

# Security Builder<sup>®</sup> MCE<sup>™</sup>

## SOFTWARE CRYPTOGRAPHIC MODULE FOR MICROCONTROLLER DEVICES

**Security Builder<sup>®</sup> MCE<sup>™</sup> provides the cryptographic primitives required to create a trusted platform for microcontroller devices.** This enables wireless networks of devices that can be uniquely identified and allows data to be securely sent to and retrieved from all devices. In addition to symmetric encryption, Security Builder MCE allows you to integrate key exchange and digital signatures based on elliptic curve cryptography (ECC), the only public-key scheme capable of meeting the footprint and power limitations of these constrained devices.

Public-key-based operation distributes intelligence in the network, allowing devices to interact and communicate securely. This enables networks that are scalable, fluid and easily reconfigurable, setting the stage for an array of new and innovative applications, to drive sales of your microcontroller devices. Security Builder MCE allows you to differentiate your products for higher value applications where security is critical, and to drive the adoption of wireless microcontroller networks.

### HIGHER VALUE, HIGHER MARGINS

Secure devices are used in more-critical, higher value applications, and will therefore have a higher average selling price. This will create higher value in the chipsets and software stacks that compose the microcontroller device.

### COMPLETE SECURITY FOR THE ENTIRE DEVICE LIFECYCLE

Security Builder MCE is part of Certicom Security for Sensor Networks, a suite of products which enable developers of low power sensor devices to build secure, reliable operation into sensor networks from design and development through to manufacturing, deployment and upgrade. Certicom Security for Sensor Networks also includes the Certicom f(2m) ECC IP Core for the acceleration of ECC in low power devices, and Certicom Key Inject, which permits device vendors to pre-inject keys into devices to provide a root of trust.

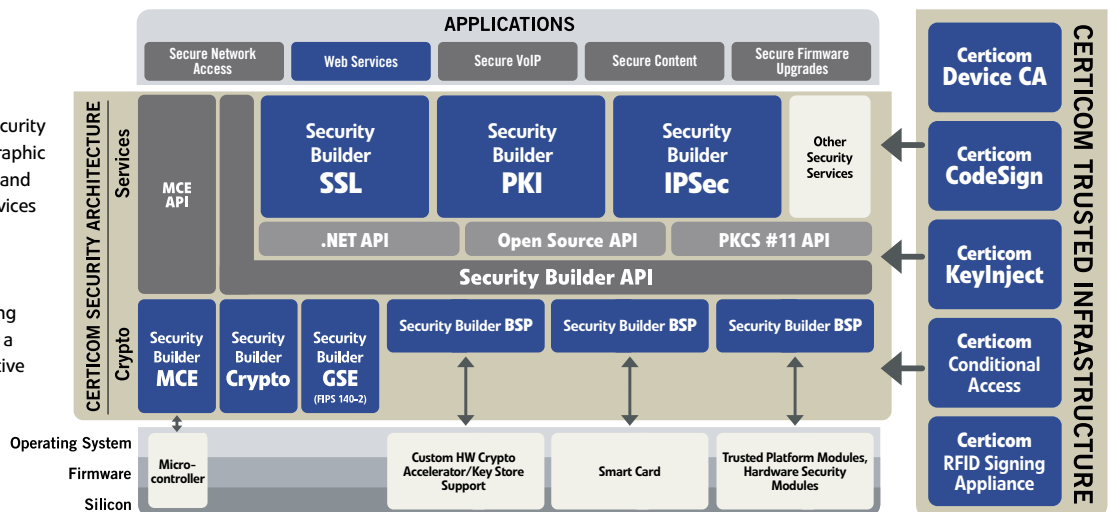
### SUPPORTS SCALABLE, AD-HOC MESH NETWORKING

With public-key, each device has its own unique set of keys, so there is no need for network key updates as the network changes. This allows for the automatic enrolment of devices to the network providing improved node mobility and flexible topologies that enable mesh networking and ad-hoc cluster formation that easily scales to a large number of devices.

### OPTIMIZED PERFORMANCE

Optimized for the power, processing and footprint constraints of a microcontroller device, Security Builder MCE delivers strong security without impacting device performance. ECC provides smaller key sizes with higher strength-per-bit than any other public-key cryptosystem, making it the only viable alternative for microcontroller devices. For even stronger performance, Security Builder MCE can be combined with the Certicom f(2<sup>m</sup>) ECC IP Core.

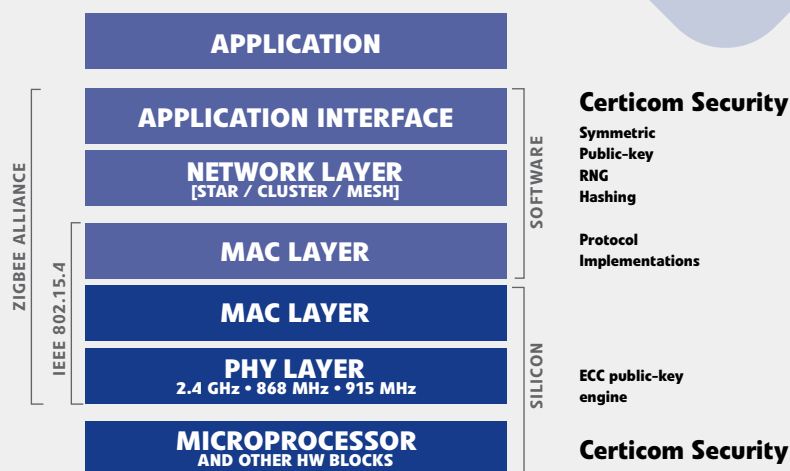
The Certicom Security Architecture is a comprehensive, portable and modular security platform that includes: software cryptographic providers that offer FIPS 140-2 Validation and meet NSA guidelines for ECC; security services like SSL, IPSec and PKI; hardware security cores and board support packages (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

<b>Programming Language</b>	C
<b>Symmetric Encryption</b>	AES
<b>Asymmetric Encryption</b>	ECC
<b>Key Agreement/Key Transport</b>	ECDH, ECMQV
<b>Digital Certificates</b>	ECQV
<b>Hash Functions</b>	MMO, SHA-1
<b>Implementation Code Size Range</b>	2K to 40K
<b>Supported Platforms</b>	Atmel AVR, other platforms under development

## Security Builder MCE Architecture



Security Builder MCE in addition to the Certicom f(2<sup>m</sup>) Hardware IP Core, allows you to quickly and cost-effectively build security into your microcontroller device.

### About Certicom

Founded in 1985 with a long-term focus on Elliptic Curve Cryptography, Certicom has been awarded over 500 patents. As a leader in applied cryptography and key management, Certicom provides managed PKI, key management and provisioning technology that helps to protect customers' device firmware, applications, and long-lived assets. Certicom is a critical element of the BlackBerry cybersecurity portfolio deploying the first and best in class end-to-end security solutions used in preventing product counterfeiting, re-manufacturing, and rogue network access. BlackBerry Certicom's secure key provisioning, code signing and identity management solutions are field-proven to protect next-generation connected cars, critical infrastructure and IoT deployments.

**Corporate Headquarters**  
 4701 Tahoe Blvd, Building A  
 Mississauga, ON L4W 0B4  
 Canada  
 Tel: 1.905.507.4220  
 Toll Free: 1.800.561.6100  
 (NA only)  
 info@certicom.com

 | certicom