



certicom

BLACKBERRY
SUBSIDIARY

NOT JUST SECURE...

BLACKBERRY SECURE

BLACKBERRY SECURE

There is a reason that BlackBerry is synonymous with mobile security. It is because security is as elemental to an electronic system as DNA is to an organism—and security is BlackBerry’s DNA.

Robust security cannot just be bolted on. It must be infused right from the start, which is why BlackBerry Security has been trusted by world leaders for over two decades and is the mobility partner of all G7 governments, 16 of the G20 governments, 10 out of 10 of the largest global banks and law firms, and the top five largest managed healthcare, investment services, and oil and gas companies. BlackBerry Security has earned more than 70 government certifications and approvals - greater than any other mobile vendor.

The iconic example of the depth of trust in BlackBerry Security is probably the NSA’s licensing (and standardizing) of Certicom’s Elliptic Curve Cryptography (ECC) algorithms, which are quickly becoming the accepted crypto standard for enterprise, government, automotive, mobile, medical, industrial, and IoT security.

Vulnerabilities are growing rapidly and present a serious risk for public and private sector organizations, so BlackBerry continues to expand its coverage with advanced technologies, tools, design consulting, and testing services for true end-to-end, layered security. The goal is simple: to ensure there

are no back doors, open windows, or lost keys to exploit—anywhere in the system.

In mobile, coverage begins at the crucial hardware root of trust. OS and software authenticity is securely verified every single time any BlackBerry device in the world boots up. Data is encrypted right on the devices, in the trusted network, and behind the corporate firewall. In operating systems, the BlackBerry-QNX Nutrino microkernel ensures safe, secure, and reliable operation robust enough for over 40 car models, the space shuttle, and nuclear plants. It is designed to fail safe, and protect against malware, tampering and data leakage. Thanks to Certicom’s Security Builder Software Libraries, certificate management solutions, and secure manufacturing systems, it is easy to obtain government approved (FIPS 140-2 Level 1) validation, manage security certificates, and secure manufacturing lines without becoming a crypto expert.

*CONFIDENTIALITY. INTEGRITY.
AUTHENTICITY.*

World leaders in government and industry trust BlackBerry Security to help run their secure communications, networks, in-car systems, nuclear infrastructure, and other mission critical functions.

Learn what they have already discovered.

CERTICOM CRYPTO

Certicom technology is at the heart of modern security

Certicom is the crypto solutions specialist in BlackBerry Technology Solutions, a global technology innovator dedicated to bringing battle-hardened safety, security, and reliability to embedded systems worldwide (and in outer space).

Certicom is a recognized leader in public key infrastructure (PKI) security design, innovation, and delivery. PKI is a foundational technology that has become the cornerstone of real world security across the internet, mobile, medical, financial, government, military, consumer, automotive, industrial, IoT, and just about every application that communicates information electronically.

Public Key Cryptography uses public-private cryptographic key pairs to sign digital certificates and provide the essential elements of security, which are confidentiality, data integrity, authentication, and non-repudiation. PKI establishes the infrastructure that defines how digital certificates are created, distributed, stored, and revoked.

Public Key Cryptography matters. It is not at all an overstatement to characterize Public Key Cryptography as having established the main way that security is provided throughout today's (and tomorrow's) connected world. In fact, anyone who has ever logged on to a secure web site such as e-commerce or e-banking has used Public Key crypto, most

likely without even knowing it. It is already built into personal computers and smart phones, and it won't be long before it is built into every embedded application as well. And, that is a very important notion to grasp.

Certicom means security. Proven PKI solutions from world leading software and security infrastructure suppliers like Certicom increase device (e.g. semiconductor chip and board) security, fight counterfeiting and cloning of products and firmware, promote product and personal identity authentication, secure asset management in supply chains, and improve the security of numerous other applications, including the emerging Internet of things ("IoT").

Public Key crypto's tremendous growth is being increasingly driven by two powerful forces: 1) the widespread adoption of autonomous communicating devices (including IoT) across many applications segments, and 2) the realization that such devices absolutely must be authenticated (as noted by Dr. Vint Cerf, who is credited as a founder of the Internet). In addition to authentication, the other critical components of security are needed for true security; namely, confidentiality, data integrity, and non-repudiation.

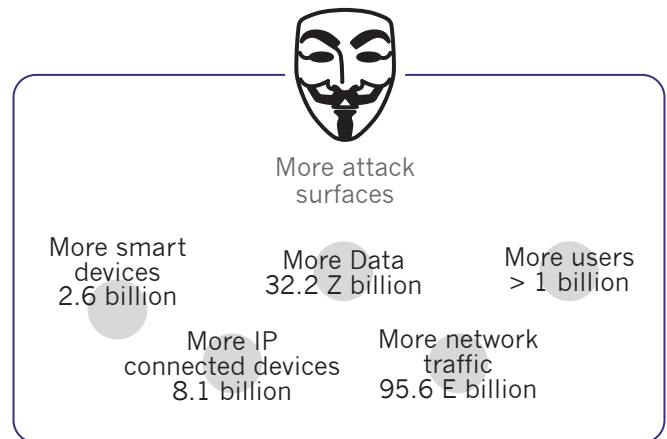
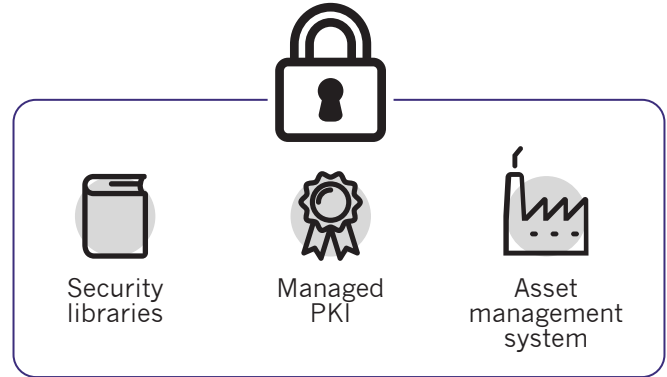
More things connecting translates directly into more targets, so security from end-to-end is becoming mandatory. In fact, vulnerability increases faster than the increase in the number of nodes. (This is a corollary to Metcalf's Law of the power of a network growing at the 4th power of the number of nodes.)

SECURITY MATTERS

Security matters to everyone because everything that connects is vulnerable.

Because Certicom solutions are resource optimized, certified, and practical it is easy to obtain world class, security and protect manufacturing supply chains to enhance revenue, profit, and protect brand equity.

Certicom's 3 products families of government validated crypto libraries, PKI certificate solutions, and asset management systems make "things" not just secure, but BlackBerry secure, without having to become a crypto expert.

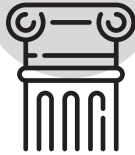


IF IT CONNECTS...CERTICOM PROTECTS

THE 3 PILLARS OF SECURITY

Certicom's crypto solutions address the three foundational pillars of security:

Confidentiality



This is ensuring that no one can read the message except the intended receiver. This is typically accomplished with encryption and decryption which hides the message from all parties except the sender and receiver. A secret cryptographic key (that is the same) is input to the encryption and decryption algorithm on each side.

Integrity



Also called data integrity, integrity is assuring that the received message was not altered. This is done using cryptographic functions such as hashing and sign-verify.

Authenticity



Ensuring that the sender of a message is who they say they are or are “real” is the simple meaning of authenticity. Certicom invented many of the modern and fundamental algorithms used in PKI to provide authentication across all applications.

Sometimes people add non-repudiation to the list of pillars which is preventing the sender from later denying that they sent the message in the first place.

SECURITY LIBRARIES

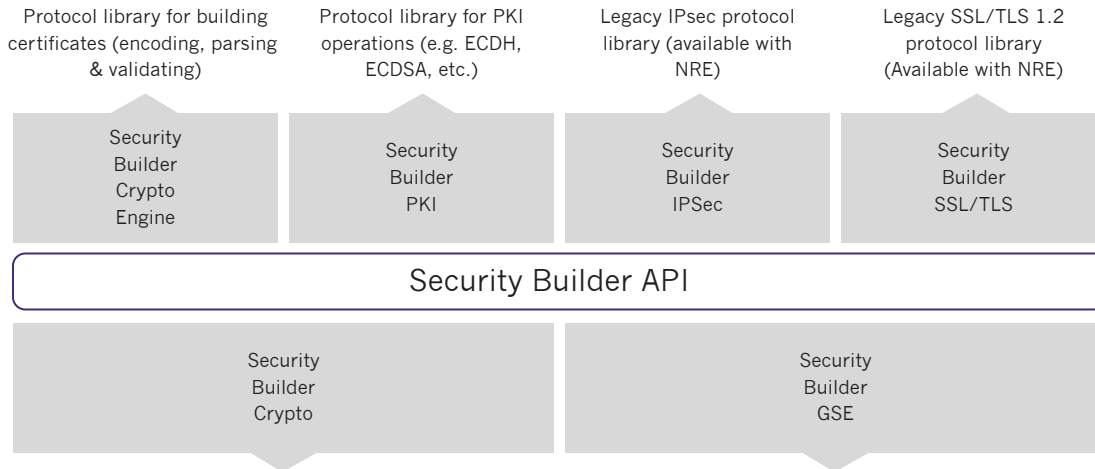


Cross platform, certified crypto algorithms for highest security applications

Certicom’s Security Builder C and Java software libraries, tool kits, and SDKs make it easy for system designers to implement proven and hardened security, for a wide range of platforms. The libraries are battle hardened and tested to the most stringent cryptographic standards.

The Government Security Edition (Security Builder GSE) is a validated version that allows designers to build client and server side applications requiring FIPS 140-2 level 1 validation without the need to make a submission to the FIPS approval process. (FIPS 140-3 is coming soon.) This shortens time to market and ensures the highest levels of security.

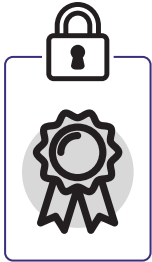
The Certicom security libraries are noted in the architecture diagram.



- Multi-algorithm libraries
- Proven in mobile, enterprise, embedded, & automotive applications
- Provides license to Certicom ECC technology

- Security Builder Crypto with FIPS 140-2 Level 1 Validation
- Ideal for government and best practices applications
- Optimized for MMU based processors (e.g. ARM Cortex M4 and higher)
- ECC license





MANAGED PKI SERVICES



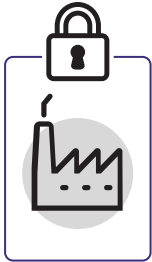
Certificate management for telematics, mobile devices, industrial networks & anything else that connects

Certicom's Managed PKI Certificate Services helps high volume manufacturers secure devices and securely enforce ecosystem requirements. Authentication is enforced via certificates, which is a method that provides the highest levels of security. Certicom's managed PKI system was initially created for BlackBerry mobile devices, which speaks to the high security and volume production scale credentials and capabilities. **IT IS SIMPLE, SECURE AND SCALABLE.**

Managed PKI performs four essential functions:

-  **ISSUE:** Automatically issue certificates to validated devices
-  **MANAGE:** Track all of the issued certificates
-  **RENEW:** Automatically renew active devices
-  **REVOKE:** Disable certificates of lost or decommissioned devices

ASSET MANAGEMENT SYSTEM



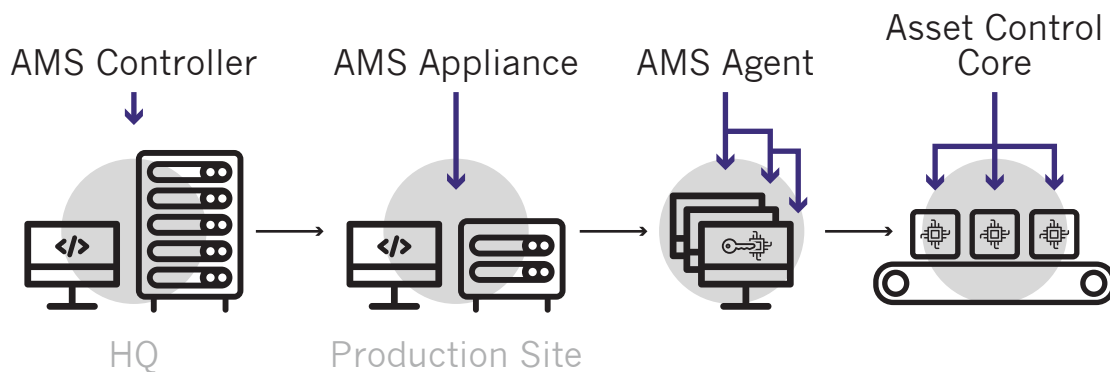
Secures manufacturing supply chain to prevent cloning and inject security keys

Certicom’s AMS Asset Management System installs cryptographic keys into customer devices (e.g. processors, memory, key storage ICs, etc.) that are used in a range of products and systems to ensure they are secure from tampering, counterfeiting, cloning, and other bad things that happen to good companies.

This process is also known in the industry as “personalization”, because each device receives a unique (i.e. personal) identity by means of an inserted cryptographic key that only that device will have.

Personalization using Certicom’s AMS solution automates the secure distribution and tracking of digital assets such as cryptographic keys and serial numbers.

A fundamental point in security is that secure crypto keys are absolutely necessary for robust security. Private or secret keys must stay secret starting from the time that they are created and injected into the device to their usage in the application. Serial numbers do not have to be secret, but assist in security and identity checking (authentication) and other cryptographic operations.



ECC: ELLIPTIC CURVE CRYPTOGRAPHY

When it comes to robust security, Certicom offers Elliptic Curve Cryptography (ECC) algorithms validated to government-grade FIPS 140-2 Level 1 which is required to sell into Veteran's Administration (VA) hospitals and other governmental establishments. Validated crypto software libraries make it easy to add cryptographic algorithms to systems without having to become a crypto expert, and are among the most advanced in the industry to provide confidentiality, data integrity, and authenticity at the highest levels. The quality of the solutions makes perfect sense since Certicom invented and holds patents for many of the most fundamental ECC technologies. In fact, the National Security Agency (NSA) licensed Certicom's patents in order to make ECC a powerful crypto standard.



BlackBerry and its subsidiaries, Certicom and QNX, provide products and services that make things not just secure, but BlackBerry Secure.

Certicom Corp., subsidiary of BlackBerry manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM, General Dynamics, and SAP. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada.

© 2016 Certicom Corp. All rights reserved. Certicom, Certicom Secure, KeyInject and Security Builder, are the trademarks or registered trademarks of Certicom Corp., the exclusive rights to which are expressly reserved. All other trademarks are the property of their respective owners
www.certicom.com

QNX Software Systems Limited, subsidiary of BlackBerry is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada.

© 2016 QNX Software Systems Limited, All rights reserved. BlackBerry, QNX, QNX CAR, Neutrino, Certicom, and related trademarks, names and logos are the property of BlackBerry Limited and are registered and/or used in the U.S. and countries around the world.
www.qnx.com