certicom™

Security Builder® BSP™

BOARD SUPPORT PACKAGE FOR OPTIMIZED HARDWARE-BASED SECURITY

Embed strong and fast hardware-based security quickly and easily: Security Builder® BSP™, a board support package for optimized hardware-based security, provides portable, high-performance security across multiple processors, trusted platform modules, hardware security modules or smart cards. Security Builder BSP exposes the security features within a specific hardware cryptographic provider, such as those mentioned below, so that any security application can take advantage of hardware security provider benefits.

- **the Intel® Wireless Trusted Platform**
- **Freescale PowerQUICC and i.MX31 processors**
- **the US Federal Government Personal Identity Verification (PIV) cards**
- **Hardware Security Modules (HSM) from nCipher, SafeNet, and Utimaco**
- **TI OMAP Processors**

IMPROVED PERFORMANCE AND STRONGER SECURITY

Through tight integration with the optimized security building blocks within the hardware, Security Builder BSP allows you take advantage of the more efficient cryptographic operations, reduced power consumption and stronger protection that security embedded in hardware delivers. In combination with the Security Builder application programming interface (API), cryptographic and key management requests are routed to available hardware, and to software for the remaining functions not provided by the chipset. This enables code sharing, minimizes code footprint and allows transparent access to hardware resources for improved performance.

PORTABILITY FOR FASTER TIME-TO-MARKET

Security Builder BSP provides flexibility in design and development decisions; write your application once for your products- with Security Builder BSP, only minimal code changes for security are needed if you alter the underlying hardware. Available for multiple hardware cryptographic providers and trusted platform modules, Security Builder BSP makes it easy to change processors without affecting time to market.

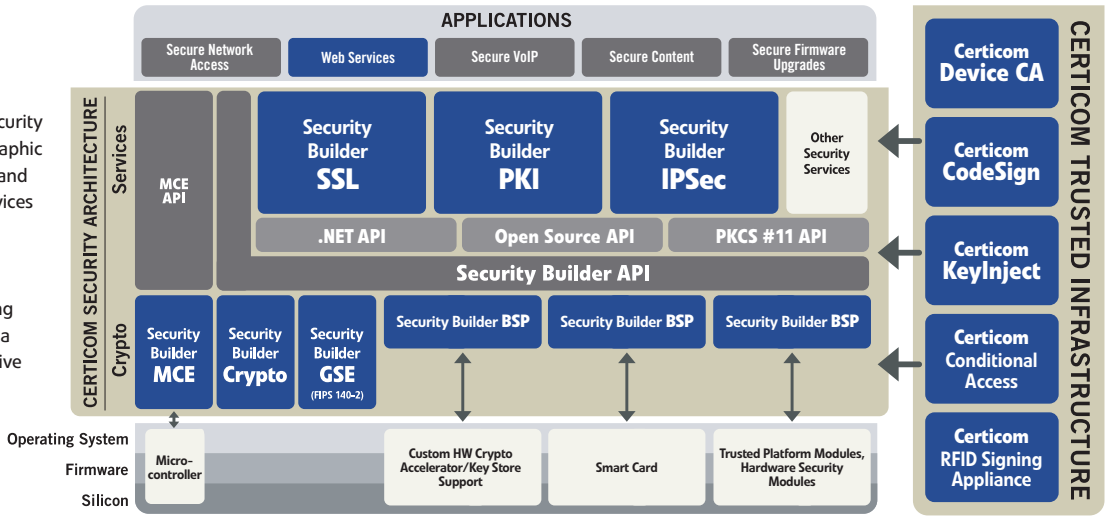
LOWER COSTS OF DEVELOPMENT

Security Builder BSP eliminates the need to integrate multiple toolkits and minimizes the need for expensive cryptography development and hardware expertise by protecting the details of underlying security resources with a common API. If changes are made to the chipset, you can leverage the same security architecture and re-use existing code.

PART OF A COMPREHENSIVE ARCHITECTURE

Security Builder BSP is a crucial component of the Certicom Security Architecture, a modular set of software cryptographic providers, security services and board support packages which expose cryptographic functionality and key management available in hardware. Security Builder BSP facilitates access to hardware-enabled security features by the higher level services, protocols and applications, providing strong, cost-effective security.

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 BSP facilitates faster time to market while lowering development costs by quickly and cost effectively embedding security across multiple families and generations of devices. The following hardware features are supported through Security Builder BSP for the platforms listed.

MICROPROCESSORS

Hardware Features Supported	Intel Wireless Trusted Platform	Freescale PowerQUICC	Freescale i.MX31	TI OMAP
Symmetric Encryption Algorithms	AES	AES	–	DES, 3DES
Hash Functions	SHA-1, HMAC SHA-1	SHA-1, HMAC SHA-1, HMAC SHA-2	SHA-1	SHA-1, MDS
Digital Signatures	RSA	ECDSA, RSA	–	–
Key Agreement/Key Transport	DH	DH, ECDH, ECMQV	–	–
Random Number Generation	✓	✓	✓	✓
Hardware Key Management				
Key Generation	✓	✓	–	–
Secure Key Storage	✓	–	Key wrapping	–
Monotonic Counter	✓	–	–	–
Supported Operating Systems	MontaVista Linux *	Wind River VxWorks *	MontaVista Linux *	MontaVista Linux *
Platform Models	–	–	–	1710, 162x, 5912

** Other RTOS and OS available upon request from Certicom.*

HARDWARE SECURITY MODULES AND SMART CARDS VIA PKCS#11

Hardware Features Supported	US Government Personal Identity Verification (PIV)	Safenet Luna PCI, Luna CA3 and Protect Server Orange (Eracom)	nCipher nFast, nForce, nShield, netHSM	Utimaco CryptoServer
Symmetric Encryption Algorithms	–	DES, 3DES, AES	DES, 3DES, AES	DES, 3DES, AES
Hash Functions	–	SHA-1, MD5, HMAC SHA-1	SHA-1, MD5, HMAC SHA-1	SHA-1, SHA-2
Digital Signatures	RSA	RSA, DSA, ECDSA	RSA, DSA, ECDSA	RSA, DSA, ECDSA
Key Agreement/Key Transport	–	RSA, DH	RSA, DH	RSA, DH
Random Number Generation	✓	✓	✓	✓
Hardware Key Management				
Key Generation	–	✓	✓	✓
Secure Key Storage	✓	✓	✓	✓
Supported Operating Systems	Win CE, Win 32*	Linux, Solaris*	Linux	Linux
FIPS 140-1/2 Level 3	✓card dependent	✓card dependent	✓card dependent	✓card dependent

** Other RTOS and OS available upon request from Certicom.*

For cryptographic functionality not provided by the above hardware, Security Builder® Crypto™ can be licensed separately to provide additional software cryptographic functionality.

FIPS 140-2 is required for sale of products implementing cryptography to the federal government. Because of the high level of security ensured by FIPS, the financial and healthcare industries are also starting to mandate FIPS 140-2 to secure their transactions. Security Builder® GSE™ is a FIPS 140-2 Validated cryptographic module that can also be licensed from Certicom.

Need to know how to use Certicom Security Architecture?

Security Builder BSP is part of the suite of Security Builder modules that are used for thousands of applications by more than 300 customers, including BEA Systems, Motorola, Research in Motion, Sybase, Texas Instruments and Unisys.

For more information, visit **www.certicom.com/securitybuilder**.

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