certicom™

Certicom Device Authentication Service for ZigBee Smart Energy

With energy costs continuing to rise and power utilities searching for ways to more efficiently use existing power plant infrastructure, utilities are deploying smart metering systems to get the most out of existing power generation infrastructure.

Metering companies are turning to ZigBee, an ad hoc wireless networking standard to enable low-cost mass market deployment. The standard itself is regulated by a group known as the ZigBee Alliance, with over 150 members worldwide. Each of these members has invested to drive a common, interoperable standard that trusted and reliable products and services can be based on.

Securely managing a network of smart metering devices is more complex than it first appears, and strong and efficient security is necessary to assure utility companies, meter manufactures and end customers that only trusted devices have access to the utility network.

The solution to the security problem 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 Energy devices with built-in strong cryptographic identities.

Certicom delivers a turnkey solution for generating batches of digital certificates and private keys, along with an easy-to-use interface with which to embed these certificates into devices as a seamlessly integrated part of your manufacturing process.

CERTICOM ENSURES AUTHENTIC, COMPLIANT AND INTEROPERABLE DEVICES

The Certicom Device Authentication Service for ZigBee Smart Energy provides a root of trust for all ZigBee Smart Energy devices. Authentic ZigBee Alliance certified products can be quickly and cost-effectively provisioned on the utility network because they have been tested and certified to be compliant with ZigBee Smart Energy standards. The service delivers out-of-the-box interoperability and security which lowers the total cost of ownership to utilities and metering companies while ensuring the integrity of the utility network.

CERTICOM IMPLICIT CERTIFICATES: STRONG SECURITY IN A SMALL PACKAGE

Certicom's Device Authentication Service for ZigBee Smart Energy is based on a scalable digital certificate architecture that leverages Implicit Certificates, a unique Certicom technology that allows authenticated key agreement in resource constrained environments such as low-cost 8-bit microcontrollers.

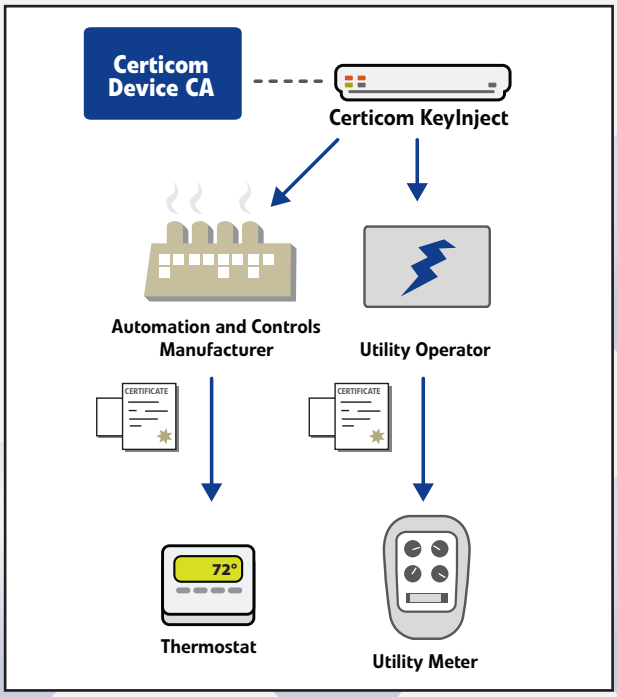
Keys and certificates are centrally generated and delivered securely in batches to mirror manufacturing runs.

How the Service Works

1. Begin by using a Certicom supplied application to identify network addresses, and other identifying information, that needs to be included in the certificates. The application will output a digitally signed request file.

2. Send the digitally signed request file to Certicom. All encryption and authentication is automatically handled by the application.

3. The Certicom managed ZigBee certificate service verifies the authenticity of the digitally signed request file and ensures that the unique data and addresses being requested have not been used before. Certicom then generates unique public and private key pairs, using dedicated bulk-generation hardware in their secure facility, and incorporates them along with Certicom's digital signature into certificates for every uniquely addressed device in your submitted address file.



4. Certicom inserts the certificates and their private keys into a certificate batch file and encrypts it for secure shipping back to the requesting customer. Only the application can decrypt the batch file.

5. Your administrator is notified by an email that your batch certificates are ready for delivery.

6. Using the Certicom application software, the batch file is downloaded and decrypted. The certificates and private keys are now available to your manufacturing systems for injection into devices on the factory line.

About Certicom

Certicom, a wholly owned subsidiary of BlackBerry Limited (Nasdaq: BBRY; TSX: BB), manages and protects the value of ɪzɪA±ɪA" "ÁÁŴGɪ"AĜzɪq "ɪ| |±0Ĝɪ±q ӄĜAĊ ôz0±ìɪđ±ɪA¸ "ÁÁìz0± q±ɪɔìĜAj¸ °ŴŴGÁAĜɪ kɔì0± kìjÁAzôì"ÁĊj ˛°kk: Áìz0Ĝ|±q AĊ± đzqA q±ɪɔìĜAj Á±ì bĜA zí "ɪj Ŧɪzӄɪ Áɔbŵɪ¸ Ŧ±j qɪĊ±đ±¸ !q AĊ± ôŴzb"Ŵ Ŵ±"|±ì Ĝɪ °kk" k±ìAĜɪzđ˜q q±ɪɔìĜAj zíí±ìĜɪôq "ì± ɪɔ˜ì±ɪAŴj ŴGɪ±ɪq±| Az Ċɔɪ|ì±|q zí đɔŴAĜɪ"AĜzɪ"Ŵ A±ɪĊɪzŴzôj ɪzđÁ"ɪĜ±q" ĜɪIŴɔ|ĜɪôěaƋ" ó±ɪ±ì"Ŵ {jɪ"đĜɪq" ɳ!ṅ "ɪ| ƵɪɲA"ì¸ ìzɔɪ|±| Ĝɪ¸¸¸¸" k±ìAĜɪzđ˜q ɪzìÁzì"A± zííĜɪ± Ĝq Ŵzɪ"A±| Ĝɪ Ƌqqqq"ɔô"" ƵɪA"ìĜz" k"ɪ|" ӄĜAĊ ӄzìŴ|ӄĝ|± q"Ŵ±q zííĜɪ±q Ĝɪ ɓɲ!" °ɔìzÁ± "ɪ| !q$"¸ CĜqĜA ӄӄӄ¸ɪ±ìAĜɪzđ¸ɪzđ¸

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

A Subsidiary of BlackBerry