Itron Secures Metering Systems with Certicom AMI Solution

A CERTICOM CUSTOMER USE CASE

AUGUST 2010

Executive summary

The transition to Advanced Metering Infrastructure (AMI) and implementation of mass market Demand Response programs requires an end-to-end security solution to safeguard consumer privacy and protect the stability of the grid for the next 30 years. To meet utility and regulatory requirements in a fast and cost-effective manner, metering companies are looking for help.

Certicom is a vendor of choice for metering companies, due to the combination of expertise in secure distributed communications systems along with available commercially proven components in AMI. Certicom AMI solution was a natural fit to Itron needs, to enhance its security position on all aspects of communications between the meter and head-end systems (refer to *Figure 1*).

"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."

Russ Vanos,
Itron Vice President of Marketing

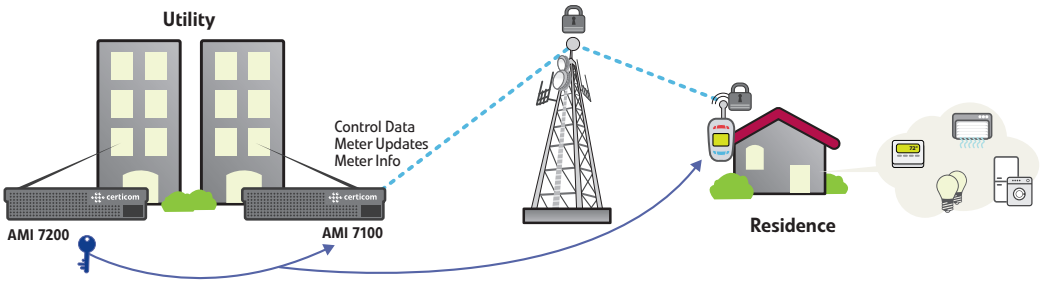


Figure 1: Certicom AMI Solution

Certicom AMI product family of hardened encryption and key management appliances were integrated into Itron OpenWay solution, securing end-to-end network messages from the OpenWay Collection Engine down to the OpenWay CENTRON® meter. The appliances were responsible for signing and encryption of command messages that the collection engine will deliver to meters, and decryption of data retrieved from meters, as well as managing the state of the keys used within the management system.

The security architecture inherent to Itron OpenWay combined with Certicom signing and encryption appliances not only address the two-way command and control needs for AMI and Smart Grid network platforms, but also provide strong integrity of control, non repudiation, availability and confidentiality of data to utility customers and their end users.

Introduction

The utility market is evolving to become much more interactive by incorporating fine-grained, real-time data collection, and real-time management of customer devices (air conditioning, pool pumps, etc). AMI produces cost savings for utilities due to reduction in labour costs and increased meter reading accuracy, making it easier for utilities to provide customers with billing data. Demand Response program involves the broadcast of pricing signals to persuade customers in response to market prices, to reduce demand, thereby reducing the peak demand for electricity during critical time periods.

Itron is a leading technology provider to the global energy and water industries, providing metering and management systems to utility companies. OpenWay by Itron is a new-generation, open-architecture advanced metering solution that provides full two-way communication to enable a smart utility grid as well as a built-in communications pathway to the meter or other smart grid device that is fully compliant with the ANSI C12.22 protocol for transport of device data over a network (refer to *Figure 2*). Itron OpenWay promises not only operational efficiency, but also empowers all customers to participate in energy management and conservation.

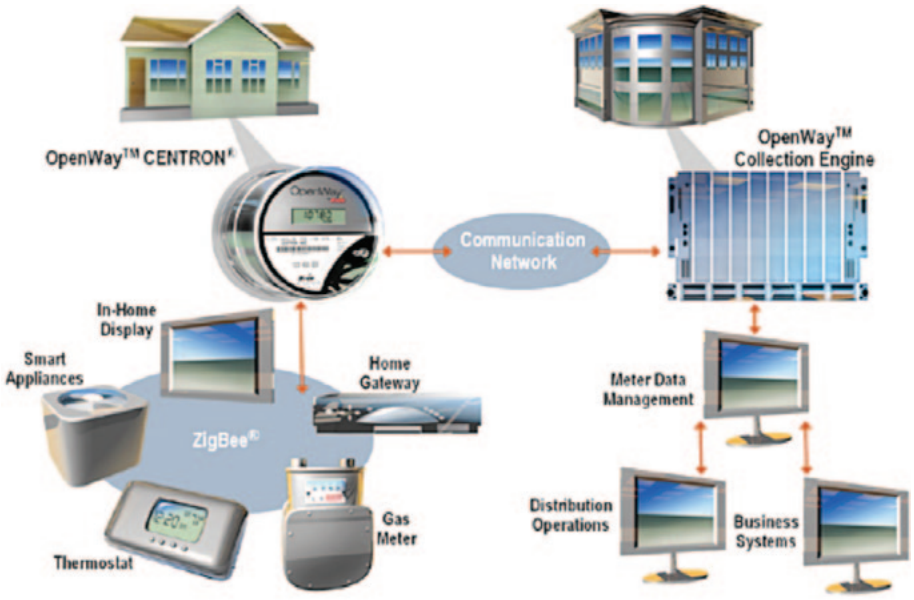


Figure 2: ITRON OpenWay CENTRON

Itron Business Challenge

There are numerous assets to be protected, number of threats to consider and several basic threat vectors that every meter device should guard against. Among the assets in meters and thermostats are the image code, core firmware, encryption and authentication keys, access controls and authorization codes. Keys and authorization codes themselves protect remote disconnect logic, service logic, billing data, and usage history. Thus, special attention should be paid to protecting these assets from unauthorized access and tampering. If compromised, the assets, encryption and authentication keys, sensitive command and control data can be used to turn off or overload a wide service area with critical ramifications on public safety.

Itron was planning to increase its security position on all aspects of communications between the meter and head-end systems, with a focus on privacy and authenticity. It envisioned a solution that will enable high speed signing of data, while maintaining a high security posture. Due to time to market and cost considerations, Itron had near term operational requirements and wished to take advantage of off-the-shelf components Certicom could tailor in a short time, and at a lower cost than building from scratch.

Certicom AMI solutions was presented to Itron, since it can secure these assets and help create a smart grid that is able, in a secure fashion, to dynamically adjust to system demands, isolate circuit faults, predict component failures, and route power efficiently from a growing number of more energy efficient generation resources. Hence, by securing the pipeline between the meter and head-end using Certicom AMI appliances, the integrity of metering data is protected; system commands are authenticated, confidentiality is protected through encryption of metering data, and non-repudiation by system acknowledgements.

Certicom AMI Solution

Certicom professional services assigned a team of security consultants to meet with Itron engineering team, understand Itron business requirements, review the technical requirements and specification, and recommend a customized AMI platform tailored for Itron OpenWay, and capitalizing on Certicom suite of AMI security solutions based on Elliptic curve cryptography (ECC).

Certicom designed a hardened hardware platform (refer to figure 3) that meets the most stringent Critical Infrastructure Protection (CIP) requirements for AMI equipment and can support large-scale deployments where security performance and robustness are critical. This includes the management of critical system keys and strong authentication of demand response events using efficient cryptographic mechanisms.

As part of Certicom AMI network security solution, the AMI 7000 series of hardened appliances were introduced to Itron, as encryption and key management platforms that support intrusion and tamper

detection; protect keying material and provisioning of new devices. The AMI 7000 series of appliances offer key benefits such as:

- Enables high speed signing of data, while maintaining a high security posture. It provides strongly authenticated command and control that prevent replay attacks and fake commands with ECDSA. It is capable of 200 signatures/second for large-scale deployments.
- Sensitive keys are stored in hardware security modules (PCI Hardware crypto card inside the 7000 series appliance) with policies and procedures for enrolling and authorizing system operators. The HSM applies safeguards to establish who has access to which keys and what parts of the system.
- Provides High-speed decryption offload & validation of meter data with Avg. 20,000 encrypt/decrypt operations per second and 128-bit AES security that ensures system longevity.

Other features include:

- Designed to adhere to NSA suite B requirements
- Uses FIPS 197 approved encryption algorithms.
- Uses FIPS 186-2 approved signature algorithms.
- Uses FIPS 180-2 approved hashing algorithms.
- Provides digital signatures for strong message authentication.
- Provides key management and key rollover events.

The AMI 7000 series appliances consisted of two key product offerings that were presented to Itron:

- AMI 7100 Signing Encryption Server (SES)
- Decryption key update server (DKUS)

Figure 3: Certicom AMI 7000 Series Appliance

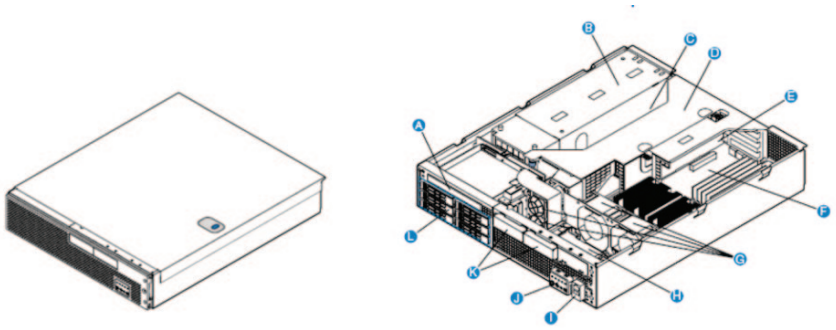
Refer to *Figure 4* for a high level overview of the appliances. They are high-density, rack mount server systems that support high availability features such as hot swappable SAS disk drives, redundant hot-swappable power supply modules and memory mirroring.

AMI 7100 Signing and Encryption Server (SES)

The Signing and Encryption Server is responsible for the signing and encryption of command messages that the collection engine will deliver to meters. Each SES is installed with a HSM (Hardware security module). It is a tamper protected PCI hardware card that has FIPS 140-2 level 3 validated. The HSM provide high performance secure cryptographic processing in server systems and supports applications that require high-performance symmetric and asymmetric cryptographic operations.

AMI 7200 Decryption and Key Update Server (DKUS)

The Decryption and Key Update Server is responsible for decrypting data retrieved from meters, as well as managing the state of the keys used within the system. It's capable of maintaining databases of meter IDs and associated metadata (AES Keys, random challenge, meter ECC public key) as well as the security state of a set of electric power meters.



Item	Description	Item	Description
A	Optical drive (optional)	G	System fans
B	Power supply cage (contains one power supply module with provision for an optional second module)	H	SAS Front Panel (SFP) board; can include optional SysCon board (which provides local memory storage)
C	Provision for PCI-X* and PCI Express* (PCIe*) full-height and full-length add-in cards	I	RJ45 COM2 and USB port 2 connectors
D	Riser card assembly (containing riser cards for both full-height and low-profile add-in cards)	J	Control panel and status indicators
E	Provision for two PCI Express low-profile add-in cards	K	Two slots for 4x GbE NIC ports (optional)
F	Intel® Server Board T5000PAL	L	Hot-swappable SAS disk drives (up to six)

Figure 4: Certicom AMI 7100 and 7200 Hardware Platform

Deployment & Implementation

Meter reading is an important business activity for utilities, and hence deployment of enterprise systems with a high level of redundancy is desired. As a result, the security SES and DKUS appliances were shipped to Itron and in turn to its utility customers. They were deployed in a redundant fashion, since equipment failure can lead to performance penalties from regulators and dissatisfaction from consumers. A standard production deployment to each site is included with redundant SES and DKUS appliances.

Furthermore, Certicom AMI solution was integrated into the OpenWay Collection Engine, leveraging its open-standards and solid two-way communications capability. The interval data collection and mass market demand response functionality of OpenWay and OpenWay-compatible meters were secured by Certicom's meter security agent. The agent provides a protected communications pathway into the home via ZigBee Smart Energy devices, and back to the headend via the American National Standards Institute (ANSI) C12.22 meter data management protocol. The Agent uses AES-128 equivalent strength encryption to secure all sensitive data and keying material.

24x7 Operations Support and Maintenance Agreements

Certicom recognizes the critical nature of smart grid and advanced metering operations and offers the expected service level agreements (SLA) that are essential for supporting leading technology providers to the global energy and water industries. Expert, in-house support staff operates our critical severity response hot line and work closely with escalation engineers in North America and the Asia Pacific region. Certicom is proactive in keeping customers on an upgrade path that is consistent with future releases and ongoing product roadmap.

Summary

Certicom AMI Solution can enable new and existing customers such as Itron to provide demand response and smart metering solutions, products and services in a secure fashion. Customers that select Certicom AMI product family will gain enhanced secure communications capability and distributed intelligence in electricity transmission and distribution infrastructure.

BlackBerry | certicom

About Itron Inc.

Itron Inc. is a leading technology provider to the global energy and water industries. Itron Inc. consists of Itron in North America and Actaris outside of North America. Our company is the world's leading provider of metering, data collection and utility software solutions, with nearly 8,000 utilities worldwide relying on our technology to optimize the delivery and use of energy and water. Our products include electricity, gas and water meters; data collection and communication systems, including automated meter reading (AMR) and advanced metering infrastructure (AMI); meter data management and related software applications; project management, installation, and consulting services.

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 and Asia.
Visit www.certicom.com.

Corporate Headquarters
4710 Tahoe Blvd, Building A
Mississauga, ON L4W 0B5
L4W 5L1, Canada

Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com

A Subsidiary of BlackBerry

Additional Certicom White Papers

To read other Certicom white papers, please visit www.certicom.com.

Sum Total: Determining the True Cost of Security
Sourcing Security: Five Arguments in Favour of Commercial Security Solutions

Government

Making the Grade: Meeting Government Security Requirements (Suite B)
Meeting Government Security Requirements: The Difference Between Selling to the Government and Not
FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

Mobility

The Inside Story
Many Happy Returns: The ROI of Embedded Security
Welcome to the Real World: Embedded Security in Action

Sensor Networks

Securing Sensor Networks

DRM & Conditional Access

Injecting Trust to Protect Revenue and Reputation: A Key Injection System for Anti-Cloning, Conditional Access and DRM Schemes
Achieving DRM Robustness: Securing the Device from the Silicon Up to the Application(PDF)

Enterprise Software

Using Digital Signatures to cut down on Bank Fraud Loss

ECC

An Elliptic Curve Cryptography Primer
ECC in Action: Real World Applications of Elliptic Curve Cryptography
Using ECC for Enhanced Embedded Security (PDF)