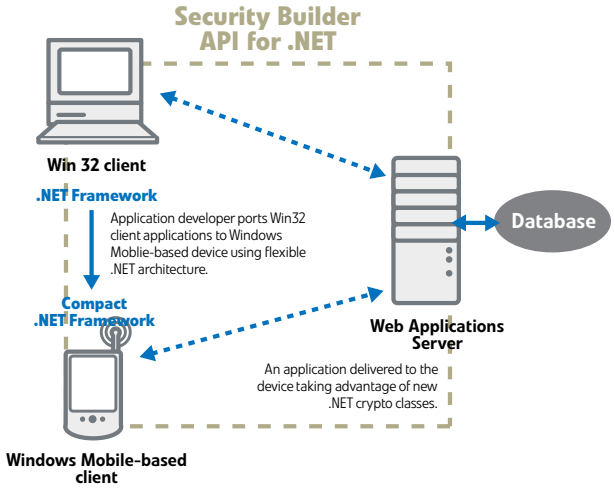
certicom™
securing innovation

Security Builder® API for .NET™

Enable Suite B support for .NET applications and reduce development time

Certicom Security Builder API for .NET enhances the security and flexibility of your applications by enabling you to quickly and easily achieve complete Suite-B level security.

Whether you're running applications on a desktop or a mobile device, Certicom Security Builder API for .NET enables you to port existing security into and between the .NET Framework and the .NET Compact Framework quickly and easily – saving you time and money while delivering superior security.



How Security Builder API for .NET helps you seamlessly port Suite B-level security between .NET architectures.

Increase ROI

Leverage your legacy systems, reduce development time required, and re-use existing code because components built using Security Builder API for .NET can be used by any of the 20+ approved .NET languages - including C# and Visual Basic. Security Builder API for .NET is also interoperable with Microsoft CAPI, the new Microsoft CNG architecture, and supports all .NET platforms

Reduce Time-to-Market

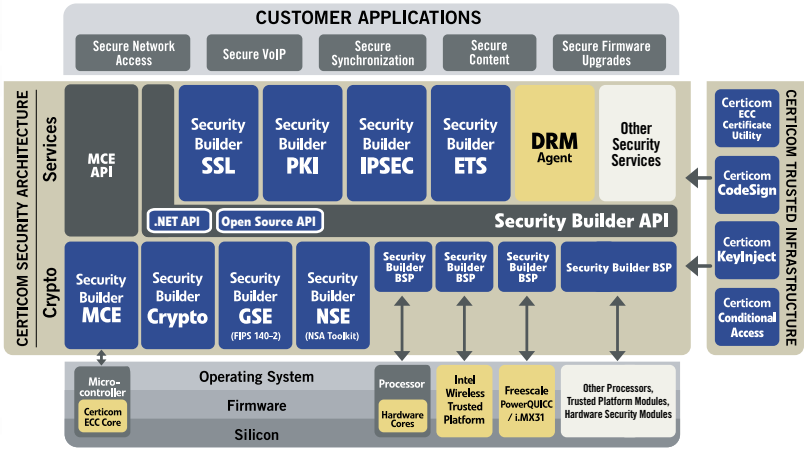
Designed to the same standard as those supported by Microsoft, Security Builder API for .NET crypto classes integrate into the .NET Framework architecture with ease, cutting development time. The .NET API enables ECC-based security to be ported seamlessly between existing desktops to both the .NET and .NET Compact Frameworks. To speed up development even more and show how the APIs are used, Certicom also supplies C# and Visual Basic samples.

Achieve Suite B-level Security

Certicom is the only provider to enable legacy .NET applications and newer environments to attain complete Suite B-level security with highly optimized implementations. The .NET API also supports RFC 4492 and the new Suite B TLS and IPSec standards co-authored by the NSA.

Part of a Comprehensive Security Solution

Security Builder API for .NET acts as an abstraction layer to the cryptographic providers within the Certicom Security Architecture (CSA) – a comprehensive, portable, and modular security platform that includes software cryptographic providers that offer FIPS 140-2 Validation and meet NSA Suite B requirements; 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.



Features

Security Builder API for .NET facilitates seamless access to a richer set of cryptographic classes, enabling you to achieve Suite B-level security and FIPS 140-2 validation. When used with a pre-approved cryptographic module that supports popular protocols including TLS and VPN in FIPS mode, Security Builder API for .NET can save you 8-12 months of development time.

	Security Builder API for .NET	Security Builder API for .NET with FIPS
Cryptographic Providers	Security Builder Crypto-C 5.x	Security Builder GSE-C 2.x*
Symmetric Encryption	AES	AES
Asymmetric Encryption	N/A	N/A
Key Agreement/Key Transport	ECDH, ECMQV	ECDH, ECMQV
Digital Signatures	ECDSA	ECDSA
Hash Functions	SHA-1, SHA-256, SHA-384, SHA-512, MD5	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Random Number Generation	ANSI X9.62, FIPS 140-2 extension	ANSI X9.62, FIPS 140-2 extension
Implementation Code Size Range	200-275 KB	approx 1.1 MB
Code Sample Languages	C#, Visual Basic	C#, Visual Basic
Platform Support	**.NET 1.0/1.1** • Win32 .NET • Win64 .NET • Windows Mobile 2003 • Windows Mobile 2003 Emulator • Windows CE 4.x/ 5.x **.NET 2.0** • Win32 .NET • Win64 .NET • Windows Mobile 2003 • Windows Mobile 2003 Emulator • Windows CE 5.x	**.NET 1.0/1.1** • Win32 .NET • Windows Mobile 2003 • Windows Mobile 2003 Emulator • Windows CE 4.x/ 5.x **.NET 2.0** • Win32 .NET • Windows Mobile 2003 • Windows Mobile 2003 Emulator • Windows CE 5.x

* FIPS Certificate #542

"With Security Builder API for .NET, Certicom is providing a valuable tool for developers to add advanced security to applications built on .NET."

Thom Robbins,
Director .NET Platform Product Management at Microsoft

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.

about certicom

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 classified and sensitive but unclassified government communications, ECC provides the most security per bit of any known public-key scheme. Visit www.certicom.com.

North America 1.800.561.6100
EMEA +44.20.7484.5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com