

Certicom AMI 7000 Series

SECURITY APPLIANCES FOR ADVANCED METERING INFRASTRUCTURE

THE NEED FOR SECURITY

Advanced Metering Infrastructure's (AMI) openness and two-way communication capabilities add new risks to what has traditionally been an isolated distribution system. As smart energy homes with demand response capabilities and smart grid infrastructure are deployed, hundreds of millions of devices will be connected in one way or another to utility networks and the public Internet. Information about energy consumption will flow out of homes and offices, remote command and control signals will flow in.

Given the two way command and control connectivity to every customer enabled by AMI, the utility must consider NERC Critical Infrastructure Protection (CIP) requirements when automating their distribution networks.

Certicom Advanced Metering Infrastructure solution was designed to meet these stringent security requirements. A highly scalable turnkey security platform, the AMI 7000 Series secures communications between utility meters and utility companies' back end meter data management infrastructure by providing data encryption and integrity validation of individual metering data as well as strong authentication of metering commands.

Certicom AMI 7100 Signing and Encryption Appliance

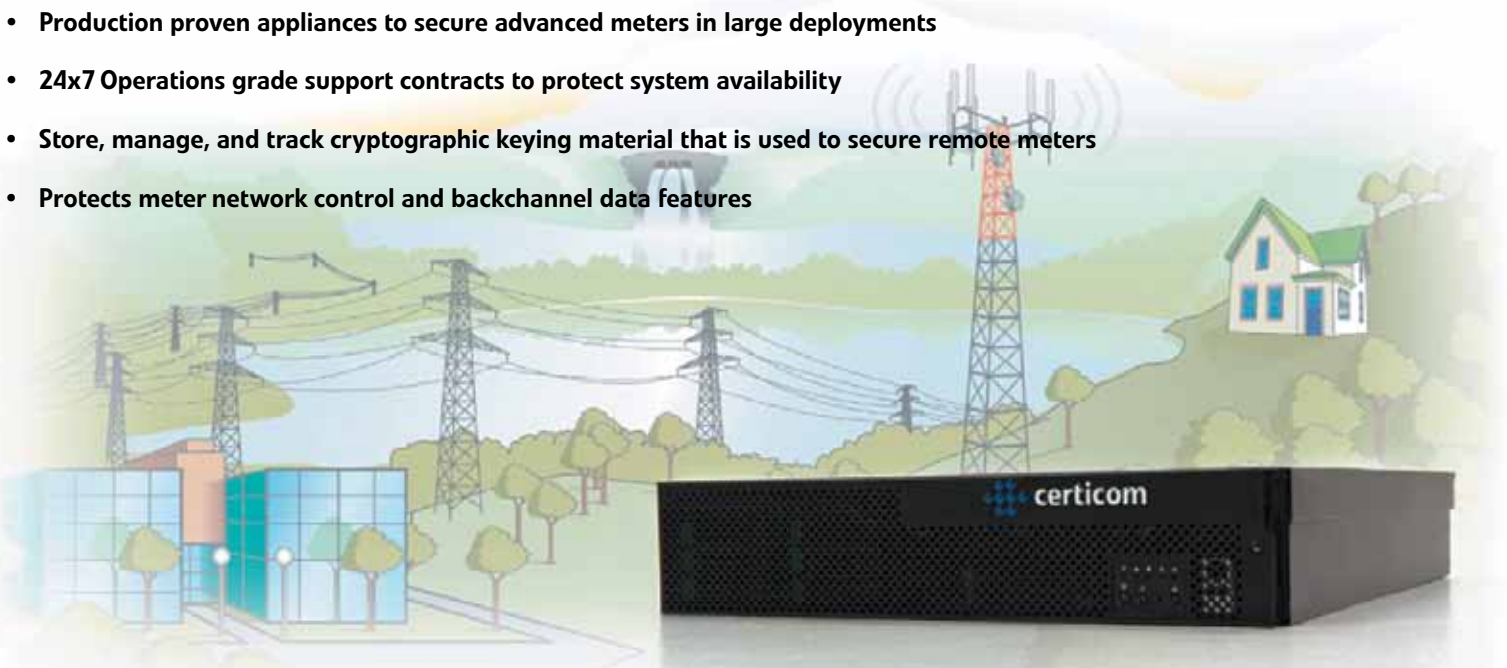
The Certicom AMI 7100 encrypts and digitally signs all command and control messages sent to the meters, using advanced Elliptic Curve Cryptography, the public key algorithm selected National Security Agency (NSA) for next generation cryptography. The AMI 7100 is a complete signing and encryption appliance that includes hardware, software and product support that will enable you to rapidly deploy an industry recognized; standards based security solution for advanced utility metering.

Certicom AMI 7200 Key Management Appliance

The Certicom AMI 7200 provides system wide security key management and decrypts all messages received from the meters, using the advanced encryption standard algorithm to protect sensitive data with bits of cipher security. The AMI 7200 is a specialized key management appliance that is specifically designed to store and manage cryptographic keys for meters and allows you to quickly deploy a root of trust using an industry recognized, security standards based turn-key solution.

BENEFITS

- Production proven appliances to secure advanced meters in large deployments
- 24x7 Operations grade support contracts to protect system availability
- Store, manage, and track cryptographic keying material that is used to secure remote meters
- Protects meter network control and backchannel data features



Features

General

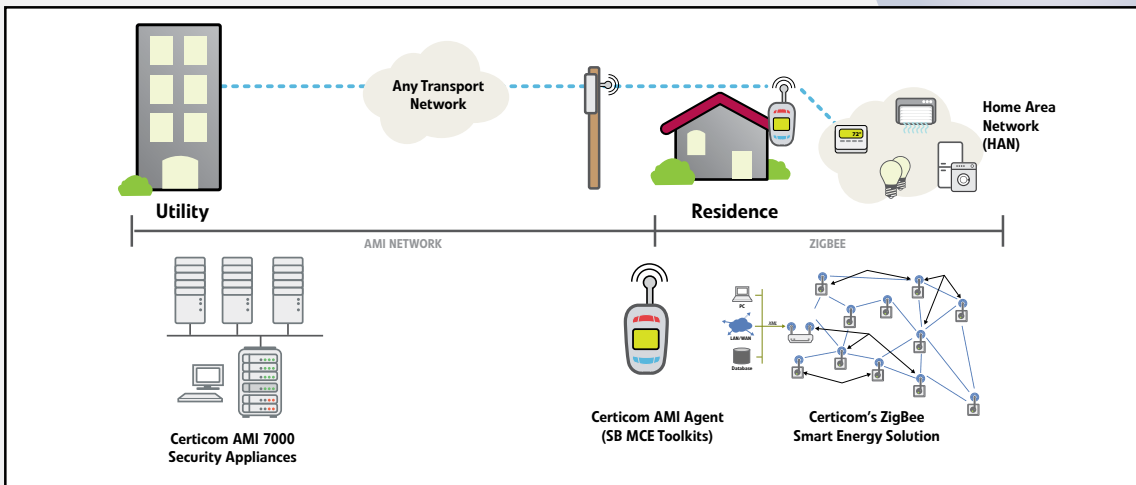
- Mitigates personnel risks with multi-administrative smart-card control of appliances
- Prevents eavesdropping and malicious infiltration of metering network
- Prevents false commands and replay attacks
- Ensures meter network availability with optional hot and warm standby redundancy configurations
- Add-on protected communications pathway into home via ZigBee Smart Energy devices

AMI 7200

- System wide key management with capabilities to perform key rollover and meter revocation
- Decrypts all transmitted meter reading data
- 20,000 decrypt operations per second using AES-128 cipher suite

AMI 7100

- Authenticates command and control messages using ECDSA based digital signatures
- Protect private signing keys using tamper-reactive Hardware Security Module (HSM)
- 200 digital signatures per second using 283 bit ECC security level



SPECIFICATIONS

Cryptographic Key Strength

- 128-bit or 256-bit effective cryptographic strength utilizing US government grade algorithms
- ECC (asymmetric), AES (Symmetric)

Processor

- Intel 45 nm Enhanced Quad Core Xeon CPU 5400 (AMI 7100)
- 2 x Intel 4 nm Enhanced Quad Xeon CPUs (AMI 7200)

Network Interfaces

- 2 x 10/100/1000Mb On-Board Interfaces

Raid Storage

- 3 x 146 Gb SAS 2.5" Hot Swap HDDs Hardware RAID 5 (AMI 7100)
- 5 x 146 Gb SAS 2.5" Hot Swap HDDs (AMI 7200)
- 2 x 2 HDDs RAID 1 Configuration (AMI 7200)
- 1 HDD Hot Spare (AMI 7200)

System Administration

- Secure Shell (SSH) Console Administration with Operator Smart Cards

Hardware Security

- FIPS 140 Level 3 rated Hardware Security Module (AMS 7100)

Enclosure

- 2 U rack mountable (20 " depth))

Power Supplies:

- 600 W AC Auto-ranging (Optional DC)
- Optional 2nd Dual Hot Swap Power Supply

Operating Environment:

- Temperature – Operating 10°C to 35°C (50°F to 95°F)
- Temperature – Non-Operating -40°C to 70°C (-41°F to 158°F)
- Humidity – Non-operating 50% to 90%, non-condensing with a maximum wet bulb of 28°C

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, Europe and Asia. Visit www.certicom.com.



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