BlackBerry | certicom

Security Builder® Crypto™

CROSS-PLATFORM CRYPTOGRAPHIC MODULE

Integrate encryption, digital signatures and other security mechanisms into any application or device, using the first toolkit to include standards-based Elliptic Curve Cryptography (ECC) implementations. Security Builder® Crypto™, Certicom's cross-platform cryptographic module, is built for small code size and includes a range of current and legacy algorithms that provide proven security to constrained environments.

Security Builder Crypto** acts as a software cryptographic provider within 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.

COMPREHENSIVE SECURITY

The long-term interoperability of your security design is assured through compliance with ANSI, IEEE and FIPS standards as well as the NSA Suite B requirements, and a wide range of algorithms including ECC, RSA, DSA, DH, SHA-2, and AES. These algorithms provide the necessary security for SSL/TLS, IKE v1/IKE v2/IPSec.

IMPROVED ROI

The same API for multiple platforms means Security Builder Crypto can be easily integrated into your applications with no porting required —cutting development costs and time-to-market. Choose from multiple programming languages—including C and Java. Used within the context of the Certicom Security Architecture, this application programming interface (API)** provides a single, common interface between the services, applications and cryptographic providers, further simplifying your development cycle.

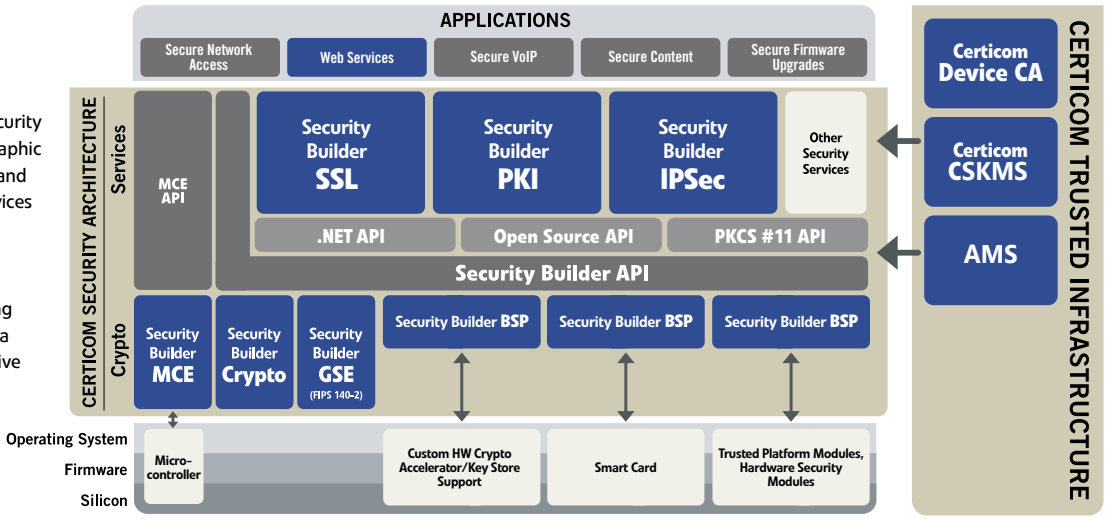
SMALLER AND FASTER

Optimized for constrained platforms, the full cryptographic suite of algorithms within Security Builder Crypto can also be used in desktops and servers. The option to link only the features you need means compact implementations resulting in faster processing, better bandwidth usage, reduced storage and longer battery life.

BETTER PERFORMANCE

As the Advanced Encryption Standard (AES) replaces older security algorithms, public-key sizes must be increased to provide equivalent strength for AES. ECC provides smaller key sizes with higher strength-per-bit of any public-key cryptosystem today, resulting in better performance in constrained environments.

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.



*Suite B is the NSA's cryptographic specifications for securing classified and unclassified communications: http://www.nsa.gov/ia/industry/crypto_suite_b.cfm?MenuID=10.2.7.
**Security Builder Crypto-C only

Features

	Security Builder Crypto-C	Security Builder Crypto-J
Programming Language	C	Java
Symmetric Encryption	AES, 3DES	AES, 3DES
Asymmetric Encryption	RSA, ECIES	RSA, ECIES
Key Agreement/Key Transport	DH, ECDH, ECMQV, RSA	DH, ECDH, ECMQV, RSA
Digital Signatures	ECDSA, ECQV, RSA, DSA, RSA-PSS,	ECDSA, RSA-PSS, DSA,
Hash Functions	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-3, MD2, MD4, MD5, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-MD5, ANSI KDF, IEEE KDF1	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD2, MD5, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-MD5, ANSI KDF, IEEE KDF1
Random Number Generation	ANSI X9.62 RNG, FIPS 140-2, Hash_DRBG, HMAC_DRBG, CTR_DRBG	ANSI X9.62 RNG, FIPS140-2, Hash_DRBG, HMAC_DRBG, CTR_DRBG
Platform Support	Available for a wide range of platforms. Please contact your Certicom sales representative for additional details.	Please contact your Certicom sales representative for additional details.

Please contact Certicom about support for other platforms, other cryptographic providers and for source code releases.

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