certicom
securing innovation

protect your content, applications and devices

with government-approved security

Certicom Corp.

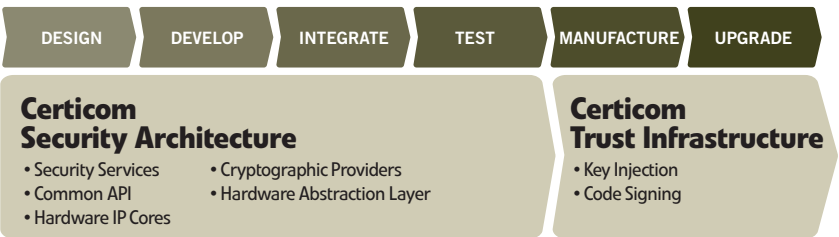
Security is about one thing—trust. At Certicom, we are committed to establishing trust for our customers through open, standards-based, security technology that withstands the test of time. Since 1985 we have been developing public-key technologies and today we are regarded as the undisputed leader in elliptic curve cryptography (ECC). Our security solutions — used to protect content, applications and devices — are unrivalled in strength, transparency and flexibility.

Certicom's expertise is grounded with a pedigree that is second to none. Our founder Dr. Scott Vanstone is a world-renowned researcher, author and professor of mathematics at the University of Waterloo. Dr. Vanstone's commitment to exploiting ECC to develop stronger, more efficient security solutions extends to the entire Certicom team.

Elliptic Curve Cryptography (ECC)

Certicom solutions are based on ECC because it provides the most security per bit of any known public-key scheme and has been selected by the National Security Agency (NSA) for Suite B cryptographic specifications to protect classified and unclassified government communications.

ECC is a fundamental part of Certicom, our research, the technology we develop and our vision that one day ECC will protect content, applications and devices everywhere.



Understanding that vulnerabilities also occur below the application layer in the OS, firmware and silicon, the Certicom Security Architecture and Certicom Trust Infrastructure was developed to protect a device throughout its entire lifecycle — from design and development through to manufacturing and upgrades.

The Importance of ECC and Suite B

CRYPTOGRAPHIC STRENGTH	SYMMETRIC ALGORITHM	HASH ALGORITHM	ELLIPTIC CURVE ASYMMETRIC ALGORITHM	RSA/DSA/DH ASYMMETRIC ALGORITHM
56 bits	DES	–	–	–
80 bits	3DES (2 key)	SHA-1	160 bits	1024 bits
112 bits	3DES (3 key)	SHA-224	224 bits	2048 bits
128 bits	AES-128*	SHA-256	256 bits	3072 bits
192 bits	AES-192	SHA-384	384 bits	7680 bits
256 bits	AES-256*	SHA-512	512 bits	15360 bits

NIST Recommended Key Sizes

Backed by almost 20 years of research, ECC has been included in key industry standards from groups including ANSI, FIPS, IEEE, IETF, ICAO and SECG.

Recently, the NSA--through its Suite B cryptographic specifications, has recommended that ECC technologies be used to protect classified as well as sensitive but unclassified government communications. Although these recommendations are for government agencies and their suppliers, other industries tend to adopt these standards as well.

In Suite B, the NSA chose the Advanced Encryption Standard (AES) for encryption with ECC-based algorithms for key agreement and digital signatures. The NSA selected ECC because it offers the most strength per bit and scales linearly with the AES. ECC offers equivalent security to other competing technologies at much smaller key sizes to enable faster computations, lower power consumption, as well as memory and bandwidth savings.

Certicom Intellectual Property

Certicom has built an extensive portfolio of more than 350 patents and patents pending covering key techniques critical to the design of cryptographic systems both in software and hardware. In particular, Certicom has an extensive patent portfolio related to ECC public-key technology.

Certicom Intellectual Property can be licensed directly or through Certicom products, depending on the way the technology is implemented.

End to End Security Solutions

Certicom is the only solution provider today to look at the entire product life-spectrum in an integrated fashion, providing the practical resources needed to ensure end-to-end security. We've developed solutions to meet the particular security requirements of new technology arenas using the Certicom Security Architecture and the Certicom Trust Infrastructure:

Certicom Security for Government
Certicom Security for Mobility
Certicom Security for Sensor Networks
Certicom Security for DRM and CA
Certicom Security for Enterprise
Certicom Security for Check21
Certicom Security for VoIP
Certicom Security for Silicon Design Protection
Certicom Security for Gaming
Certicom Security for RFID Product Authentication

Certicom Products

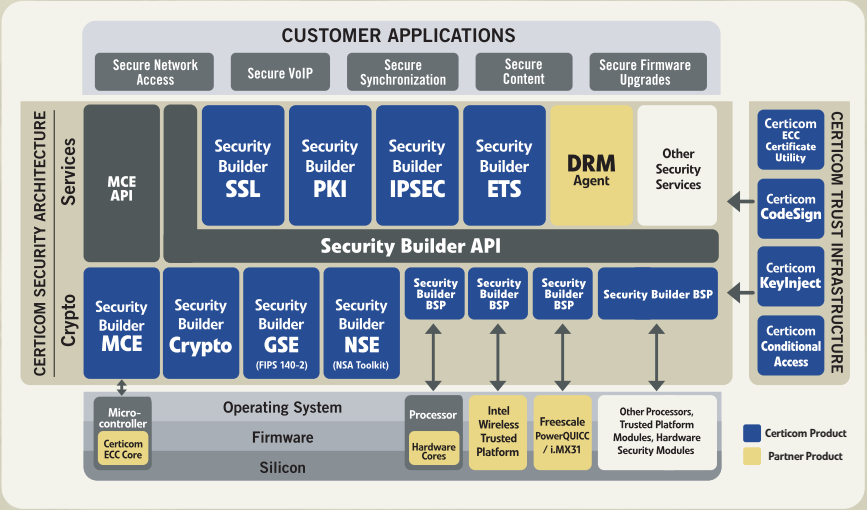
The Certicom Security Architecture is a comprehensive, portable and modular security platform that includes: software cryptographic providers that offer FIPS 140-2 Validation and meet NSA guidelines for ECC; security services like SSL, IPSec, PKI, DRM and Embedded Trust Services (ETS); hardware IP cores; and board support packages (BSP) that expose cryptographic functionality available in hardware.

Components of the Architecture are unified by a common application programming interface (API) that sits between the security services or applications and the cryptographic providers. The API accesses the fastest and/or strongest security available, whether it resides on the chipset or in the software cryptographic provider.

The result is cost-effective software development and faster time-to-market:

- **portability and code re-use in products with different chipsets as a result of standardizing on a cryptographic API**
- **easy migration from legacy crypto systems such as RSA, to today's standard for public-key cryptography, ECC**
- **adherence to industry standards and stringent government security requirements, enabling access to new markets**

The Certicom Trust Infrastructure allows application and device vendors to securely manufacture and upgrade their products with a cost-effective, off-the-shelf platform that offers flexibility, reliability and strong security. A complementary extension to the Certicom Security Architecture, Certicom Trust Infrastructure includes Certicom CodeSign for digitally signing firmware and code updates, Certicom KeyInject, a trusted key injection platform and the ECC Certificate Utility for easy generation and installation of ECC Certificates.



Certicom Security Architecture Modules

CRYPTOGRAPHIC PROVIDERS

Security Builder® Crypto™
cross-platform cryptographic module

- easy integration of encryption, public-key cryptography and other security mechanisms into C, C# and Java applications
- only embedded toolkit to supply efficient ECC technology and legacy systems such as RSA
- license Security Builder Crypto to implement patented ECC technologies on more than 30 standard platforms

Security Builder® BSP™
board support package for optimized hardware security

- provides optimized hardware abstraction layer
- links the Security Builder API, and thereby all applications, to specific crypto functionality found in hardware
- supports leading mobile/embedded chipsets, smartcards and other trusted platform modules, including the Intel Wireless Trusted Platform, Freescale PowerQUICC and i.MX31 chipsets

Security Builder® NSE™
cryptographic module for national security information

- quickly build applications and devices that meet NSA field-of-use guidelines
- includes ECDH, ECMQV and ECDSA for NSA Type 1 certification for Suite B
- support for Windows and Linux platforms

Security Builder® MCE™
software cryptographic module for microcontroller devices

- enables unique identification of and secure data exchange between microcontroller devices
- supports scalable, ad-hoc mesh networking for automatic enrolment of a large number of devices
- includes ECC, the only viable public-key scheme for constrained sensor environments

Security Builder® GSE™
FIPS 140-2 Validated/NSA Suite B-enabled cryptographic module

- build applications in C and Java for client and server side products that meet FIPS 140-2 and NSA Suite B requirements
- support for standard client and server platforms including UNIX-based, Palm, Symbian, Windows and Windows Mobile operating systems
- enables TLS and IPSec to run in FIPS-approved mode of operation

Certicom ECC Core™
hardware core for acceleration of ECC on microcontroller devices

- low-risk, high performance hardware IP blocks for SOC, ASIC and FPGA-based solutions
- offloads and accelerates the computationally-intensive calculations , allowing constrained systems to benefit from public-key cryptography
- provides open interfaces and a variety of flexible implementation options

Certicom Professional Services

With an eye on helping organizations obtain an optimal balance between features and investment, Certicom Professional Services offers expertise on a wide spectrum of information security and cryptographic services. This team of accomplished engineers and scientists, including top-secret cleared members, use their security and technology expertise for project design consulting, porting and development assistance as well as the very difficult applications that can border on being obscure.

Security Builder® SSL™
complete Secure Sockets Layer protocol module

- supports over 20+ SSL and TLS cipher suites for C and Java applications including RFC 4492 (ECC)
- supports SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 , WAP 2.0, EAP-TLS, EAP-TTLS, and EAP-PEAP
- enables high performance environments with compression and hardware support

Security Builder® IPSec™
high performance IPSec for resource-constrained devices

- embed standards based IPSec network access into devices and applications
- compatible with all leading gateways and operating systems
- supports IKEv1/v2, MOBIKE, AES, 3DES, SHA-1, MD5, ECDH, RSA, DH, EAP

Security Builder® PKI™
comprehensive digital certificate management module

- add robust PKI security to applications written in C or Java
- supports CMS to develop S/MIME and EDI over Internet applications
- interoperable with third-party PKI/CAs

Security Builder® ETS™
embedded trust services module

- provides secure key storage, key management and authentication services for trusted platforms
- interfaces with hardware-based trusted platform modules through Security Builder BSP

Certicom Security for Multi-DRM
integrated DRM agent support for OMAv2 and WMDRM

- allows OEMs to meet the enhanced security requirements of content owners and service providers
- support for video, music and gaming content allows rapid creation of new services
- compliant with CMLA and OMTP specifications and requirements
- allows integration on proprietary RTOS, Linux and Symbian platforms with minimal recoding

Certicom Partner Connection

The Certicom Partner Connection brings together leading embedded software and hardware vendors to offer developers complete solutions that leverage the Certicom Security Architecture. Certicom collaborates with its partners up front so the heavy lifting of solution design and integration is done, allowing companies to get to market quickly and cost-effectively with solutions that have strong and efficient security.

Certicom Trust Infrastructure Modules

Certicom ECC Certificate Utility™
enabling crypto-modernization transition with existing infrastructure

- generate ECC certificates and test applications
- supports hybrid certificates that combine ECC with RSA signatures
- convert identities, files, and certificate chains between PEM, PFX, Base-64, and binary formats

Certicom KeyInject™
trusted key injection for anti-cloning

- protects fabless semiconductor manufacturers against chip overproduction
- controls, tracks and reports key usage during secure device manufacture
- manufacturing support for HDCP, CPRM, OMA DRM 2.0 and other third-party content protection schemes

Certicom CodeSign™
browser-based code signing application

- create tamper-resistant firmware updates
- supports ECC-based and legacy public-key signing standards

Certicom Suite B Power Bundles

Certicom Suite B Power Bundles combine a wide range of high-performance hardware and software products into a comprehensive solution that can make your entire infrastructure completely Suite B compliant. As the primary source of Suite B technology, Certicom delivers everything you need to meet Suite B requirements quickly and easily. With Certicom Suite B Power Bundles that are scalable and optimized for constrained environments, products get certified more quickly and time-to-market is sped up.

Certicom Suite B Power Bundles are ideal for government agencies taking part in crypto-modernization efforts and perfect for commercial enterprises that must meet government mandates for protecting customer information.

Certicom Suite B Power bundles include:

- **Suite B Web Security Power Bundle**
- **Suite B Hardware Security Power Bundle**
- **Suite B Professional Services Power Bundle**
- **Suite B ECC Extensions Power Bundle**

certicom
securing innovation

Certicom protects the value of your content, applications and devices with security offerings based on Elliptic Curve Cryptography (ECC). Adopted by the National Security Agency (NSA) for both classified and sensitive but unclassified government communications, ECC provides the most security per bit of any known public-key scheme.

Corporate Headquarters
5520 Explorer Drive
Mississauga, ON, L4W 5L1
Tel: +1-905-507-4220
Fax: +1-905-507-4230
info@certicom.com

US Sales
Worldwide Sales Headquarters
1800 Alexander Bell Drive, Suite 400
Reston, VA 20191
Tel: +1-703-234-2357
Fax: +1-703-234-2356
sales@certicom.com

Western Region
393 Vintage Park Drive
Foster City, CA 94404
Tel: +1-650-655-3950
Fax: +1-650-292-4615
sales@certicom.com

Canadian Sales
349 Terry Fox Drive
Kanata, ON K2K 2V6
Tel: 613-254-9270
Fax: 613-254-9275
sales@certicom.com

EMEA Sales
United Kingdom
Golden Cross House
8 Duncannon Street
London WC2N 4JF UK
Tel: +44 1344 624970
Fax: +44 1344 624960
sales@certicom.com

Sweden
Engelska Huset
Trappv 9
13242 Saltsjo-Boo SWEDEN
Tel: +46 8 747 17 41
Fax: +46 708 74 41 61
sales@certicom.com

Israel
Atidim, POB 58019
Tel-Aviv 61580
Israel
Tel: +972-3-648-4121
Fax: +972-3-647-8365
sales@certicom.com

APAC Sales
Japan
6-4-11-401 Minami Shinagawa
Shinagawa-ku
Tokyo, Japan 140-0004
sales@certicom.com

Korea
DongMyoung Bldg.
#202, 2nd Floor 165-7
SeokChong-Dong
Songpa-Gu
Seoul, Korea 138-844
Tel: 82-2-417-1786
Fax : 82-2-417-1781
sales@certicom.com

www.certicom.com