certicom™

Security Builder® GSE™

FIPS 140-2 VALIDATED/NSA SUITE B–ENABLED CRYPTOGRAPHIC MODULE

Build trusted, government-approved security into your products. Security Builder® GSE™ enables developers to quickly build client and server-side applications that require a FIPS 140-2 level 1 validation and NSA Suite B-enabled cryptographic module.

Security Builder GSE 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.

MEETS GOVERNMENT SECURITY REQUIREMENTS

A number of government regulations mandate the use of FIPS Validated modules for the protection of data, especially in a wireless setting. Security Builder GSE has been validated on a wide variety of operating systems, languages and environments, including: AIX, HP-UX, Java, Linux, Palm, Solaris, Symbian, Windows, and Windows Mobile. Security Builder GSE also enables you to meet the NSA Suite B recommendations, a set of cryptographic specifications that require AES for encryption and elliptic curve cryptography (ECC) for key agreement and digital signatures to secure classified and unclassified communications. Security Builder GSE includes the named algorithms that address this new government requirement.

READY FOR THE FUTURE

Security Builder GSE for server-side is the only toolkit to support ECDSA, ECDH and ECMQV, three ECC-based algorithms specified in FIPS, Suite B and NIST Special Publications. As government cryptography requirements continue to evolve, the Certicom Security Architecture, which supports both ECC and RSA, provides a bridge from legacy RSA to ECC implementations.

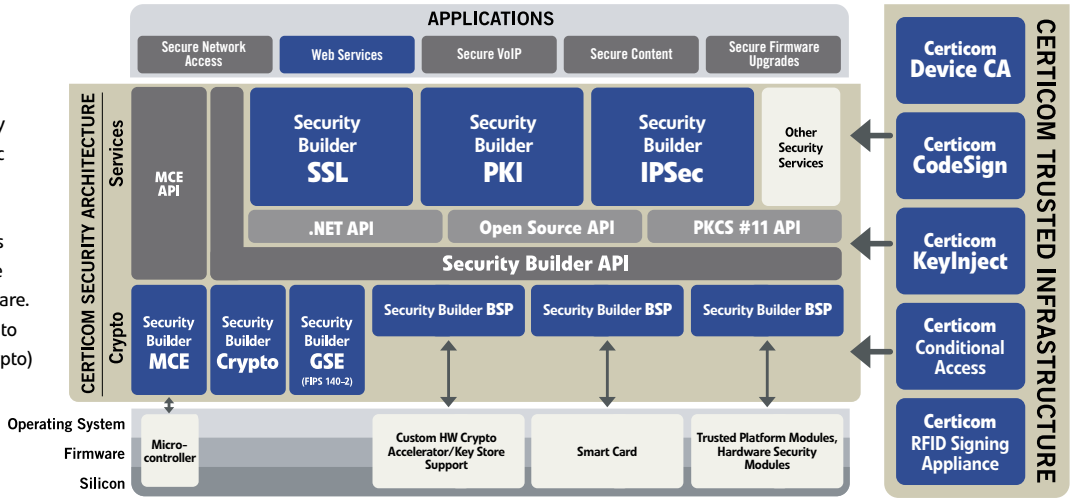
REDUCES TIME TO MARKET

By building on Security Builder GSE, you can avoid the lengthy and expensive FIPS Validation process and get your product to market more quickly. As well, by using a pre-validated module you can meet security requirements without having to pull valuable resources from your core competency. All the toolkits within the Certicom Security Architecture share a common API, which minimizes learning curve and enables easy integration.

COMPREHENSIVE SECURITY SOLUTION

With support for leading client and server-side operating systems in an implementation as small as 50 KB, Security Builder GSE helps you achieve end-to-end security using a single, common API. Within the Certicom Security Architecture, Security Builder GSE provides the module that allows Security Builder protocol toolkits to run in FIPS-approved mode of operation, further extending the range of applications that can be secured.

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.



Features

Security Builder GSE is available for both client and server-side platforms, providing end-to-end security. Unless otherwise listed, all components operate in FIPS-approved mode of operation. Choose a shared library architecture if your operating system supports shared or dynamic load libraries. For certain operating systems that do not support shared libraries, the object module architecture of Security Builder 3.x allows the code to be compiled into a single object file that can then be linked with the application code.

	Security Builder GSE-C 2.x	Security Builder GSE-J 2.x
Programming Language	C	Java
Architecture	Shared Library	Single JAR file
FIPS 140-2 Validation	Certificate #542, #829, #882	Certificate #578, Certificate #792
Suite B support	Yes	Yes
FIPS Validated Algorithm Implementations For certificate #s, visit http://csrc.nist.gov/cryptval/	AES, 3DES, DSA, ECDSA, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, RSA, RNG, SHA-1, SHA-256, SHA-384, SHA-512	AES, 3DES, DSA, ECDSA, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, RSA, RNG, SHA-1, SHA-256, SHA-384, SHA-512
TLS/IPSec support	Yes	Yes
Symmetric Encryption	AES, 3DES	AES, 3DES
Key Agreement/ Key Transport All these techniques may be used by a cryptographic module in an approved mode of operation	DH, ECDH, ECMQV, RSA	DH, ECDH, ECMQV, RSA
Digital Signatures	RSA, DSA, ECDSA	RSA, DSA, ECDSA
Hash Functions	HMAC, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, SHA-1, SHA-256, SHA-384, SHA-512	HMAC, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, SHA-1, SHA-256, SHA-384, SHA-512
Additional Algorithm Support (non-FIPS approved mode of operation)	RC2, RC4, MD2, MD4, MD5, HMAC-MD5, ARC2, ARC4, DES, DESX	RC2, RC4, MD2, MD4, MD5, HMAC-MD5, ARC2, ARC4, DES, DESX, ECIES
Random Number Generation	ANSI X9.62, FIPS 140-2 extension	ANSI X9.62, FIPS 140-2 extension, Hash_DRBG, HMAC_DRBG, CTR_DRBG††
Implementation Code Size Range	300KB-4 MB†	385 KB
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.

† depending on final algorithm combinations
†† Note: Hash_DRBG, HMAC_DRBG, CTR_DRBG are only available in Version 2.2

Object Module and Firmware Module validations available on a custom basis.

Need to know how to use the Certicom Security Architecture?
Over 300 customers and thousands of applications have already licensed Security Builder Developer Toolkits and Certicom Intellectual Property, including the National Security Agency, the Federal Aviation Authority, Honeywell, Research in Motion, Sybase and Texas Instruments. For a sampling of some of the ways you can use the toolkits to provide strong security for your project, 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