Achieving High Level .NET Application Security in Hours

How Certicom Helps You Dramatically Reduce Development Time, Increase Efficiency, and Achieve FIPS Validation for .NET Applications and Products

A Certicom Technology Brief
October 2007

certicom™

Executive Summary

In the government market, applications and products associated with the communication of sensitive data must meet FIPS requirements. It can take 8-12 months and significant budget. The .NET community can now meet this requirement in hours and show ROI.

According to NIST, 48% of cryptography functions have flaws and 30% of algorithms don't conform to standards. Rather than slip competitive development schedules and strain tight project budgets, developers can dramatically reduce development time, increase efficiency, lower costs, and achieve FIPS validation in hours by relying on third party support to supply crypto classes. In addition, developers gain access to an expanded number of crypto classes - Elliptic Curve Cryptography (ECC) - that enables additional high security functions, significantly increase application security, boosts efficiency, and provides a lasting competitive advantage.

Beyond government requirements, mobile devices are expected to work with a host of applications, networks, and other devices. By nature, remote devices are subject to interoperability and security concerns that are resolved by universal standards and effective porting of inherent security applications.

Microsoft's .NET Framework for Desktops and .NET Compact Framework for mobile devices makes it easy for developers to address interoperability issues, but doesn't automatically port cryptographic functions. Certicom Security Builder API for .NET solves these issues by enhancing the security and flexibility of applications. By enabling complete FIPS 140-2 and Suite B-level security in mobile devices, developers can port existing security into and between .NET Frameworks to deliver superior security.

This comprehensive solution also functions inside the .NET environment as managed code, to offer the dual advantage of leveraging existing operating system interactions while still allowing calls to the native, unmanaged code maintained within the wrappers. This means code can be reused in any .NET Framework application, drastically speeding up development and increasing ROI.

For over 20 years, industry leaders such as General Dynamics, Texas Instruments, RIM, and the NSA rely on Certicom technology because they recognize the value of intuitive programming, high-performance, guaranteed code, professional documentation, solution roadmaps, immediate FIPS Validation, Suite B-level security, and an enduring commitment to keeping up with evolving standards.

certicom™

Why FIPS 140-2 and Suite B?

Federal Information Processing Standards (FIPS) is a stringent security requirement that must be met by any company wishing to sell products to a government agency. The FIPS directive specifically relates to products that include encryption as a security feature.

As you know, some government standards and mandates have not yet reached the stage where they have become mandatory requirements. This is not the case with FIPS. In order to win deals in the government market, vendor products must meet FIPS requirements. FIPS is the de facto standard for government security and it has become a requirement for any product or application associated with the communication of sensitive data.

For example, routers, handheld devices, and applications being built for the Defense Department need to achieve FIPS validation before an agency can purchase these products.

Suite-B level security is the next step for government agencies and industry. This standard was first announced in 2005, after the NSA licensed the core technology from Certicom. Since then, leading government agencies and global companies have started to adopt this stronger security standard. Beyond the benefits of stronger security, Suite B also enables significant operational benefits relating to bandwidth and memory requirements for constrained devices.

The following directives refer specifically to FIPS 140-2 requirements for security related products purchased by the government:

- **Department of Commerce Directive 16-02 (December, 1992)**
- **National Information Assurance Acquisition Policy (NSTISSP) no. 11 (June 2002)**
- **Department of Defense Directive 8500 (October 2002)**
- **Department of Defense Directive 8500.1/8500.2 (October 2002/ February 2003)**
- **NIST Special Publication 800-23**
- **Department of Defense Directive 8100 (April 2004)**

A number of European and financial standards also refer to FIPS 140-2.

Suite B Components Include

ENCRYPTION	**Advanced Encryption Standard (AES) – FIPS 197** (with key sizes of 128 and 256 bits)
DIGITAL SIGNATURE	**Elliptic Curve Digital Signature Algorithm – FIPS 186-2** (using curves with 256 and 384-bit prime module)
KEY EXCHANGE	**Elliptic Curve Diffie-Hellman or Elliptic Curve MQV Draft NIST Special Publication 800-56** (using curves with 256 and 384-bit prime module)
HASHING	**Secure Hash Algorithm – FIPS 180-2** (using SHA-256 and SHA-384)

NIST Cryptographic Standards

CRYPTOGRAPHIC STRENGTH	SYMMETRIC ALGORITHM	HASH ALGORITHM	ELLIPTIC CURVE ASYMMETRIC ALGORITHMS	RSA/DSA/DH ASYMMETRIC ALGORITHMS	KEY SIZE RATIO	EXPECTED LIFETIME EXPIRY
56 bits	DES	–	–	–	–	Expired
80 bits	3DES (2 key)	SHA-1	160 bits	1024 bits	–	2010
112 bits	3DES (3 key)	SHA-224	224 bits	2048 bits	–	2030
128 bits **	AES-128	SHA-256	256 bits	3072 bits	1:12	2031+
192 bits		SHA-384	384 bits	7680 bits	1:20	2031+
256 bits **	AES-256	SHA-512	512 bits	15360 bits	1:30	2031+

SHADED = Suite B Requirements

** NIST recommended key sizes.128-bit is commercial strength and 256-bit is for classified information

certicom™

Easily Port Cryptography Functions Throughout your Network Infrastructure

Producing applications for rapidly evolving environments is challenging enough without additional interoperability or security hurdles. This is especially true in constrained devices such as smart phones or PDA's. By definition, a mobile device must interoperate with a host of other applications, devices and networks. However, due to its exposed nature, mobile devices demand the same level of security as desktop environments, if not more. Where typical desktop environments benefit from established security policies and a fixed location behind locked doors and security personnel, wireless networking creates additional security challenges, including the potential for loss or theft.

To address interoperability issues, many developers have turned to the universal runtime and common standards of the Microsoft .NET Framework in desktop implementations and .NET Compact Framework in mobile ones. The multiple-language capability of the .NET Framework enables developers to use the programming language most appropriate for a given task, and to combine languages within a single application. With this flexibility, developers can quickly convert to the .NET Framework and then to .NET Compact Framework if necessary.

Although the .NET framework makes it easy for developers to transfer code to the .NET Compact framework, a variety of issues arise when porting cryptographic functions. Only a subset of cryptographic classes are available for use with the .NET Framework.

.NET 2.0 and 3.0 incorporate substantial cryptography, but they don't contain FIPS 140-2 or Suite B-Level security.In addition, developers can't leverage existing code. This increases development time and keeps programmers from focusing on the core functionality of the applications.

Making it Easy to Achieve Complete FIPS 140-2 & Suite B-Level security

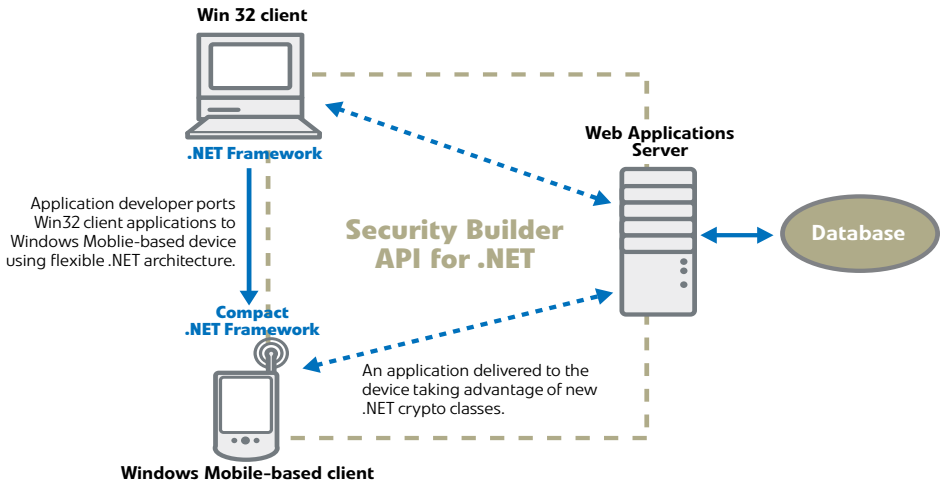
Rather than slip competitive development schedules and strain tight project budgets, software vendors can rely on third-party support to supply crypto classes for .NET Framework implementations. Likewise, prepackaged code wrappers enable developers to reuse .NET Framework crypto classes in .NET Compact Framework architectures. This expanded number of .NET Framework crypto classes enables additional high-security functions, such as ECC algorithms, which significantly increase application security, boosts efficiency, and provides a lasting competitive advantage.

ECC, a highly efficient public key technology that was chosen by the NSA to be the basis for Suite B, offers significantly more security-per-bit than any other public key cryptography system. With ECC, you gain access to the strongest public key technology while using much smaller key sizes. Maintaining high performance while minimizing the consumption of bandwidth and processing power is valuable for all networks – but it is imperative in constrained and wireless environments. Certicom's Security Builder API for .NET is a cost effective way to support ECC, including Suite B algorithms, as well as achieve FIPS 140-2 compliance.

"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

How Security Builder API for .NET Automatically Transfers Security Functions
The diagram shows how Security Builder API for .NET can help port an existing desktop Windows 32 client to a new desktop .NET Framework-based client, or a Windows Mobile™ client. Likewise, an application for a mobile device can take advantage of new .NET cryptography classes delivered from a central server.



Once operational, the Windows Mobile™ device relies on Certicom's managed code wrappers and unique ECDSA cryptography class for efficient and trusted communication with the Web Applications Server.

Quickly Port Cryptographic Functionality Across Your .NET Applications

With the introduction of Security Builder API for .NET, Certicom's cross-platform cryptographic toolkit has been extended to include new .NET Framework crypto classes designed to the same standard as those supported by Microsoft. Only available from Certicom, these new crypto classes allow developers to add ECC to desktop .NET Framework-based applications through a standard Microsoft application program interface (API).

Your system can be Suite-B level secure and FIPS validated in a matter of hours.

A comprehensive solution, Security Builder API for .NET also functions inside the .NET Common Language Runtime environment as managed code. This offers the dual advantage of leveraging existing operating system interactions available to all managed code, while still allowing calls to the native, unmanaged code contained within the wrappers. This enables programmers to build on existing code bases in a variety of languages such as C, C++, Visual Basic and many others rather than discard them. Once built, wrapped code can be used and reused in any appropriate .NET Framework application, drastically speeding up development and increasing ROI.

certicom™

Sample Code: Certicom API for .NET code wrapper (ECDH algorithm)

Security Builder API for .NET includes .NET Compact Framework code wrappers for most cryptographic algorithms. Designed to meet the same standard as those supported by Microsoft, Certicom crypto classes easily integrate with the .NET architecture. To further speed up development, Certicom provides C# and Visual Basic .NET samples.

```
SampleUtil.SetCryptographicProvider();
byte[] sharedSecretAlice;
byte[] sharedSecretBob;
ECDH ecdhAlice = new ECDHCryptoServiceProvider();
ECDH ecdhBob   = new ECDHCryptoServiceProvider();
    string AliceXML = "<ECCKeyValue><Curve>secp256r1</Curve><PubKey>ArthGn38eP4fYC+vOg+w
ZXUDRv18Zm93qEbaw8t6r6GY</PubKey><PrvKey>TnVG8VQH3bIQvMtDPjBJ0abbiSTyIlqw7rgHKDTem7I=</
PrvKey></ECCKeyValue>";
string BobXML =  "<ECCKeyValue><Curve>secp256r1</Curve><PubKey>AxnbzYHMiu2D1I8542mRICtnjG
qASGyviwfkwr347+9A</PubKey><PrvKey>3DSOFpkxFIJU74rMotf7cDfTBqxQVfLtCOJCnUTiW5k=</PrvKey></
ECCKeyValue>";
ecdhAlice.FromXmlString(AliceXML);
ecdhBob.FromXmlString(BobXML);
sharedSecretAlice = ecdhAlice.SharedSecret( ecdhBob.PublicKey );
sharedSecretBob   = ecdhBob.SharedSecret( ecdhAlice.PublicKey );
```

Choose From Two Versions of Security Builder API for .NET

Security Builder API for .NET enables seamless access to a rich set of cryptographic classes that enable you to achieve Suite B-level security as well as FIPS 140-2 validation with a pre-approved cryptographic module that supports popular protocols – including TLS and VPN in FIPS mode and can save you 8-12 months of development time. You can choose from two different versions of Security Builder API for .NET – a version that provides both Suite B-level security and a FIPS 140-2 cryptographic module and another version that just provides Suite B-level security.

Table 1: Supported Algorithms

Security Builder API for .NET with Suite B

ALGORITHM	Security Builder Crypto-C 5.2*	.NET Compact Framework	.NET Framework
AES	YES	-	-
MD5	YES	-	3.0
SHA1	YES	-	3.0
SHA256	YES	-	3.0
SHA384	YES	-	3.0
ECDH	YES	-	3.0
ECDSA	YES	-	3.0
ECMQV	YES	-	-

Security Builder API for .NET with Suite B and FIPS

ALGORITHM	Security Builder Crypto-C 5.2*	.NET Compact Framework	.NET Framework
AES	YES	-	-
MD5	YES	-	3.0
SHA1	YES	-	3.0
SHA256	YES	-	3.0
SHA384	YES	-	3.0
ECDH	YES	-	3.0
ECDSA	YES	-	3.0
ECMQV	YES	-	-

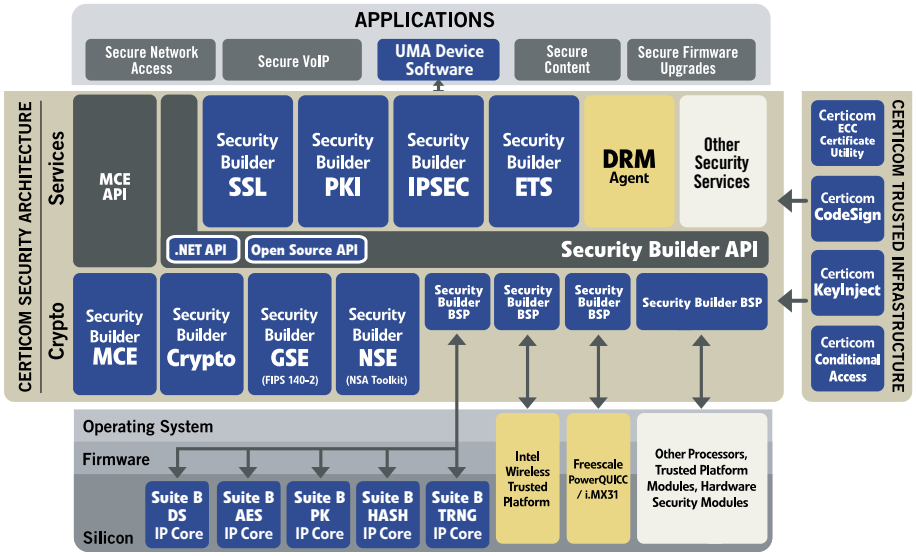
*first release

Table 2: Supported Platforms

Security Builder API for .NET with Suite B		Security Builder API for .NET with Suite B and FIPS	
.NET 1.0/1.1	**.NET 2.0**	**.NET 1.0/1.1**	**.NET 2.0**
• Win32 .NET	• Win32 .NET	• Win32 .NET	• Win32 .NET
• Win64 .NET	• Win64 .NET	• Windows Mobile 2003	• Windows Mobile 2003
• Windows Mobile 2003	• Windows Mobile 2003	• Windows Mobile 2003 Emulator	• Windows Mobile 2003 Emulator
• Windows Mobile 2003 Emulator	• Windows Mobile 2003 Emulator	• Windows CE 4.x/ 5.x	• Windows CE 5.x
• Windows CE 4.x/ 5.x	• Windows CE 5.x		

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.



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™

Certicom White Papers

To read Certicom white papers, visit www.certicom.com/whitepapers.

Sum Total: Determining the True Cost of Security
Sourcing Security: Five Arguments in Favour of Commercial Security Solutions

Government

Making the Grade: Meeting Government Security Requirements (Suite B)
Meeting Government Security Requirements: The Difference Between Selling to the Government and Not
FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

Mobility

The Inside Story
Many Happy Returns: The ROI of Embedded Security
Welcome to the Real World: Embedded Security in Action

Sensor Networks

Securing Sensor Networks

DRM & Conditional Access

Injecting Trust to Protect Revenue and Reputation: A Key Injection System for Anti-Cloning, Conditional Access and DRM Schemes
Achieving DRM Robustness: Securing the Device from the Silicon Up to the Application(PDF)

Enterprise Software

Using Digital Signatures to cut down on Bank Fraud Loss

ECC

An Elliptic Curve Cryptography Primer
ECC in Action: Real World Applications of Elliptic Curve Cryptography
Using ECC for Enhanced Embedded Security (PDF)