandwidth across mobile handset families. As a result, a scalable security system is required and must meet the available memory and battery power requirements, without impacting performance. The problem is compounded by processor and bandwidth-intensive cryptography calculations that negatively impact the user experience in areas such as performance and battery life.

[1] http://www.secretservice.gov/financial_crimes.shtml#Telecommunications

The level of effort required to optimize security performance for a mobile handset creates another hurdle in the form of higher switching and time-to-market costs when a new chipset is required. These costs can be incurred repeatedly across the entire product line. Rather than duplicating effort with each new handset, the Certicom Security Architecture offers a future-proof security strategy that allows manufacturers to use their existing application code when migrating to a new chipset.

## Mobile Processor Vendors: The Business Challenge

Like mobile handset vendors, mobile processor vendors face erosion of average selling prices and are struggling to differentiate their products. The need for new wireless services has converged with the need for comprehensive security to protect consumers and revenue. This situation presents mobile processor vendors with an opportunity to distinguish their products by providing all the security building blocks a mobile handset manufacturer needs.

Incorporating low level security features into the chipset would differentiate the product and contribute to rapid development and chip migration for customers. Performing encryption in hardware is not only faster in terms of performance, it's also more secure because it is tamper resistant. This has led other members of the mobility ecosystem to request hardware-based encryption. However, security is outside the core expertise of most mobile processor vendors. To integrate security cost-effectively, mobile processor vendors can benefit from a partner with mobile security expertise.

## Mobile Processor Vendors: The Technical Challenge

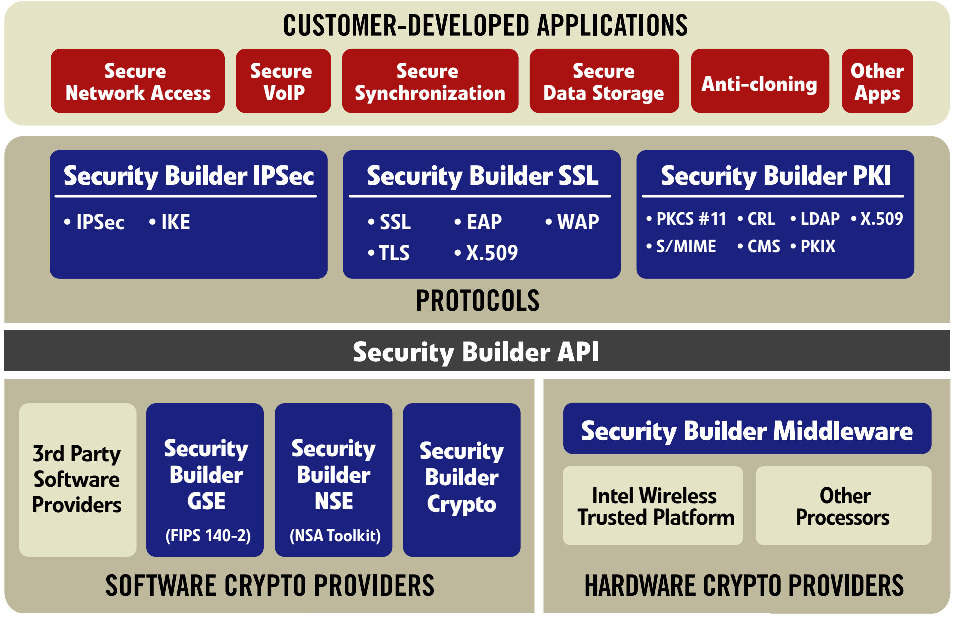
Mobile processor manufacturers also face technical issues in differentiating their products through security. For example, facilitating hardware accelerated encryption or providing low level security features such as key management and secure storage in hardware requires a software adaptor to communicate between higher level protocols and the chip. To leverage security as a competitive advantage, mobile processor manufacturers must supply designs that are completely optimized for security. Customers must be able to call on chip-based security operations from an efficient developer toolkit.

The complexity and computational demands of cryptographic functions means processor vendors need to partner with a mobile security specialist to deliver security solutions to their mobile handset customers that cover the full range of security demands. Like handset vendors, processor manufacturers must continually trade new functionality against performance. The security solution mobile processor vendors choose must provide maximum security with minimum impact on available resources. The Certicom Security Architecture accomplishes this.

**Starting in 2007, the increase in shipments of mobile processors will not offset the downward trend in average selling prices (ASPs) and revenue growth will actually start falling.**

(source: ABI Research, 2004)

# What is the *Certicom Security Architecture for Mobility?*



Mobile handset vendors and mobile processor vendors require all-inclusive security that addresses the business and technical requirements outlined above. Certicom has years of experience supplying security solutions for the mobile industry and has worked with handset and processor manufacturers to provide the platform required by the marketplace: the *Certicom Security Architecture for Mobility*.

The *Certicom Security Architecture for Mobility* is a comprehensive, modular, 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.

The *Certicom Security Architecture for Mobility* includes:

- **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 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
- **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.

This approach allows developers to standardize on one cryptographic API across all of their mobile devices and across one family of toolkits. By coding security features to a common API, manufacturers can change chipsets, or take advantage of new features in their existing chipsets, without re-integrating or re-writing all of their security code.

The authentication, integrity and privacy required for effective mobile handset security can only be provided by a public key cryptosystem that is effectively integrated with symmetric cryptosystems. Certicom has years of experience developing standards-based cryptography that is already optimized for mobile environments and is the acknowledged leader in elliptic curve cryptography (ECC). Certicom technologies for ECC provide the most security per bit of any known public key scheme making it ideal for use in mobile devices constrained by memory, processing power and bandwidth. ECC has been incorporated into a number of key international standards including ANSI, IEEE, IETF and ISO. In 2003, The National Security Agency purchased extensive licensing rights to Certicom's ECC technology and ECC is becoming a crucial technology for protecting national security information. Certicom's cryptographic providers provide complete RSA and ECC algorithm support.

# The Components of *Certicom Security Architecture for Mobility*

## Security Builder API

The foundation of the Certicom Security Architecture for Mobility is the Security Builder® API™. It provides the means by which applications access various cryptographic providers. The API enables the seamless addition of cryptographic support from a variety of Certicom-supported cryptographic providers to an application. A cryptographic provider could be a software toolkit, such as Security Builder Crypto, or a piece of hardware. Security Builder API abstracts away the differences among cryptographic providers without requiring significant code changes. This means that changing providers or chipsets requires only changes in linkage to the application, and not drastic changes to the application itself.

## 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.

Security Builder Middleware is currently available for the Intel® Wireless Trusted Platform . Through Certicom’s relationships with leading mobile processor vendors, additional versions of Security Builder® Middleware™ will be developed for other market leading mobile processors with hardware cryptographic providers. This will allow handset manufacturers to easily take advantage of optimized cryptographic building blocks within mobile processors, and to quickly and easily integrate new processors into their product line.

Security Builder Middleware for the Intel Wireless Trusted Platform allows developers to take advantage of the following security functions provided by the Intel Wireless Trusted Platform hardware cryptographic providers:

- **Hardware accelerated symmetric and asymmetric cryptographic algorithms: AES and RSA**
- **Hardware accelerated hash functions: SHA-1, HMAC SHA-1**
- **Key Exchange Protocol: Diffie-Hellman (DH)**
- **Hardware-based random number generation**
- **Hardware Key Management (secure key generation, manipulation and storage)**

For cryptographic functions not provided by the hardware cryptographic provider, or for devices with chips that do not have cryptographic providers, Certicom offers two software cryptographic providers: Security Builder Crypto and Security Builder GSE. Applications access these software cryptographic providers through the Security Builder API just like the hardware cryptographic providers.

## Software Cryptographic Providers

### Security Builder Crypto

Security Builder Crypto can augment the security offered by the hardware cryptographic provider by providing 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:

- **Broad range of symmetric and asymmetric cryptographic algorithms such as AES, 3DES, ECC and RSA**

- **Key agreement and transport: DH, ECDH, ECMQV, RSA**

- **Hashing algorithms such as HMAC SHA-1 and HMAC MD5**

- **Digital Signatures: ECDSA, DSA, RSA**

- **Random Number Generation**

### 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.

## Protocols

CSA also provides toolkits for the higher level protocols necessary to implement security in your devices:

### 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 capable of adding robust PKI security to applications. 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.

### Security Builder IPSec

Security Builder IPSec, a client-side virtual private network toolkit, enables developers to easily embed standards-based network access onto constrained devices. With the smallest code size and widest support for all industry-leading VPN gateways, Security Builder IPSec provides efficient security and enables better performance than is normally achievable with traditional IPSec implementations.

### Certicom Professional Services

In addition to providing the tools you need to add comprehensive security to your mobile platforms, Certicom also shares the benefits of nearly 15 years experience in designing security for mobile environments through Certicom Professional Services. In addition to offering general information security and cryptographic services, Certicom Professional Services provides a range of offerings specifically tailored to the requirements of mobile handset and processor manufacturers, including: platform porting, creating custom security applications or implementation of hardware security features. Certicom Professional Services help developers achieve the optimal balance among features, performance and investment.

## The Benefits of the *Certicom Security Architecture for Mobility*

Choosing the Certicom Security Architecture offers mobile handset and processor manufacturers a number of benefits:

### Comprehensive standards-based platform

Central to the interoperability and longevity of the Certicom Security Architecture is its standards-based design. *Certicom Security Architecture for Mobility* complies with a range of industry and government standards and can provide a FIPS 140-2 validated cryptographic module for use in government applications. Tools are included for adding complete security to applications ranging from cryptography to advanced protocols such as IPSec, SSL/TLS and PKI. Each of these toolkits works in concert and transparently through the common Security Builder API.

### Flexibility and portability

Already optimized for use with industry-leading chipsets, *Certicom Security Architecture for Mobility* delivers the portability developers need to move among more than 30 different platforms including Linux, Symbian, Microsoft Windows Mobile and Palm OS. Leveraging a single flexible architecture for all product offerings allows for the most efficient use of existing code, minimizing the time-to-market and development costs of switching chipsets.

### Fast time-to-market

By shielding the details of underlying security resources with a common API, *Certicom Security Architecture for Mobility* eliminates the integration of multiple toolkits, minimizes the need for expensive cryptography development expertise, and contributes to accelerated time-to-market for entire product families.

[2] These modules must be supported by Certicom.

### Optimized for size and performance

With all applications sharing a common security code base, *Certicom Security Architecture for Mobility* helps ensure the smallest possible security footprint. The modular design means developers need only compile the security modules each project requires.[2] This small size together with highly efficient ECC results in faster cryptographic performance which is further accelerated by optimization with market leading chipsets

### Security strategy partner

Certicom is a dedicated security organization with a core competency in embedding security in mobile devices. Customers like Motorola, RIM, and Texas Instruments are already benefiting from Certicom solutions and professional services expertise while licensees like the NSA are leveraging Certicom's extensive intellectual property portfolio. Partnering with Certicom allows mobile handset and processor vendors to avoid investing in security R&D while still achieving the future-proof security strategy the market demands.

## Real World Applications

Several real world applications where *Certicom Security Architecture for Mobility* is ideal are described below.

### Secure Firmware Upgrades

Using over-the-air (OTA) mechanisms to deliver feature upgrades and patches to a handset goes a long way to improving service and reducing costs for mobile operators and handset manufacturers. A complete end-to-end security model is recommended to defeat potential attackers who may attempt to intercept and tamper with the upgrade.

The *Certicom Security Architecture* provides complete support for both handset manufacturers and mobile operators, with features like digital signatures, certificates, hash functions and encryption algorithms.

On the operator side, a provisioning application like Certicom CodeSign can digitally sign and encrypt an update package as well as include a hash integrity code. In addition, the provisioning application can verify the integrity of the target device. A secure firmware agent developed for a handset allows the authentication of the source of the update, decryption of the payload and verification of the hash code.

In this way three key principles of information security are achieved – authenticity, privacy and integrity – building a formidable barrier to would-be attackers.

## Digital Rights Management (DRM)

The increasing value of digital media and content requires a secure DRM chain of trust to administer the use of licensed content. When a consumer orders digital content via a mobile handset, the content is delivered along with an attached rights object containing policy information describing the authorized use of that content. This policy is read and enforced by a DRM application on the handset. For the DRM business model to succeed, mobile operators and content providers require assurance that the handset is operating in a 'known-good' state and that communications between the mobile operator and handset are secured.

With a secure boot process to assure the platform integrity, developers can build a secure DRM application using the *Certicom Security Architecture for Mobility*.

Using symmetric keys like AES or public key algorithms like RSA or ECC, Certicom Security Architecture for Mobility can secure the rights object against tampering and secure content from illicit decryption. The protocol toolkits can also be used to secure communication channels to external parties, assuring the privacy and integrity of the information exchange.

Using the same components, developers can also supply their DRM application on the handset with the underlying cryptography services it requires to decrypt and check the integrity of incoming digital rights objects and their corresponding content.

Finally, Security Builder Middleware provides a link to hardware cryptographic providers to enable transparent acceleration of compute-intensive operations, which ensures the fast performance required to play large audio and video files.

## Secure Voice over IP (VoIP) over WiFi

VoIP telephony can offer substantial cost savings to the enterprise but the networking protocols it relies on also make it more susceptible to attack than traditional telephone service.

VoIP developers can choose to integrate SSL/TLS–based security or IPSec-based security to protect the vulnerable protocols in their solutions. Although encrypting the signaling protocols using SSL is the easiest solution, IPSec is also a very good approach. IPSec runs at the network layer and it will work over any network to encrypt both the signally and voice-channel protocols. Through the Certicom Security Architecture, developers can access both Security Builder SSL and Security Builder IPSec to achieve strong security. Both of these toolkits call the cryptographic providers through the Security Builder API..

Security Builder SSL can also be used with ECC to further improve the efficiency of the TLS key exchange. The performance of the IPSec key exchange can be improved with Security Builder IPSec and the use of ECDH.

## The Future

With over 15 years of experience, Certicom is a recognized leader in embedding security into constrained environments. Today, all of this expertise has been brought together to deliver the Certicom Security Architecture for Mobility: a comprehensive, cross-platform security solution for developers designed to address the challenges of embedding security in mobile handsets. The benefits that this architecture provides to handset and mobile processor vendors are myriad:

- **a single, common API**
- **hardware-optimized security which can be easily ported across multiple chipsets with no changes to code**
- **cost-effective software development and faster time to market**
- **delivery of applications with faster performance and stronger security**

Over time, the Architecture will continue to closely track industry requirements for mobile security and embrace other evolving standards such as Trusted Computing.

Mobile handset vendors will soon face a marketplace in which they either hold a competitive advantage through products differentiated by comprehensive security or they will lose to those competitors who do so first. The Certicom Security Architecture for Mobility allows these vendors to seize a low cost market opportunity to lock in continuously evolving security without hindering the time-to-market of their rapid release products. For their part, mobile processor vendors can attract these handset customers by working with a mobile security partner like Certicom to optimize and integrate their chipset architectures into a comprehensive security architecture such as described in this paper.

## 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 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*

# 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**