certicom | BlackBerry Subsidiary

SECURITY BUILDER™
SOFTWARE LIBRARIES

GO TO THE LIBRARY TO GET HIGH SECURITY

Validated security software libraries make security easy.

Certicom, a Blackberry subsidiary, is a recognized leader in public key infrastructure (“PKI”) security design, innovation, and delivery. Certicom offers government validated crypto libraries, PKI certificate services, and asset management systems to make products, ecosystems, and manufacturing chains not just secure, but BlackBerry Secure.

Certicom’s Security Builder software libraries make it easy to gain security without having to become a crypto expert, and being validated to the highest standards such as FIPS 140-2, allows companies to address applications that store or transfer "sensitive" information to government agencies or entities that interact with them (such as VA hospitals).

But, the need for validated security goes beyond strict government mandates and is being increasingly adopted as “Best Practices” for industrial automation (e.g. industrial gateways and networking), mobile, medical, smart grid, automotive/telematics, and other applications.

Security Libraries

CONFIDENTIALITY. INTEGRITY. AUTHENTICATION

The modern supply chain is filled with points of attack where cloning and counterfeiting happen.

Certicom’s government validated crypto libraries make products, ecosystems, and manufacturing chains not just secure, but BlackBerry Secure, without having to become a crypto expert.

SECURITY BUILDER LIBRARIES

Multi-platform, patented, proven, validated security.

Certicom's Security Builder C and Java software libraries are Software Developer Kits (SDKs) which make it easy for system designers to implement security features, without having to become a crypto expert. Certicom's libraries have been proven in hundreds of millions of devices and are a convenient and cost-effective way to license core ECC technology.

Signing Algorithms: Support for ECDSA, RSA, DSA, and ECQV digital signature algorithms.

Hashing Algorithms: Support for a wide range of hashing algorithms is provided, ranging from several of the SHA protocols to HMAC and others.

Key Agreement: ECDH and RSA Key agreement and other Elliptic Curve models such as ECMQV.

Symmetric Algorithms: Symmetric protocols used in encryption and authentication are provided including AES, DES, 3DES, and others.

Asymmetric Algorithms: Asymmetric protocols used in encryption and authentication are also provided, including RSA and ECIES.

FIPS Level 1 Validated 140-2

VALIDATED

Government level, best practices.

Government Security Edition (Security Builder GSE) validated crypto libraries allow designers to build client and server side applications requiring FIPS 140-2 Level 1 validation without the need to make a submission to the FIPS approval process. This shortens time to market and ensures compliance to government mandates. Certicom FIPS 140-2 Level 1 crypto libraries run the same code base as standard crypto libraries but are validated according to NIST (National Institute of Standards & Technology) CMVP (Cryptographic Module Validation Program) requirements & processes.

Security Builder libraries are available in both C and Java. As such, they represent one of the industry's most complete, flexible, and proven sets of security software. The libraries are provided in binary (lib) or JAR format and represent a comprehensive, optimized, and robust set of standard crypto algorithms. The software is available on a per project or custom enterprise license basis.

SECURITY BUILDER BENEFITS

1 **OPTIMIZED:** Small code space, faster processing, better bandwidth, reduced storage needs, and longer battery life.

2 **PKI SUPPORT:** Supports PKI certificate encoding, decoding, nd validation

3 **FLEXIBLE:** Ability to link to only the features needed for use on desktops, laptops, and servers. Compact implementations of a minimal algorithms set can be as small as 40 KB.

4 **FIPS CERTIFIED:** Help OEMs and application providers meet important government security requirements such as FIPS140-2, and NSA's NIAP.

5 **RANGE OF ALGORITHMS:** Provides security to SSL/TLS (TLS 1.2), IKEv1/IKEv2, IPSec, and other data at rest or data in motion security applications.

6 **TIME TO MARKET:** Fully tested and certified algorithms shortens time to market.

7 **SIMPLE:** End to end security via a single common API simplifies design. Complete documentation, support and maintenance.

8 **AVAILABLE:** On many operating system platforms including QNX, Linux, iOS, Android, and Windows.

Certicom also offers porting service to enable customers to use the libraries on a wide number of embedded and enterprise platforms using 32 or 64-bit processors.

9 **ECC LICENCE:** Per project or custom enterprise licenses are available.

ALGORITHMS

Full complement of support.

Security Builder is a powerful, flexible, and certified security solution supporting a wide range of algorithms.

Feature	Security Builder Crypto-C	Security Builder Crypto-J
Programming Language	C	Java
Symmetric Encryption Algorithms	AES, DES, 3DES, RC2, RC4, RC5*	AES, DES, 3DES, RC2, RC4, RC5*
Asymmetric Encryption Algorithms	RSA, ECIES	RSA, ECIES
Key Agreement/Key Transport	DH, ECDH, ECMQV, RSA	DH, ECDH, ECMQV , RSA
Digital Signatures	ECDSA, ECQV, RSA, DSA, RSA-PSS, ECNR	ACDSA, RSA, DSA
Hash Functions	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, 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, FIPS 140-2, Hash, RBG, HMAC_DRBG, CTR_DRBG
Implementation Code Size	As low as 40 KB depending on algorithms linked	N/A
Supported Platforms	Support for leading enterprise, mobile and embedded platforms including: Linux, Windows, Apple OS X, iOS, Android, and QNX on x86, ARM and other processor architectures.	JDK 1.5, 1.6, 1.8, and Android Dalvek

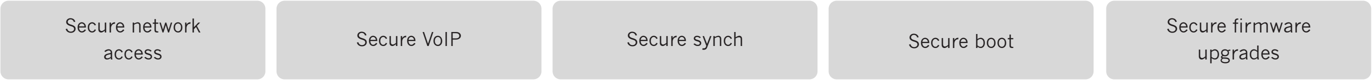
* RC5 available to customers outside the United States only.

Algorithms that are not on the list can be provided as custom developments, as needed.

SECURITY BUILDER ARCHITECTURE

Applications.

Typical applications that the libraries cover are network access, secure VoIP, secure synch, secure boot, and secure firmware upgrades.



Secure network access

Secure VoIP

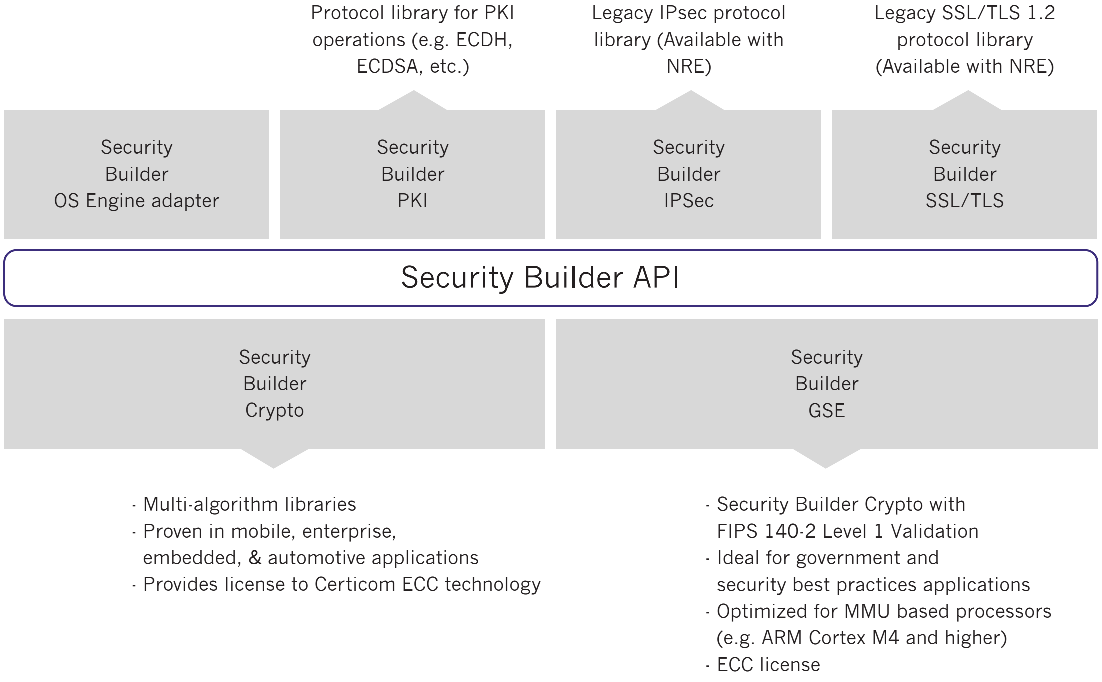
Secure synch

Secure boot

Secure firmware upgrades

Architecture.

Certicom's security architecture modules are described in the diagram below.



Protocol library for PKI operations (e.g. ECDH, ECDSA, etc.)

Legacy IPsec protocol library (Available with NRE)

Legacy SSL/TLS 1.2 protocol library (Available with NRE)

Security Builder OS Engine adapter

Security Builder PKI

Security Builder IPSec

Security Builder SSL/TLS

Security Builder API

Security Builder Crypto

Security Builder GSE

- Multi-algorithm libraries
- Proven in mobile, enterprise, embedded, & automotive applications
- Provides license to Certicom ECC technology

- Security Builder Crypto with FIPS 140-2 Level 1 Validation
- Ideal for government and security best practices applications
- Optimized for MMU based processors (e.g. ARM Cortex M4 and higher)
- ECC license

NOT JUST SECURE, BUT BLACKBERRY SECURE

There is a reason that BlackBerry is synonymous with security

It is because security is as elemental to an electronic system as DNA is to an organism—and security is BlackBerry's DNA.

Robust security cannot just be bolted on. It must be infused right from the start, which is why BlackBerry Security has been trusted by world leaders for over two decades and is the mobility partner of all G7 governments, 16 of the G20 governments, 10 out of 10 of the largest global banks and law firms, and the top five largest managed healthcare, investment services, and oil and gas companies. BlackBerry Security has earned more than 70 government certifications and approvals - greater than any other mobile vendor.

Vulnerabilities are growing rapidly and present a serious risk, especially in the evolving automotive industry, so BlackBerry continues to expand its coverage with advanced technologies, tools, design consulting, and testing services for true end-to-end, layered security.

World leaders
in government and
industry trust
BlackBerry Security
to help run their secure
communications,
networks,
in-car systems,
nuclear infrastructure, and
other mission-critical
functions.

Learn what they have
already discovered.

BlackBerry and its subsidiaries, Certicom and BlackBerry QNX, provide products and services that make things not just secure, but BlackBerry Secure.

Certicom Corp., subsidiary of BlackBerry manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM, General Dynamics, and SAP. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada.

www.certicom.com

QNX Software Systems Limited, subsidiary of BlackBerry is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada.

www.qnx.com