

wireless security solutions



- security applications 
- developer toolkits 
- professional services 

Security for Wireless Handhelds

integrating strong, transparent security without increasing costs or time-to-market



securing the wireless world

Incorporating security is no longer an option – it's mission critical.

Corporations and government organizations are demanding it. Businesses operating at warp-speed are providing their employees with a range of devices and applications to enable them to easily access and share information from anywhere in the world.

As more organizations embrace this multitude of new devices, IT departments must find cost-effective solutions that work within their established security policies and network infrastructure to enable secure, anytime, anywhere connectivity without compromising the user experience.

Proven, standards-based cryptographic functions and protocols, however, are processor intensive.

Certicom understands that anything that affects performance and usability is a serious problem for your customers. We also realize that meeting the security needs of end-users must not negatively impact your time-to-market or development cost.

Certicom's award-winning products and ECC public key technology offer the **most secure, highest performance, and smallest footprint on the market.**

Our integrated Developer Toolkit suite runs on the most popular embedded platforms, and is constantly optimized for size and performance, while still offering the strongest security available. If saving time is what you are after, our Security Applications offer wireless security that's easy to deploy and fits with your customer's existing infrastructure.

The Technology Behind the Security

Today's security hurdle is bringing the same level of security enjoyed by traditional networks to smaller devices and the wireless world. For encryption, this means the algorithm must be as strong as possible without creating a key length that devours the resources and battery life of mobile devices. These unique demands can be addressed with the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), a standards-based, public key technology.

AES comes in three strengths: 128 bits, 192 bits and 256 bits. Not only does AES provide more security than 3DES, it also has better performance, making AES highly attractive for use in wireless handhelds.

To successfully protect your data, a high security algorithm like AES demands equivalent security for the accompanying digital signatures and key exchanges. Otherwise, AES can be

compromised through the weaker security of your public key cryptography. Normally, this would mean the large key sizes required to match AES levels of security would overwhelm the processors of most mobile devices.

Fortunately, ECC maintains relatively compact key sizes at all security levels. This makes it ideal for use in constrained, mobile device environments such as PDAs. AES used in conjunction with ECC allows for high security solutions to wireless networking despite the limitations of the operating environment.

Certicom has established its leadership in embedded security solutions through ultra-secure, high performance cryptography and was the first to bring ECC to market with the introduction in 1997 of the Security Builder[®] toolkit.

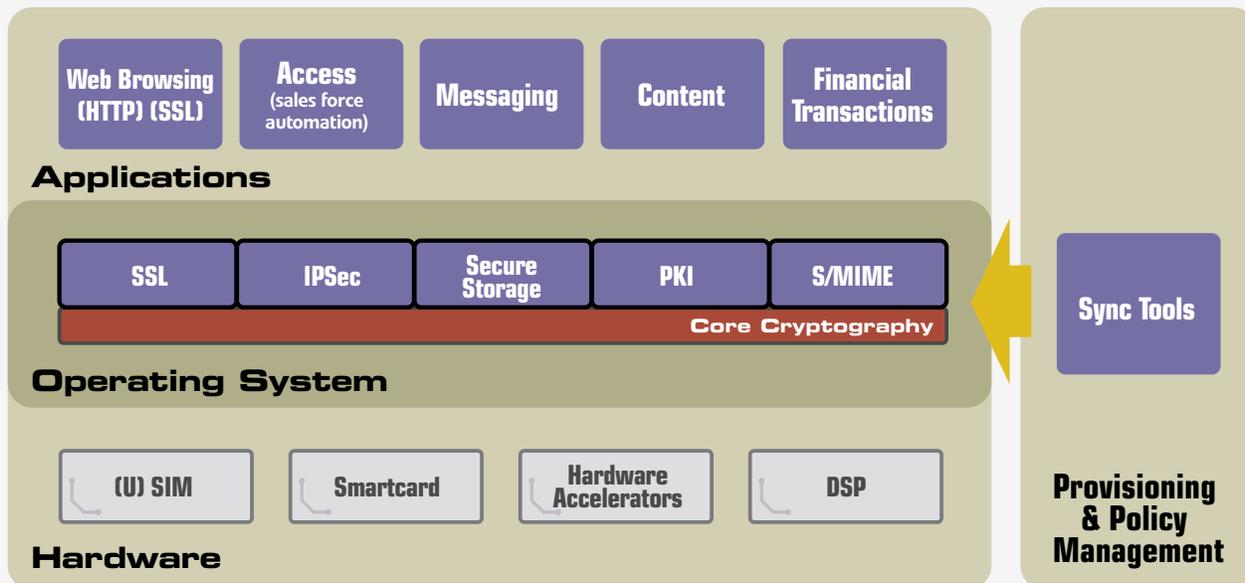
Securing Today's Devices

Many emerging devices today require security – including handhelds, smartphones, PDAs and other wireless devices that offer multimedia voice and data. Depending on your requirements, security can be added at many different levels.

Integrated at the hardware level, Certicom Developer Toolkits offer your customers simple, proven APIs that can be used to enable hardware-level security functionality. Cryptography directly implemented in silicon offers the highest level of integrity and performance.

You can also integrate security functionality into the OS with APIs exposed to other applications. Certicom Developer Toolkits are ideally suited to be the cryptographic service provider for all leading handheld OSs as well as the proprietary ones used to power other devices.

For device manufacturers looking to quickly value-add their offering, bundling Certicom Security Applications with a device is an easy way to satisfy organizations requirements for secure network access, secure messaging and secure data storage for handhelds.

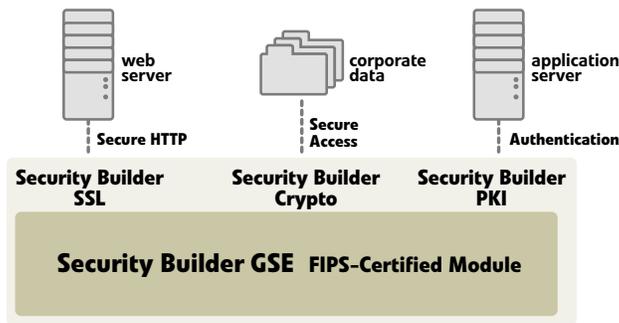


Certicom solutions and ECC technology can be quickly integrated into any wireless handheld architecture to offer strong security with minimal impact on footprint and performance.

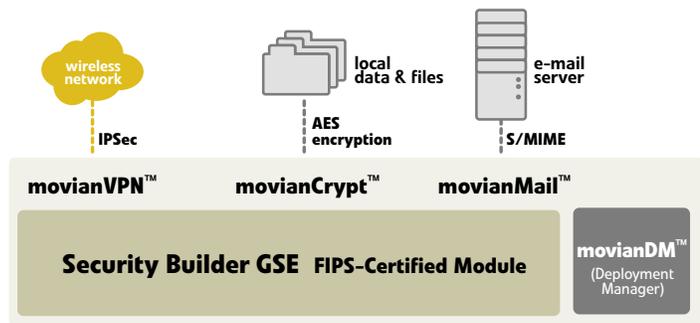
Developer Toolkits and Security Applications ■ ■ ■

As the demand continues for more capabilities in applications and increasingly smaller Internet-enabled devices, you need to ensure that your product will work securely and still be easy to use. You also need to get your product to market as soon as possible while remaining cost-competitive. Certicom Developer Toolkits and Security Applications let you embed proven, efficient security technology into your devices and applications without prohibitive delays or expense.

With support for a wide range of platforms, standards and protocols, you can be sure that the Certicom technology embedded in your latest device or processor is not only strong and fast, but also extensible and interoperable.



Developer Toolkits



Security Applications

Developer Toolkits ■ ■ ■

The Developer Toolkits reduce your time-to-market with a common API that is intuitive to integrate and supports multiple platforms.

Security Builder® Crypto™
cross-platform cryptographic toolkit

Security Builder® SSL™
complete Secure Socket Layer protocol security toolkit

Security Builder® PKI™
digital certificate management toolkit

Security Builder® GSE™
FIPS 140-2 Validated cryptographic module

Security Applications ■ ■ ■

The Security Applications can be easily integrated into any device to ensure the secure storage and transmission of data using a smartphone or other handheld.

movianVPN™
secure access to the corporate network via mobile devices

movianCrypt™
secure data storage for mobile devices

movianMail™
secure e-mail application for mobile devices

Professional Services ■ ■ ■

Certicom Professional Services provides a wide spectrum of information security and cryptographic services. Whether you need an end-to-end enterprise-wide security solution, assistance with a project or application-specific solution, help in engineering a particular security solution, or individual consulting services, we provide the experience and expertise to address your security requirements.



embedded expertise



innovative cryptography



customer focus

The Certicom Advantage

Certicom has over 15 years experience developing security for constrained devices, enabling you to use our strengths to your advantage:

leading innovator of ECC technology

ECC (Elliptic Curve Cryptography) has been endorsed by standards and organizations such as ANSI, IETF, IEEE, FIPS and NIST and is quickly becoming the choice of organizations (such as the US Government) that want highly secure technology which scales with the Advanced Encryption Standard (AES) without compromising on performance. Certicom holds over 120 patents (filed and pending) based on our research into ECC and was the first vendor to ship products developed using this technology.

optimized security for size and performance

Certicom's patented technologies deliver the strongest cryptography with minimal impact on performance and usability. The Developer Toolkits are highly modular so that unused algorithms can be compiled out to save on footprint and the code is completely thread-safe. With support for over 30 platforms, as well as legacy cryptosystems such as RSA, Certicom is uniquely positioned to offer the most efficient security to the widest variety of applications.

delivery and support of complete solutions

Given the importance of security today, it's important to ensure that your product gets it right the first time. Certicom Professional Services can work with you to help clarify and solve a wide range of tough security challenges throughout the full project lifecycle—from requirements gathering through to design, development and testing. They have many years of experience and the depth of expertise to assist with the implementation of a comprehensive security solution.

North America
1.800.561.6100

Europe
+1.905.507.4220

Corporate Headquarters
5520 Explorer Drive, 4th Floor
Mississauga, ON, L4W 5L1
Canada
Tel: 905-507-4220
Fax: 905-507-4230
info@certicom.com

Regional Offices

Western US

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

Eastern US

1175 Herndon Parkway, Suite 750
Herndon, VA 20170
Tel: 571-203-0700
Fax: 571-203-9653
sales@certicom.com

Canada

84 Hines Road
Ottawa, ON, K2K 3G3
Canada
Tel: 613-254-9270
Fax: 613-254-9275
sales@certicom.com

Europe

Golden Cross House
8 Duncannon Street
London WC2N 4JF
United Kingdom
Tel: +44 20 7484 5025
Fax: +44 20 7484 5150
europa@certicom.com

Certicom is a leading provider of wireless security solutions, enabling developers, governments 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.

Certicom products are currently licensed to more than 300 customers including Texas Instruments, Palm, Research In Motion, Cisco Systems, Oracle and Motorola.

For more info and to access these and other resources, please visit:
www.certicom.com/solutions/oem

