

Certicom Security for ZigBee Smart Energy

COMPACT, EFFICIENT SECURITY FOR LOW POWER WIRELESS MESH NETWORKS

Certicom Security for ZigBee Smart Energy is a cross-platform cryptographic module which supports the Smart Energy application security profile for ZigBee devices. Elliptic Curve Cryptography (ECC) strength and efficiency provides an enhanced level of security to resource-constrained wireless mesh networks.

COMPACT, EFFICIENT SECURITY

Certicom's ZigBee implementations of ECDSA and ECMQV offer the same highly efficient digital signature and key agreement schemes selected by the NSA, with software optimized for performance as well as minimal code footprint.

Elliptic Curve Cryptography (ECC) based Qu-Vanstone "Implicit Certificates" bring strong security to the resource-constrained ZigBee environment without the overhead of bulky X.509 certificates. Implicit digital certificates allow metering companies to take advantage of mass-produced ZigBee Smart Metering devices with built-in cryptographic identities.

ECMQV and ECDSA can be utilized in variety of resource constrained applications which may benefit from mutual authentication yet resource constraints prohibit the use of ordinary PKI technology.

SMALLER AND FASTER

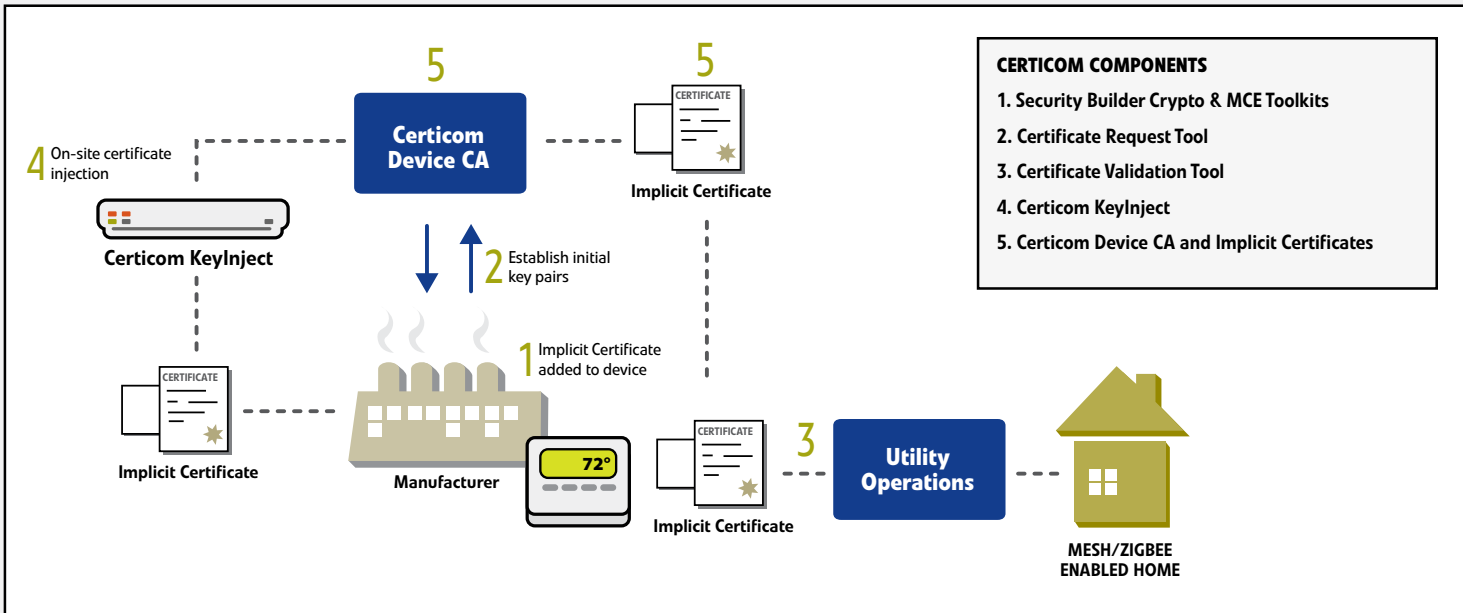
Optimized for constrained platforms, the ZigBee suite of algorithms can be implemented in as little code space as 10 K of ROM. Working with Certicom professional services implementations can be quickly tuned to support a wide variety of (RAM, ROM and stack) configurations. The ECC enabled implementations are ideal for residential and commercial energy management systems that are low bandwidth and require maximum battery life.

CERTICOM SOLUTION

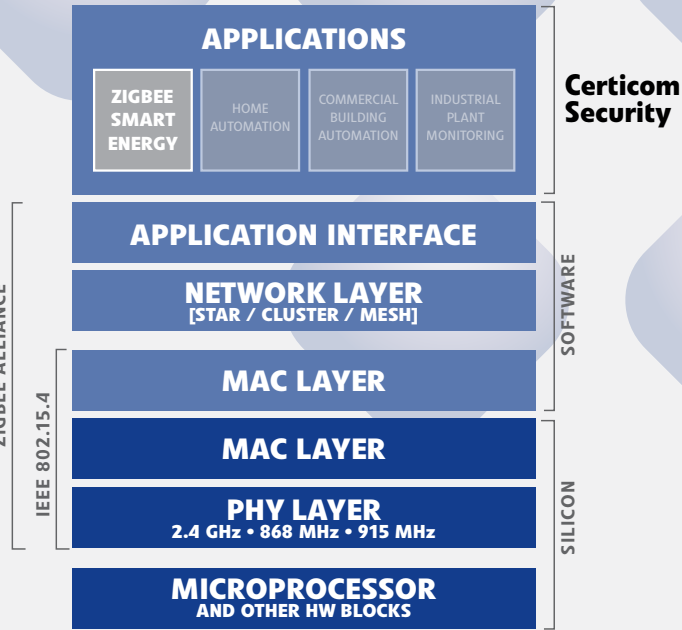
The solution to the key distribution problem for ad hoc wireless sensor networks is Public Key Infrastructure using Elliptic Curve Cryptography (ECC) based Implicit Certificates. Implicit Certificates bring strong security to the resource-constrained ZigBee environment. Requiring all devices to be authenticated with digital certificates allows metering companies to take advantage of mass-produced ZigBee Smart Metering devices with built-in strong cryptographic identities.



Features



| | |
|--------------------------------------|-----------------|
| Environment | 8 and 16-bit |
| Programming Language | C |
| Hash Functions | AES-MMO |
| Asymmetric Encryption | - |
| Key Agreement/ Key Transport | ECMQV |
| Digital Signatures | ECDSA |
| Implicit Certificate handling | ECQV |
| Implementations: | |
| Code Size Range | 10 – 20 K |
| Code Ram Usage | <1 K |
| Platform Support | 8051 |
| | Arm 7/ARM 9 |
| | EM250 and EM260 |
| | Linux x86 |
| | MSP 430 |
| | Windows x86 |
| | M16C |



Security Builder MCE for Zigbee Smart Energy

About Certicom

Certicom, a wholly owned subsidiary of BlackBerry Limited (Nasdaq: BBRy; TSX: BB), manages and protects the value of...
 "ø"ø" "p"pt øt øæÐ t t " tp"t ø "...ø ø_ t_ Ð" æ"..._ øt æ" t ø t Vø
 É" " " Vø t "æ t "æ"Ð V"t"pt ø"..._t ø " t ø " Æ øÐ "t" t "øt tp "æ p tp "É
 ø"ø "t"æ Ð" "ø"ø" pøÐ"J "t"t"o "ø"ø" "p" "É ptpø" _t ø " "t
 Ætø" "tpø" ø ø "Ð" "ø"_"p" øæ p øt"t "Ætø" "..."t"p" ø"øø" t ø



Corporate Headquarters
 4701 Tahoe Blvd., Building A
 Mississauga, ON L4W 0B5 Canada
 Tel: 1.905.507.4220
 Toll Free: 1.800.561.6100 (NA only)
 info@certicom.com