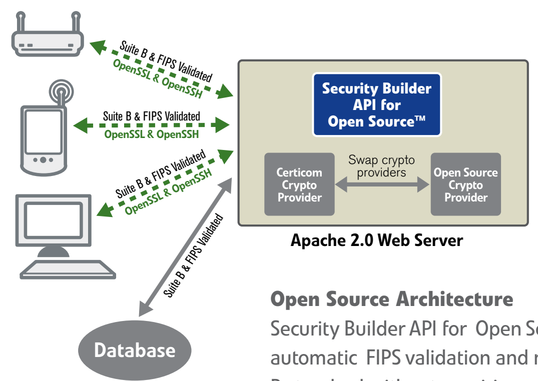
Security Builder® API for Open Source™

INCREASE NUMBER OF TRANSACTIONS PROCESSED BY 300%, MEET SUITE B SECURITY REQUIREMENTS, AND AUTOMATICALLY GAIN FIPS VALIDATION ON ALL MAJOR PLATFORMS

Certicom Security Builder API for Open Source enables developers to dramatically improve the performance and enhance the security of their SSL and SSH applications with Elliptic Curve Cryptography (ECC) – without requiring developers to re-code.

In addition, developers are able to plug into Certicom ECC cryptographic providers quickly and easily – gaining complete Suite-B level security, achieving FIPS 140-2 validation on all major platforms automatically, and enhancing performance to significantly increase the number of SSL/TLS transactions processed.



Open Source Architecture

Security Builder API for Open Source enables automatic FIPS validation and meeting of Suite B standard without requiring any re-coding.

DRAMATICALLY IMPROVE PERFORMANCE

Using 224-bit ECC in OpenSSL leads to a performance improvement that enables 300% more transactions to be processed in any given timeframe. This increased efficiency – which results from switching to ECC from RSA – is attributed to the small key size of ECC algorithms.

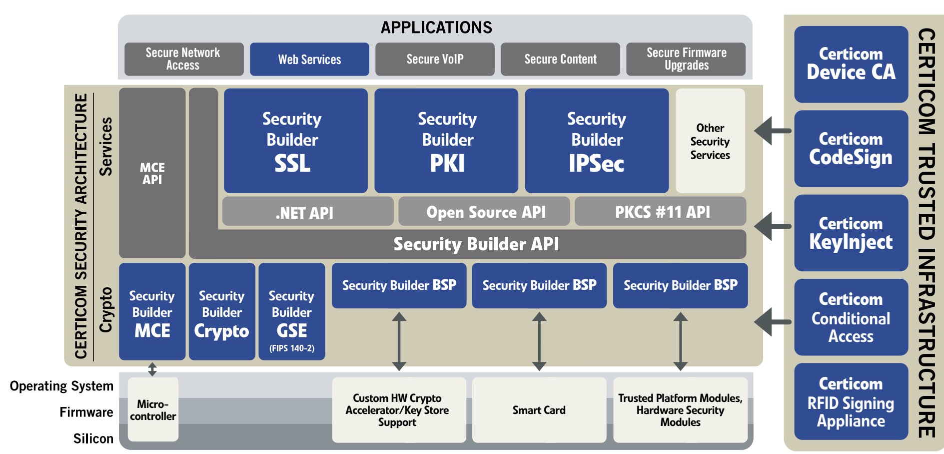
REDUCE TIME-TO-MARKET

Meeting FIPS requirements can take 8-12 months – assuming you get it right the first time. Most don't. 48% of crypto modules have security flaws and 30% of algorithms do not conform to standard. 20% fail the second time around as well. Security Builder API for Open Source enables developers to plug in Certicom's pre-approved cryptographic module and cryptographic providers – saving an enormous amount of development time without requiring any re-coding or changes to your legacy systems.

MEET SUITE B AND FIPS REQUIREMENTS

Companies can't sell products that use encryption to government agencies without FIPS validation. And since government networks use a wide range of platforms, Certicom enables customer to meet FIPS 140-2 validation on all major platforms with a pre-approved cryptographic module. As the primary source of Suite B technology, Certicom can help you achieve complete Suite B compliance quickly and easily.

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 and PKI; hardware security cores and board support packages (BSP) that expose cryptographic functionality available in hardware. An application using SSL can benefit from CSA to enable either a FIPS, non-FIPs provider (SB-Crypto) or native hardware crypto provider.



Features

Certicom Security Builder API for Open Source delivers tremendous performance and portability while enabling developers to dramatically enhance security, achieving complete Suite B-level security and automatic FIPS 140-2 validation for all major platforms and leading applications.

	Security Builder API for Open Source with Certicom Crypto Provider	Security Builder API for Open Source with Certicom Crypto Provider and FIPS
Programming Language	C	C
Cryptographic Providers	Security Builder Crypto-C 5.x	Security Builder GSE-C 2.x *
Symmetric Encryption	AES, DES, RC2 and RC4	AES, DES, RC2 and RC4
Asymmetric Encryption	RSA	RSA
Key Agreement/Key Transport	ECDH, DH	ECDH, DH
Digital Signatures	ECDSA, RSA	ECDSA, RSA
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
Platform Support	• Linux ARM • Linux x86 • Windows x86	• Linux x86 • Windows x86

* FIPS Certificate #542

Table 1: Security Builder SSL-C vs. OpenSSL:
Comparing time required for authentication using ECDH/ECDSA cipher suites and RSA cipher suites **

Server Authenticated	OpenSSL (ms)			Security Builder SSL-C (ms)		
CIPHER SUITE	**CLIENT**	**SERVER**	**TOTAL**	**CLIENT**	**SERVER**	**TOTAL**
TLS RSA with AES 256 SHA 1024	5.98	11.03	17.01	2.77	6.19	8.96
TLS RSA with AES 256 SHA 2048	7.55	50.58	58.13	6.28	39.27	45.55
TLS RSA with AES 256 SHA 3072 (Suite B)	**11.06**	**152.73**	**163.79**	**11.70**	**121.85**	**133.55**
TLS ECDH ECDSA with AES 256 CBC SHA 224 R1	39.39	8.74	48.13	9.16	3.93	13.09
TLS ECDH ECDSA with AES 256 CBC SHA 256 R1 (Suite B)	**31.97**	**10.46**	**42.43**	**15.41**	**5.47**	**20.88**

** 2 processor 933 MHz Pentium III running Windows 2000 Professional Service Pack 4

Minimal code changes required.

Have your systems up and running in a matter of hours.

Table 2: Suite B Performance Comparison: Security Builder Crypto-C vs. OpenSSL***

	ALGORITHM/ CURVE	OPERATION	THROUGHPUT
OpenSSL	secp384r1	ECDSA_sign ECDSA_ver ECDH_raw	630 op/s 120 op/s 140 op/s
	secp256r1	ECDSA_sign ECDSA_ver ECDH_raw	1364 op/s 270 op/s 321 op/s
Security Builder	secp384r1	ECDSA_sign ECDSA_ver ECDH_raw	1150 op/s 220 op/s 263 op/s
	secp256r1	ECDSA_sign ECDSA_ver ECDH_raw	2297 op/s 440 op/s 510 op/s

*** Intel Pentium 4 CPU, with 3.00GHz, running on Linux Red Hat.

About Certicom

Certicom, a wholly owned subsidiary of Research In Motion Limited (RIM) (Nasdaq: RIMM; TSX: RIM), manages and protects the value of content, applications and devices with government-approved security. Adopted by the National Security Agency (NSA) for government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the global leader in ECC, Certicom's security offerings are currently licensed to hundreds of multinational technology companies, including IBM, General Dynamics, Motorola and Oracle. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada with worldwide sales offices in USA and Asia. Visit www.certicom.com.

certicom™

USA
3600 Glen Canyon Rd., Suite 1
Scotts Valley, CA 95066
USA
Tel: 1.831.438.4100
Fax: 1.831.438.4111
Sales: 1.800.561.6100
sales@certicom.com

Corporate Headquarters
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Canada
Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com

Japan
Research In Motion Japan Ltd.
Nippon Brunswick, Building 7F
5-27-7 Sendagaya,Shibuya-ku,
Tokyo 151-0051, Japan
Tel: 03 6367 3567
sales@certicom.com