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, PDAs, cable modems, desktops, servers and any other networked electronic products. With optimized cryptographic libraries, FIPS-approved algorithms and a common API across multiple platforms, Security Builder PKI enables you to get to market quickly using proven security.

Security Builder PKI* provides 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.

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 X9.37 (Specifications for an Electronic Exchange of Check & Image Data) and ANSI X9.62 (The Elliptic Curve Digital Signature Algorithm).

FLEXIBLE

Security Builder PKI can be integrated on a wide range of devices and platforms—and supports a range of hardware or software cryptographic providers. Security Builder PKI can be used with Security Builder® GSE™, a FIPS 140-2 Validated cryptographic module, to meet government requirements. Function calls specifically designed for Check 21 support plug easily into Security Builder PKI to make it easy to support image verification requirements.

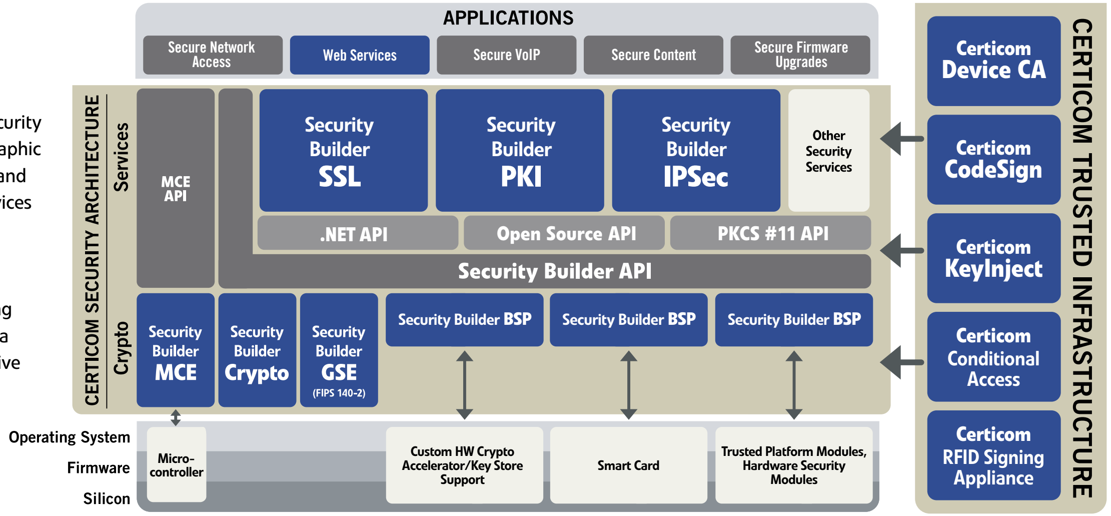
INTEROPERABLE

Security Builder PKI adheres to a wide range of industry standards including: ANSI, CableLabs DOCSIS BPI+, IETF PKIX, ISO, PKCS, and FIPS, allowing your product to interoperate with other PKI-enabled applications and all major commercial Certification Authorities. Quickly add support for protocols such as S/MIME v3 or EDIINT (AS1/AS2) to your applications.

INCREASED ROI

The same API across platforms means Security Builder PKI drops into your application easily with no porting required, cutting development costs and time-to-market. Used within the context of the Certicom Security Architecture*, this API provides a single, common interface between the protocols and cryptographic providers, further simplifying your development cycle.

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 PKI-C only

Features

	Security Builder PKI-C	Security Builder PKI-J
Programming Language	C	Java
Supported Hardware Accelerators/Hardware Tokens	Chrysalis-ITS Luna 2 and CA3 Eracom protectOrange PKCS #11/Cryptoki	Chrysalis-ITS Luna 2 and CA3 JCE compliant token
PKCS Compliant	# 1, 3, 5, 7, 8, 9, 10, 11, 12	# 1, 3, 5, 7, 8, 9, 10, 11, 12
X.509 Certificates	Versions 1, 2 and 3 supported character sets: • ASCII • Latin-1 • UTF-8 • UCS-2 supported key types: • ECC • DH • DSA • RSA	versions: 1, 2, and 3 supported character sets: • ASCII • BMP • IA5 • Printable • T61 • Visible • Latin-1 • UTF-8 • UCS-2 supported key types: • ECC • DH • DSA • RSA
X.509 CRLs	versions 1 and 2	versions 1 and 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 result
Certificate Requests	PKCS #10	PKCS #10, CRS, CMP
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-key 3DES with SHA-1 • 3-key 3DES 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	EnvelopedData (ECMQV, ECDH, DH, PKCS#1, …) SignedData (ECDSA, DSA, PKCS#1, …) EncryptedData (with PBE and non-PBE cryptography) unlimited data size (BER) unlimited # of attributes secure mailing lists signed receipts	EnvelopedData (ECMQV, ECDH, DH, PKCS#1, …) SignedData (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 • Cryptoki/PKCS#11*	• Security Builder Crypto-J • JCE 1.2.2 • Cryptoki/PKCS#11
IETF RFC compliant	PKIX: 3280, 3279, 2459 HMAC-MD5	PKIX: 3280, 3279, 2459 S/MIME:3852, 3565, 3370, 3369, 3278, 2634
Implementation Code Size Range	100 KB-400 KB	1.5 MB
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.

Need to know how to use the Certicom Security Architecture?
Security Builder PKI is part of the suite of Security Builder modules that are used by more than 300 customers for thousands of applications, including Telecommunication Systems, Sterling Commerce, Sybase, Terayon and Unisys. 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

A Subsidiary of Research In Motion Limited RIM®