BlackBerry | 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) and is optimized for a variety of environments including constrained devices and wireless applications. 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* supports 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.

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.

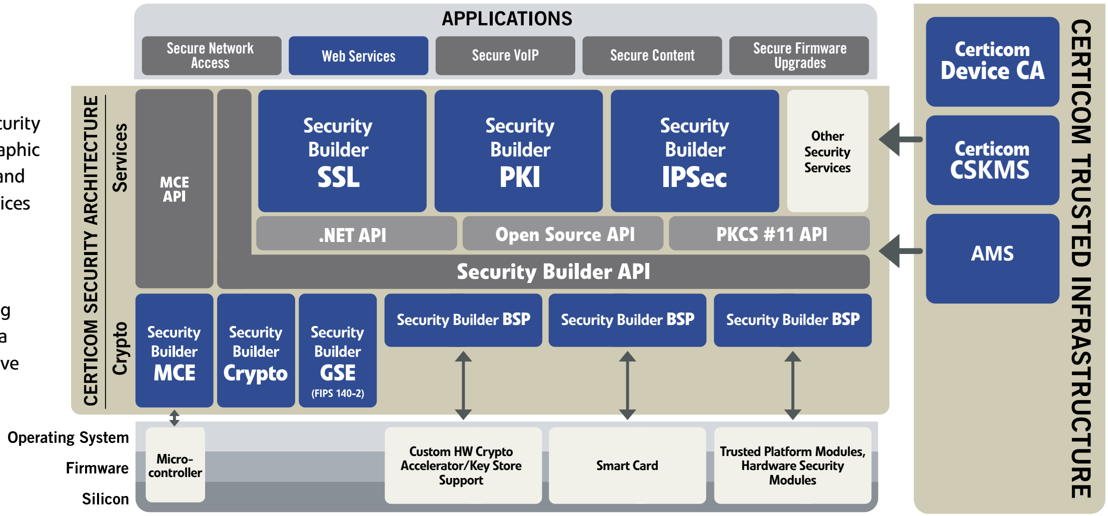
OPTIMUM PERFORMANCE

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.

PROVEN INTEROPERABILITY

Thoroughly tested and supported, Certicom's implementation offers compliance with standards such as ANSI, FIPS, IETF, ISO and NIST and 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 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

	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, FIPS 140-1/2 extension ANSI KDF, IEEE KDF1	ANSI X9.62, FIPS 140-1/2 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 Crypto-J, Security Builder GSE-J
X.509 v3 Digital Certificates EAP-TLS,	Yes	Yes
EAP-TTLS, EAP-FAST, PEAP, SCTP	Yes	Yes
TLS V 1.0, TLS V 1.1, TLS V 1.2, 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
Suite B	Yes	Yes
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
Supported Platforms	Please contact your Certicom sales representative for more details.	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

Founded in 1985 with a long-term focus on Elliptic Curve Cryptography, Certicom has been awarded over 500 patents. As a leader in applied cryptography and key management, Certicom provides managed PKI, key management and provisioning technology that helps to protect customers' device firmware, applications, and long-lived assets. Certicom is a critical element of the Blackberry cybersecurity portfolio deploying the first and best in class end-to-end security solutions used in preventing product counterfeiting, re-manufacturing, and rogue network access. Blackberry Certicom's secure key provisioning, code signing and identity management solutions are field- proven to protect next-generation connected cars, critical infrastructure and IoT deployments.

BlackBerry | certicom

Corporate Headquarters
4701 Tahoe Blvd, Building A
Mississauga, ON L4W 0B4
Canada
Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com