certicom™

Security Builder® SSL™

COMPLETE SECURE SOCKETS LAYER PROTOCOL SECURITY MODULE

Add complete Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol security to your Internet communications without sacrificing development time or incurring security risks. Security Builder® SSL™ by Certicom offers a single application programming interface (API) for more than 30 platforms and is optimized for a variety of environments including constrained devices and wireless applications. Eighty percent smaller than open source alternatives, this unique design supports client and server authentication, is backed by an expert support organization and can be configured with Security Builder® GSE™—Certicom's FIPS 140-2 Validated cryptographic module. Security Builder SSL also contains Suite B algorithms that support the National Security Agency's (NSA) requirements for the U.S. Government Crypto Modernization Program.

Security Builder SSL* provides protocols to the Certicom® Security Architecture™ — a comprehensive, portable and modular solution designed to allow developers to quickly and cost-effectively embed security across multiple families and generations of devices.

REDUCE TOTAL COST OF OWNERSHIP

Backed by years of experience, extensive testing and expert service, Security Builder SSL uses patented technologies and is designed to meet the most rigorous certifications to avoid the vulnerabilities of open source solutions. This helps you to get your product to market faster with fewer errors and protects your bottom line from legal and security risks. Gain additional peace of mind knowing that Certicom monitors Internet security advisories such as CERT and NISCC, and provides customers with immediate updates if affected.

OPTIMUM PERFORMANCE

Optimized to be fast and efficient, Security Builder SSL offers the performance required for security on everything from mobile and embedded devices to desktops and servers. This results in faster processing, better bandwidth usage, reduced storage and longer battery life. As an option, organizations can choose compression and standards-based SSL/TLS cipher suites that support elliptic curve cryptography (ECC), further enhancing performance abilities.

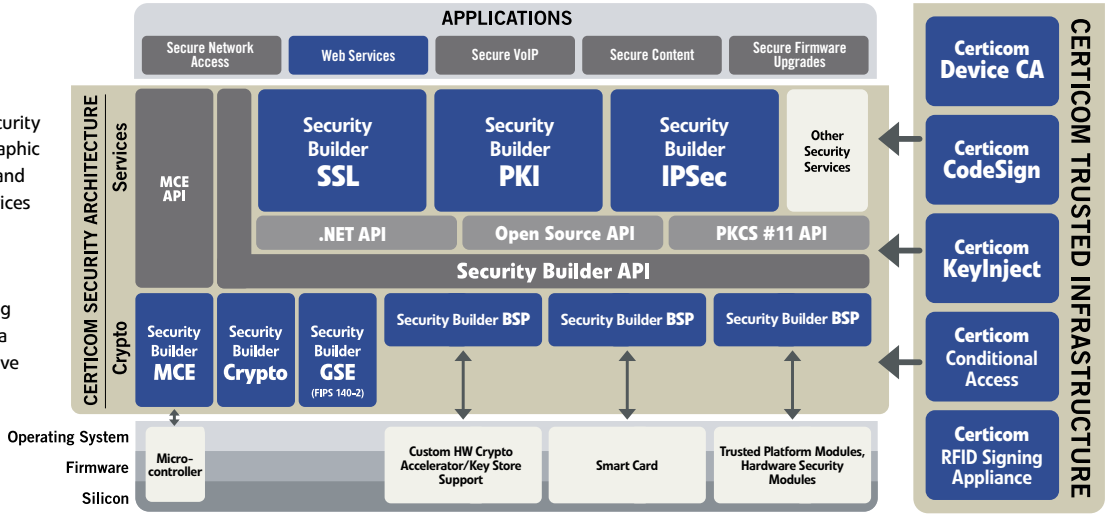
RAPID DEPLOYMENT

Security Builder SSL ships with an API that provides a single, common interface between the protocols and cryptographic providers of the Certicom Security Architecture*, simplifying your development cycle and speeding time to market. The Rapid Application Development option enables Security Builder SSL to be dropped into your application or device quickly, further saving development time and money.

PROVEN INTEROPERABILITY

Thoroughly tested and supported, Certicom's implementation offers compliance with standards such as ANSI, FIPS, IETF, ISO and NIST and the newly published NSA Suite B requirements. Security Builder SSL also supports leading browsers and third-party certificate authorities such as VeriSign and Thawte. Combined with support for x.509 v1 and v3 certificates, Security Builder SSL can secure any size application or device.

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.



*Security Builder SSL-C only

Features

Enabling you to make your devices and applications Certicom Secure

Security Builder SSL is part of the suite of Security Builder modules that are used by more than 300 customers for thousands of applications, including Citrix, Motorola, Oracle, Sterling Commerce, and Sybase. For examples of how the CSA can add strong security to your project, visit **www.certicom.com/csa**

Certicom Professional Services can help integrate security within your existing applications, develop custom applications, provide guidance relating to Elliptic Curve Cryptography (ECC), and architect solutions. For more information, call **1-800-561-6100.**

	Security Builder SSL-C	Security Builder SSL-J
Programming Language	C	Java
Symmetric Encryption Algorithms	AES, DES, 3DES, RC2, RC4	AES, DES, 3DES, RC4
Asymmetric Encryption Algorithms	RSA	RSA
Authenticated Crypto Algorithms	AES-GCM	AES-GCM
Key Agreement/Key Transport	DH, ECDH, ECMQV	DH, ECDH, ECMQV
Digital Signatures	ECDSA, RSA, DSA	ECDSA, RSA, DSA
Hash Functions	SHA-1, SHA-2 (224, 256, 384, 512), MD5	SHA-1, SHA-2 (224, 256, 384, 512), MD5
Random Number Generation	ANSI X9.62, FIPS140-1/2 extension ANSI KDF, IEEE KDF1	ANSI X9.62, FIPS140-1/2 extension
Supported Hardware Accelerators/ Hardware Tokens	Safenet Cryptoswift, nCipher nShield	Via Sun JCE, nCipher nShield
Supported Software Cryptographic Providers	Security Builder Crypto-C, Security Builder GSE-C, Security Builder NSE-C	Security Builder Crypto-J, Security Builder GSE-J
X.509 Version 1 or 3 Digital Certificates	Yes	Yes
EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, SCTP	Yes	Yes
SSL 2.0, SSL 3.0, TLS V 1.0, TLS V 1.1, TLS V 1.2, WAP 2.0, DTLS 1.0	Yes	SSL 2.0, SSL 3.0, TLS V 1.0, TLS V 1.1, TLS V 1.2
Implementation Code Size Range	200 KB - 250 KB	570 KB - 650 KB
Compression Support	HiFn LZS, ZLIP, MiniLZO	—
Pre-shared Key (PSK)	Yes, including support for IMS	Yes
Virtual Hosting Module	Server name indication RCF 3546 TLS extensions	Server name indication RCF 3546 TLS extensions
TLS Extensions (RFC 4366)	Server Name Indication, Maximum Fragment Length Negotiation, Client Certificate URL	Server Name Indication
MOD_SSLC	Apache plug in for SSL	—
Suite B	Yes	Yes
Supported Platforms	Available for a wide range of platforms. Please contact your Certicom sales representative for additional details.	Supports JDK 1.5 and 1.6. Please contact your Certicom sales representative for additional details.

Cipher Suites (SSL-C and SSL-J)

RFC 4492
TLS_ECDH_ECDSA_WITH_NULL_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_NULL_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_NULL_SHA
TLS_ECDH_RSA_WITH_RC4_128_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_NULL_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_anon_WITH_NULL_SHA
TLS_ECDH_anon_WITH_RC4_128_SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA

RFC 5246
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_RC4_128_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_DH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA

DRAFT IETF
TLS_ECMQV_ECDSA_WITH_NULL_SHA
TLS_ECMQV_ECDSA_WITH_RC4_128_SHA
TLS_ECMQV_ECDSA_WITH_DES_CBC_SHA
TLS_ECMQV_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECMQV_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECMQV_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECMQV_RSA_WITH_NULL_SHA
TLS_ECMQV_RSA_WITH_RC4_128_SHA
TLS_ECMQV_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECMQV_RSA_WITH_AES_128_CBC_SHA
TLS_ECMQV_RSA_WITH_AES_256_CBC_SHA

RFC 3268
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA

RFC 4279
TLS_PSK_WITH_RC4_128_SHA
TLS_PSK_WITH_3DES_EDE_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA
TLS_PSK_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_CBC_SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA
TLS_RSA_PSK_WITH_RC4_128_SHA
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
TLS_RSA_PSK_WITH_AES_128_CBC_SHA
TLS_RSA_PSK_WITH_AES_256_CBC_SHA

RFC 5246
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_DSS_WITH_AES_128_CBC_SHA256
TLS_DH_DSS_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_128_CBC_SHA256
TLS_DH_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256

RFC 5288
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_DH_RSA_WITH_AES_128_GCM_SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_DSS_WITH_AES_128_GCM_SHA256
TLS_DH_DSS_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384

RFC 5288
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384

DRAFT IETF
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA

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

A Subsidiary of Research In Motion Limited RIM