BlackBerry | certicom

Security Builder® PKI™

DIGITAL CERTIFICATE MANAGEMENT MODULE

Add the confidence of digital certificates and signatures to your applications and devices using a module optimized for constrained environments. Security Builder® PKI™ provides trust and non-repudiation by enabling developers to add robust, standards-based digital certificate and key management to applications and devices including mobile phones, medical devices, connected cars, cable modems, IoT devices or any other networked electronic products.

Security Builder PKI provides certificate management protocols to the Certicom® Security Architecture™ – a comprehensive, portable and modular solution designed to allow developers to quickly and cost-effectively embed security into applications and across multiple families and generations of devices. Complemented by optimized Security Builder cryptographic libraries, the flexible architecture can take advantage of multiple cryptographic providers, including optional FIPS-validated components.

SMALLER AND FASTER

With a footprint as small as 100 KB, Security Builder PKI is ideal for constrained device platforms. The option to compile only the features you need enhances the compact design. Elliptic Curve Cryptography (ECC) provides additional performance benefits for such industry standards as ANSI X9.62 (The Elliptic Curve Digital Signature Algorithm) and ANSI X9.37 (Specifications for an Electronic Exchange of Check & Image Data).

INTEROPERABLE

Security Builder PKI adheres to a wide range of industry standards including: ANSI, IETF PKIX, ISO, PKCS, and FIPS, allowing your product to interoperate with other PKI-enabled applications and all major commercial Certification Authorities. The Java module enables enterprise software developers to quickly add support for protocols such as S/MIME v3 or AS1/AS2 Electronic Data Interchange over Internet (EDIINT) to your applications.

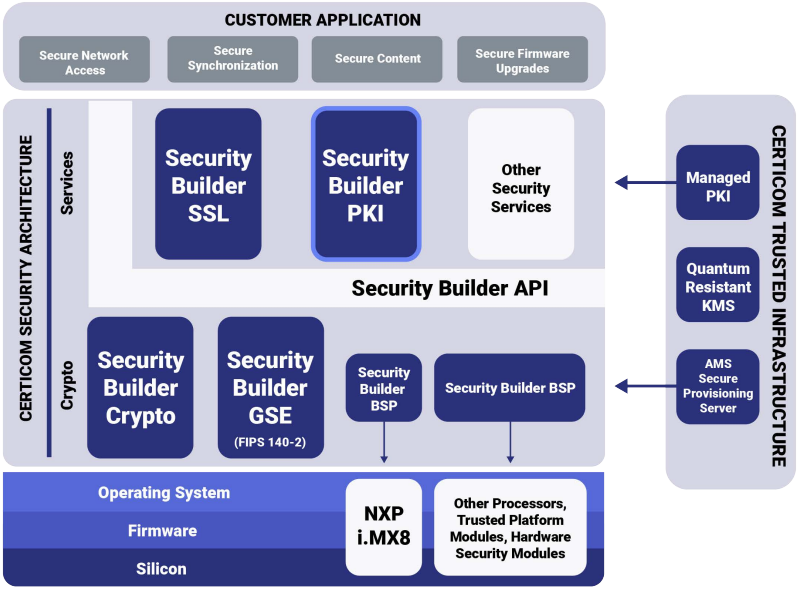
FLEXIBLE

Security Builder PKI can be integrated on a wide range of devices and platforms—and can be used with Security Builder® GSE™, a FIPS 140-2 Validated cryptographic module, to meet government requirements.

INCREASED ROI

The same API across platforms means Security Builder PKI drops easily into your application, cutting development costs and time-to-market and simplifying your development life-cycle

Security Builder® PKI™ is part of the Certicom Security Architecture, a comprehensive, portable and modular security platform that includes: software cryptographic providers that offer FIPS 140-2 validation and meet industry guidelines for ECC; security services like SSL, IPSec, PKI; hardware security cores and board support packages (BSP) that expose cryptographic functionality available in hardware.



Features

	Security Builder PKI-C	Security Builder PKI-J
Programming Language	C	Java
PKCS Compliant	# 1, 5, 7, 8, 9, 10, 12	# 1, 5, 7, 8, 9, 10, 12
X.509 Certificates	Version 3 supported key types: • ECC • DH • DSA • RSA	Version 3 supported key types: • ECC • DH • DSA • RSA
X.509 CRLs	Version 2	Version 2
X.509/PKIX Certificate Validation	• CRLs • LDAP certificate and CRL lookup • configurable validation rules • stored certificate and CRL lookup • hybrid certificate chains • per-certificate validation results	• CRLs • LDAP certificate and CRL lookup • configurable validation rules • stored certificate and CRL lookup • hybrid certificate chains • per-certificate validation results
Certificate Requests	PKCS #10	PKCS #10
Password-Based Encryption (PBE)	PKCS#5v1.5: • DES with MD2 • DES with MD5 • DES with SHA-1 • RC2 with MD2 • RC2 with MD5 • RC2 with SHA-1 PKCS#12v1.0: • RC2-40 with SHA-1 • RC2-128 with SHA-1 • RC4-40 with SHA-1 • RC4-128 with SHA-1 • 2-key3DES with SHA-1 • 3-key3DES with SHA-1 PKCS#5v2.0: • DES with HMAC SHA-1 • 3DES with HMAC SHA-1 • AES-128 with SHA-256 • AES-256 with SHA-256	PKCS#5v1.5: • DES with MD2 • DES with MD5 • DES with SHA-1 • RC2 with MD2 • RC2 with MD5 • RC2 with SHA-1 PKCS#12v1.0: • RC2-40 with SHA-1 • RC2-128 with SHA-1 • RC4-40 with SHA-1
CMS/PKCS #7	Enveloped Data (ECMQV, ECDH, DH, PKCS#1, ...) Signed Data (ECDSA, DSA, PKCS#1, ...) Encrypted Data (with PBE and non-PBE cryptography) unlimited data size (BER) unlimited # of attributes secure mailing lists signed receipts	EnvelopedData (ECMQV, ECDH, DH, PKCS#1, ...) Signed Data (ECDSA, DSA, PKCS#1, ...) EncryptedData (with PBE and non-PBE cryptography) unlimited data size (BER) unlimited # of attributes secure mailing lists signed receipts
PKCS #8 PrivateKeyInfo	encrypted and unencrypted with PBE and non-PBE cryptography	encrypted and unencrypted with PBE and non-PBE cryptography
PKCS #12 PFX	• unlimited certificates • unlimited private keys • unlimited # of attributes	• unlimited certificates • unlimited private keys • unlimited # of attributes
Cryptographic Providers	• Security Builder Crypto-C • Security Builder GSE	• Security Builder Crypto-J • JCE 1.2.2
Implementation Code Size	100 KB-400 KB	1.5 MB
Range Supported Platforms	QNX, Linux, Windows, MAC on various hardware architectures	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, devices, telematics modules, smart meters and enterprise servers around the world. For a sampling of some of the ways you can use 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