Certicom's **Advanced Metering Infrastructure (AMI)** series 7000 appliances are a turn-key system that improves operational security with flexible solutions. The 7000 series provides a secure layer between the utility head-end and the meter via high-speed encryption and key management.

Certicom is the world leader in **elliptic curve cryptography (ECC)** selected by NSA to secure classified government communications as it provides the highest security per bit. This allows the AMI 7000 series to provide un-paralled security with minimum network overhead. Such security is critical when deploying millions of meters which are two-way capable and can send meter data to the utility as well as receive other commands from the utility.

**Improve operational security with robust and flexible solutions for utilities.**

Certicom’s **Advanced Metering Infrastructure (AMI)** series 7000 appliances are a turn-key system that improves operational security with flexible solutions. The 7000 series provides a secure layer between the utility head-end and the meter via high-speed encryption and key management.

Certicom is the world leader in **elliptic curve cryptography (ECC)** selected by NSA to secure classified government communications as it provides the highest security per bit. This allows the AMI 7000 series to provide un-paralled security with minimum network overhead. Such security is critical when deploying millions of meters which are two-way capable and can send meter data to the utility as well as receive other commands from the utility.

**Revolutionizing AMI Security**

**Improve security.**
- Prevent false commands and replay attacks triggering load shed.
- Prevent counterfeit meters and devices from utilizing the network.
- Prevent eavesdropping and malicious infiltration of metering network.
- Comply with ANSI C12.22 and NERC/FERC Critical Infrastructure Protection (CIP) requirements.
- Deploy millions of devices with a future proof technology, suitable for an in-service life of 20-30 years.

> “Certicom’s infrastructure offers unparalleled network and metering system security, further enhancing our energy management and measurement technologies as we work toward development of the Smart Grid”.
> Ross Vanos, VP Marketing at Itron

**Improve costs.**
- Outsource manufacturing and installation of meters.
- Broadcast commands to individual meters, groups of meters, or all meters.
- Reduce cost and risk at the utility head-end in terms of operating and backing up systems. Also, eases outsourcing such systems to third parties.
- Eliminate risk of system wide key exposure and need to store a symmetric key for every meter at the head-end.

> “Remember the days when meters were in people’s basements and in some cases, customers would provide utilities a copy with a key to their front door, in which case, utilities had to store the keys in a vault and put in place strict controls and procedures to ensure the sanctity of the key. Storing a distribution of symmetric keys is very analogous”.
> Industry Executive

A turnkey solution consisting of secure, scalable and production hardened appliances for the head-end and lightweight software agent for the meter.

**Network**
- Multi-protocol support
  - TCP/IP
- Multi-topology support
  - Hub and spoke
  - Mesh
- Multi-transport layer support
  - Ad-hoc wireless
  - Powerline
  - Cellular

*MDMS* 7000

*MDMS* 7000

*Utility Head-end*

*Network*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*

*MDMS* 7000

*Utility Head-end*
**Why ECC?**
- ECC offers highest security per bit of any PKI system
- At NIST recommended security levels RSA keys are 9X to 12X larger than ECC keys of equivalent strength (e.g. 256 bit ECC vs. 3072 bit RSA)
- ECC binary curves at 283 bits are deemed secure until 2030

**Proven**
- ECC deployed on over 50 million handheld devices
- AMI 7000 deployed at a number of utilities including SDG&E and SCE
- ECC is the only public key cryptosystem endorsed by the US government for use past 2010

**Lightweight**
- Minimal impact on network bandwidth and overhead as ECC provides the highest security per bit, a lightweight infrastructure:
  - At the home, the meter agent, is small and lightweight, ideal for low-power microprocessors. As a reference point, ECC is part of the ZigBee Smart Energy profile, which runs on even smaller, lower-power, battery operated devices
  - At the utility head-end, a single rack of equipment can support millions of meters

---

**Advanced Meter Infrastructure 7000**

**Key Management: Symmetric Key**

**Case 1: Same key for each meter**
- Meter
  - Symmetric key 1
  - Symmetric key 1
- Utility Head-end
  - Symmetric key 1

**Case 2: Different key for each meter**
- Meter
  - Symmetric key 1
- Utility Head-end
  - Symmetric key 1

**Check list**
- non-repudiation
- high security posture
- outsourc flexibility
- operational flexibility
- mitigate risk

---

**Advantages of ECC vs. Public Key Infrastructure (PKI)**
- PKI enables secure key agreement schemes to establish pairwise shared secrets suitable for symmetric cryptography
  - Keys are generated in pairs; a “private” key and a corresponding “public” key
- The private key is only known to one entity which uses it to:
  - Sign messages that can be verified by any entity using the corresponding public key
- All messages from the utility head-end are signed using its private key (to which only it has access). These digital signatures, used with utility’s public key provide receiving meters:
  - Authentication - message as coming from utility
  - Data-integrity - high assurance the message hasn’t been modified
  - Non-repudiation - meters have ability to demonstrate it acted appropriately on a utility sent message
- Utility head-end can send signed messages not only to individual meters, but, to groups of meters, or, even all meters
- Authenticated meter enrollment with secure over the air (OTA) key provisioning and updates
- PKI is widely used in a number of applications including internet web browsers (SSL/TLS)
- Strong technical controls at the meter head-end:
  - Critical system keys protected by hardened security appliances
  - Strong two-factor authentication and logging to protect system access

---

**Why PKI?**

**Check list**
- non-repudiation
- high security posture
- outsourc flexibility
- operational flexibility
- mitigate risk

---

**BlackBerry certicom**

www.certicom.com

North America: 1.800.561.6100
International: 1.905.507.4220 E-mail: info@certicom.com