BlackBerry | certicom

Security Builder® GSE™

FIPS 140-2 VALIDATED 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 for the 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 and applications.

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. FIPS also helps demonstrate adherence to security best practices. In the US, for instance, compliance with FIPS 140-2 can help manufacturers of network-connected devices and application software demonstrate best practice encryption capabilities for protecting patient and user data.

Security Builder GSE has been validated on a wide variety of high-level and embedded operating systems, including QNX real-time OS, Android and iOS.

READY FOR THE FUTURE

Security Builder GSE is the only toolkit to support ECDSA, ECDH and EC MQV, three ECC-based algorithms specified in FIPS and NIST Special Publications. As government cryptography requirements continue to evolve, the flexibility of the Certicom Security Architecture, can provide a bridge to forward looking applications.

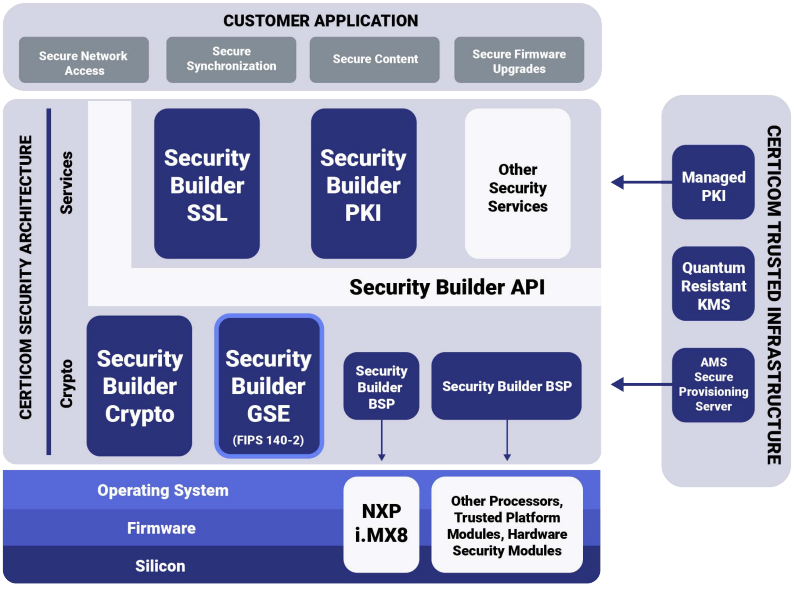
REDUCES TIME TO MARKET

By building on Security Builder GSE, you can avoid the lengthy and expensive FIPS validation process and get your product to market more quickly. Re-validation and re-branding options are also available if you wish for your product to be listed on the NIST Cryptographic Module Validation Program active validation list. By using a pre-validated module you can meet security requirements without diverting valuable resources and keep your developers focused on your core application.

COMPREHENSIVE SECURITY SOLUTION

With support for leading client and server-side operating systems, Security Builder GSE helps you achieve end-to-end security using a single, common API. This minimizes learning curve and enables easy integration across your company's product portfolio.

The Certicom Security Architecture is a comprehensive, portable and modular security platform supported by FIPS 140-2 validated Security Builder GSE-C. It offers cryptographic performance through assembly language and hardware instruction set optimizations for select platforms.



Features

Security Builder GSE is available for both client and server-side platforms, providing end-to-end security.

	Security Builder GSE-C 5.x	Security Builder GSE-C 6.x	Security Builder GSE-J 2.x
Programming Language	C	C	Java
Architecture	Shared Library	Shared Library	Single JAR file
FIPS 140-2 Validation	Certificate #1579	Certificate #1729 Certificate #3362	Certificate #2504 Certificate #2778 Certificate #3391
FIPS Validated Algorithm Implementations For certificate #s, visit http://csrc.nist.gov/cryptval/	AES, 3DES, DSA, ECDSA, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, RSA, DRBG, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	AES, 3DES, DSA, ECDSA, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, RSA, DRBG, SHA-1, SHA-224, 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, DRBG, SHA-1, SHA-256, SHA-384, SHA-512
TLS/IPSec support	Yes	Yes	Yes
Symmetric Encryption	AES, 3DES	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	DH, ECDH, ECMQV, RSA
Digital Signatures	RSA, DSA, ECDSA	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	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)	MD2, MD4, MD5, HMAC-MD5, ARC2, ARC4, DES, ECIES	MD2, MD4, MD5, HMAC-MD5, ARC2, ARC4, DES, ECIES	MD2, MD4, MD5, HMAC-MD5, ARC2, ARC4, DES, DESX, ECIES
Random Number Generation	ANSI X9.62, FIPS 140-2 extension, DRBG	ANSI X9.62, FIPS 140-2 extension, DRBG	ANSI X9.62, FIPS 140-2 extension, DRBG
Supported Platforms	QNX	Android iOS Linux MacOS QNX Windows	JDK 1.6, 1.7 and 1.8

Need to know how to use the Certicom Security Architecture?
Security Builder SDKs are portable cryptographic and Transport Layer Security protocol libraries used by device manufacturers and developers to secure their applications. Field-proven in hundreds of applications, Security Builder libraries have been deployed in hundreds of millions of devices including mobile handsets, telematics modules, smart meters and secure servers around the world. For a sampling of some of the ways you can use the Security Builder toolkits to provide strong security for your project, visit https://blackberry.certicom.com/en/products/sdk

BlackBerry | certicom

Founded in 1985 with a long-term focus on Elliptic Curve Cryptography (ECC), Certicom has been awarded over 500 patents. As a leader in applied cryptography, Certicom provides cryptographic libraries, PKI, key management and secure provisioning technology that helps to protect customer devices and sensitive assets. Acquired by BlackBerry in 2010, BlackBerry Certicom's secure provisioning, code signing and PKI solutions protect next-generation connected cars, critical infrastructure and large-scale IoT deployments.

www.certicom.com