CERTICOM WHITEPAPER SERIES

Critical Infrastructure Protection for AMI Using a Comprehensive Security Platform

February 2009

certicom™

certicom™

Executive summary

Driven by strong economic and environmental benefits, utilities are deploying new Advanced Metering Infrastructure (AMI) systems in pursuit of a smart grid vision that delivers operational efficiency, enables consumers to participate in personal energy management and conservation and supports smart energy and distribution grids. This is an evolution of metering beyond automated reading and data collection systems. AMI offers benefits across the utility organisation, from load forecasting to meter management and field operations. Efficiencies are realized in: outage management, customer care, reducing dependence on fossil fuels, deferring investment in power generation capacity, lowering exposure to spot market energy pricing and moderating greenhouse gas emissions.

AMI benefits consumers by allowing utilities the ability to provide consumers with real-time energy monitoring and Demand Response programs, dynamic energy pricing and new energy management services. Consumers save with lower bills and enjoy their contribution to improving the environment while utilities benefit from a manageable power load.

As is common with new information technology, potential benefits come with new risks as utilities extend their information network and distributed control systems boundaries to meters at their customers' homes. Such far reaching networks with millions of end nodes, increase the risk posed by potential attackers and eavesdroppers. A strong security foundation is critical to creating a robust and reliable smart grid.

This paper presents the security requirements for advanced metering infrastructure and a how to meet them with Certicom's robust turnkey encryption and key management appliances that provide an end-to-end security layer for AMI networks.

.

certicom™

Introduction

Relatively quiescent for the previous 100 years, the utility and metering industry is now going through an evolution, starting with Automatic Meter Reading (AMR) systems in the 1990s and now investing to upgrade distribution networks with smart meters and Advanced Metering Infrastructure (AMI) and other Smart Grid technologies that can help improve energy efficiency and lower utilities' operational costs.

AMR systems deployed in the 1990s supported remote meter reads with walk-by and drive by data collection. New AMI systems provide two-way communication between the meter data management system and on premise electric meters, allowing meter data to be sent from the meter to the utility and demand response commands to be send from the utility to the meter.

Meter data, can be read periodically or on-demand, allow hourly or more frequent collection of usage data and system information. Such data provides detailed information including cumulative kWh usage, daily kWh usage, time-of-use kWh and peak kW readings, last interval demand, voltage and voltage event logs, phase information, outage logs, and tamper notification. Data can be collected from groups of meters or selectively read from one meter at a time. In addition, many smart meters measure energy consumers put back on the grid from alternative energy distribution such as solar.

This information is available on demand in near real-time, allowing for improved operations and customer management. Remote service connect and disconnect is just one example of savings by eliminating the costly truck roll, allowing utilities to deploy operating capital elsewhere. Frequent interval measurements enable Critical-Peak-Pricing (CPP) and Time-of-Use (TOU) pricing models that can shift energy demand away from peak consumption periods. Enhanced communications and data management software allow utilities to remotely manage their metering assets, forecast loads, respond to outages, remotely disconnect services and issue final bills.

AMI enables more controlled demand response and load management schemes for targeted customers. It can modulate loads from power hungry systems such as air conditioning compressor circuits during critical peak energy events. In aggregate this load shedding capability can be quite powerful for removing excess demand from the network.

Communication bridges extend utility data networks beyond the meter, and into the home. Consumers can view dynamic pricing data, information which helps consumers understand their energy consumption profiles, reduce or shift their energy consumption and lower their electricity bills. The connectivity also provides utilities an opportunity to offer new services such as property monitoring. With AMI-enabled home area energy networks, power consumption data can be collected even at the appliance level and used for detecting maintenance problems.

certicom™

The Need for Security

Advanced Metering Infrastructure's 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.

Once these devices are on a network, they will need remote management and firmware upgrade capability to stay up to date. Allowing firmware updates creates potential vulnerabilities – places a hacker can attack to inject unauthorized remote disconnects or broadcast load shedding signals to blackout a region; places that criminals can lurk to spy on a homeowners; ways to provide fraudulent readings and steal energy.

A malevolent attacker or unwitting hacker could harm someone connected to in-home medical equipment, cripple a business or cause a wide-scale blackout and hundreds of millions of dollars in economic damage. This creates a compelling argument to protect the AMI network and metering assets.

Other threats such as breaches of privacy may have less dramatic impact from a distribution system viewpoint but should give utilities pause as they think about their legal liabilities. For instance a burglar could monitor residential meter readings on an unprotected or poorly secured AMI radio network. Interval meter measurements implicitly divulge living patterns which could allow a burglar to systematically plan break-ins.

Add a Home Energy Network to the mix and consumers have more reason for concern – they want to ensure that smart energy devices on their network are controlled by a customer approved utility demand response program and information transmitted between their energy service portal, such as a in-home gateway or smart meter, is protected.

These vulnerabilities have led to the formation of industry groups studying security for AMI and home energy networks. One of those organizations is the UCA® International Users Group, a not-for-profit corporation consisting of utilities and their supplier. The UCAIUG is dedicated to promoting the integration and interoperability of electric, gas and water utility systems through the use of international standards-based technology.

The UCAIUG's Utility AMI security working group (AMI-SEC) recognized that security is a critical enabler for smart metering. They aim to establish baseline AMI security requirements at the outset and are drafting a specification which serves as a useful guide for utilities evaluating vendor offerings.

The objective of the specification is to protect smart grid services from malicious attack or unintended side effects of normal operations which might threaten the integrity or availability of the system. With a proper security framework established, utilities can work through AMI deployments in confidence.

AMI-SEC has identified numerous stakeholders, from the billing system to installation, operations and maintenance and on to the consumer. Each has unique concerns depending on the processes they are involved in.

Baseline security requirements can be classified by high-level functionality. These include confidentiality and privacy, integrity, availability, identification, authentication and authorization, non-repudiation and accounting/logging services.

The foundation of much of this functionality is based on cryptographic services including cryptographic key management and cryptographic operations for a number of purposes, including to:

- Cryptographically authenticate metering assets to the network to ensure that only known and approved devices participate in the network
- Authenticate and integrity check system commands, at the meter, to ensure they are authorized and haven't been tampered
- Guard against replay attacks to prevent denial of service attacks or load shedding and ensure availability of system resources
- Encrypt meter data to protect consumer privacy
- Provide a means of non-repudiation for consumer demand response programs
- Provide integrity protection and origin authentication of meter data.
- Authenticate and integrity check meter firmware and configuration images when updates are provisioned

Beyond baseline cryptographic services, systems and processes are also needed to manage assets in a secure fashion. For instance, system keys must be protected from disclosure through physical and policy-based mechanisms. Role based access controls should authenticate utility operations personnel authorized to manage the system and provide a secure audit trail when system management or maintenance tasks, such as updating of keys is performed.

certicom™

Code Signing and Firmware Authentication

A key step in building a strong security foundation is to establish a root of trust for every device. This enables each device to validate its operating environment, including any modifiable software or configuration files. It is when firmware is being reprogrammed that devices can be most vulnerable.

To ensure image code integrity and authenticity, the core boot loader should be stored in protected (read only) memory. Signatures should authenticate firmware and sensitive configuration data. In order for those signatures to be legitimate, OEM authentication keys should also be protected from unauthorized modification – preferably stored in one-time-programmable (OTP) memory. Configuration data should be bound to the device identity, such as a unique MAC address.

Technical Challenges: The Smart Metering Environment

AMI networking technology is fairly heterogeneous - with all manner of technology – from proprietary 900MHz and 2.4GHz wireless radios to various flavors of 802.15.4 (ZigBee/6LoWPAN) mesh networks to broadband power line (BPL) to cellular providing local communications and backhaul. Deployments mix networking technologies to provide the right balance of power consumption, bandwidth, throughput, latency and cost. Given this network diversity, end-to-end security must be transparent to the network.

As Smart Grid applications evolve, utilities will evaluate which is suitable for their network. Each application has a benefit but also a cost in terms of reserve bandwidth. The use of low-power radios operating in license-free spectrum for local distribution networks is common. These devices are typically bandwidth constrained and work best when sending small packets which don't require fragmentation and reassembly and don't eat up reserve bandwidth. Security should not add a significant amount of network overhead or require fragmentation and reassembly of authenticated commands or acknowledgements.

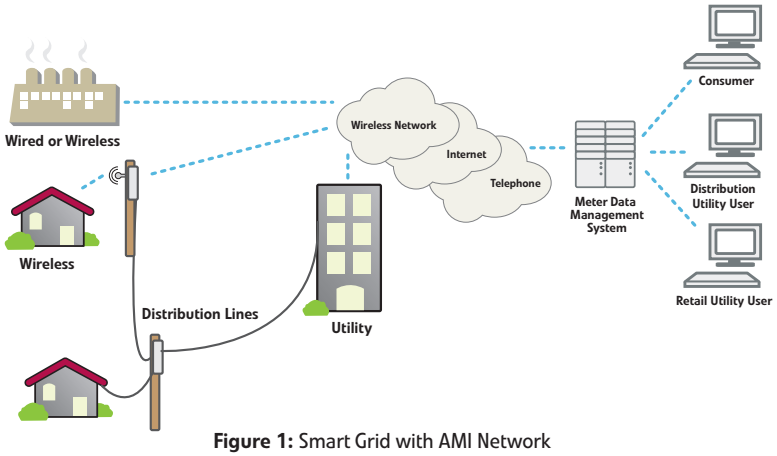

Figure 1: Smart Grid with AMI Network

In the meter endpoints, embedded microprocessors, 8 or 16-bit microcontrollers (MCUs), are quite common. These devices have limited amounts of RAM or flash memory, typically challenging devices to make both open and secure. To preserve existing investment, security should not require a wholesale change to a new meter computing platform.

Once installed, meters might be expected to be deployed for twenty years or more. Rework and redeployment can be prohibitively expensive. The security scheme needs to be robust enough to stand the test of time.

The Certicom Solution

Certicom AMI security solution is based on a highly scalable turnkey security architecture that provides an automated, end-to-end security between utility meters and utility companies' back-end IT infrastructure. The high performance AMI security solution can supports millions of meters, multiple reads/hour and runs on low-power microcontrollers (MCUs).

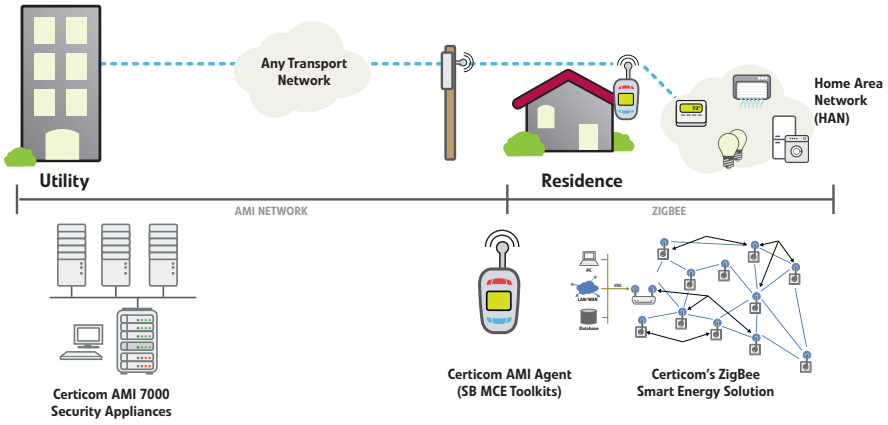

Figure 2: Smart Grid Network: Certicom AMI 7000 Appliance, Certicom Security Builder AMI Agent, and Certicom Zigbee Smart Energy Agent

The Certicom AMI security solution consists of Certicom AMI 7000 Series Security Appliances and a Certicom AMI Meter Agent.

Certicom AMI 7000 appliances are security-hardened rack mountable appliances designed to help utilities meet NERC Critical Infrastructure Protection (CIP) requirements for AMI deployments.

Certicom supports large-scale deployments where security performance and robustness are vital. By providing turnkey management of critical system keys and strong authentication of demand response events, Certicom enhances a utility's security posture and reduces the burden of CIP compliance.

Certicom's AMI solution was specifically designed to support emerging AMI-SEC requirements yet work in today's low-bandwidth, resource constrained metering environments. It is an end-to-end security solution that supports ANSI C12.22 compliant devices. It is network and protocol agnostic, so, it can be deployed with any network topology, from today's heterogeneous environments to tomorrow's all-IP network.

Certicom achieves these requirements applying strong cryptography algorithms and enforcement of robust key management practices from start to finish.

AMI 7100 Signing and Encryption Server

The AMI 7100 enables high speed signing of system commands, while maintaining a high security posture, and provides strongly authenticated command and control that prevents forged commands and replay attacks.

The AMI 7100 can authorize commands for a single meter, a group of meters, or an entire network. System keys are based on Elliptic Curve public key cryptography and use the Elliptic Curve Digital Signature Algorithm, ECDSA to provide integrity and non-repudiation. The meters, which have the public key portion of the Elliptic Curve key pair, verify system command signatures and perform integrity checks to ensure that only authentic system commands are processed.

NIST-approved 283-bit ECC binary curve keys have AES 128-bit equivalent strength and create a formidable cryptographic impediment to message forgery. Small signatures enabled by ECC allow short commands and authenticated responses to quickly traverse any network topology.

The performance advantages of ECDSA make it feasible to secure meter commands for even the largest scale AMI deployments. In contrast, an equivalent strength RSA-based authentication scheme would require 3072 bit keys. Over ten times longer and ten times slower, RSA signatures would require significantly more network bandwidth and processing power.

In addition to being signed, critical messages are also protected with a mechanism to prevent replay attack. This ensures that the AMI system does not fall victim to a denial of service induced by a replayed load shed, remote disconnect or pricing signal messages.

Optional message encryption allows new meter symmetric keys or other sensitive data to be sent over the air in a protected manner. Device authentication ensures that only trusted devices receive key updates.

Symmetric and public keys deployed in the meters themselves are generated using FIPS-approved random number generation techniques to ensure that the system isn't vulnerable to a basic but all-to-common security flaw. These aspects are easily overlooked by designers unfamiliar with how such a flaw could undermine system security.

As an additional precaution, signing keys managing the system are protected in tamper-resistant hardware. Access requires multiple security officers to authorize a new key. Security policies and procedures are used to enroll and authorize new system operators, applying safeguards to establish who has access to which keys and what parts of the system.

Secure log files are updated whenever any management activity is performed to reduce the likelihood that utility personnel perpetrate an attack from the inside.

AMI 7200 Key Management and Decryption Server

The AMI 7200 performs high-speed meter data validation, offloading integrity checking from the data collection system. In order to protect the confidentiality and integrity of metering data, data sent from the meter is encrypted with 128-bit level AES encryption using unique keys stored in each individual meter. This keeps customer interval data and personal profiles confidential and reduces any legal liability that utilities may have in collecting usage data. Customers do not need to worry about burglars or even nosey neighbors tapping into private information.

Given the sheer volume of potential messages performance issues are minimized by authenticating and integrity checking messages with an efficient hashed message authentication scheme and a high-performance decryption engine. As a result, throughput can be maintained even for the largest metering deployments.

Key management and key updates are treated as sensitive operations, both in the meter and in the meter data management system. The AMI 7200 can manage millions of meters using multiple meter keys per meter whilst rotating keys as required to ensure that a strong security posture is maintained.

Meter IDs and associated metadata (AES keys, random challenge and meter ECC public keys) are stored along with the security state of individual meters. Provisioning facilities allow new meters to be commissioned as a deployment unfolds.

Availability and performance is enhanced by providing the AMI 7000 appliances as redundant, load balancing platforms. A backup system supports failover requirements so that the system can continue operating in the event of a hardware malfunction or during scheduled maintenance.

Support for Itron Open Way Architecture

The Certicom AMI7000 appliances are integrated with Itron's Open Way AMI architecture and meter data collection engine through secure Web Services interfaces, offloading C12.22 meter data processing and key management. By cleanly separating security functionality from meter data management, Certicom and Itron are able to provide utility customers with robust CIP compliant AMI security without impacting their traditional back-office operations.

Certicom Security Builder AMI Agent

Certicom Security Builder AMI agent provides the cryptographic primitives required to create a trusted platform for resource-constrained smart metering devices. The library supports the cryptographic algorithms and protocols which, when coupled with the AMI 7000 AMI series security appliances, provide end-to-end security of the AMI network without impacting network transport infrastructure.

Optimized for resource-constrained MCUs, the library supports AES encryption, decryption, digital signature signing and verification, and keyed hashing for message authentication. Performance and footprint optimized software ensures that the meters themselves do not need expensive MCU upgrades.

As an added option, secure boot and software validation modules can be added to further enhance the security of meter designs.

Certicom Secure Boot

Validating firmware from a root of trust in the meter ROM prevents hacking of individual meters and reduces the likelihood of theft of service attacks. Any static images such as over-the-air configuration data or software updates are likewise digitally signed so that they can be validated by the meter. This ensures that the system maintains its integrity even when metering assets are deployed in the field.

The diagram below illustrates how Certicom's secure boot secures smart meter devices by digitally signing and validating device firmware. Any accidental or intentional tampering with code or configuration data will almost certainly change the hash value, making it not match the hash digest signed with an Elliptic Curve Digital Signature Algorithm (ECDSA) private key.

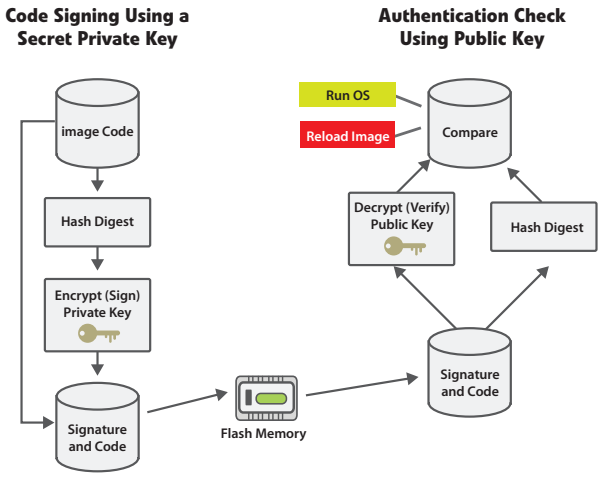

Figure 3: Secure devices using digitally signed and validated firmware

Certicom's secure boot module ensures that only authentic, OEM authorized code and configuration data runs in remote endpoints.

Conclusion

The utility market is embracing the convergence of electricity metering, communication and information technology, investing in a smart grid vision that is poised to deliver lasting cost and environmental benefits. But creating the world's largest distributed command and control systems has its risks. Certicom AMI 7000 security platform and Itron Open Way Collection Engine can protect utility investments and help deliver a robust and resilient solution that meets today and tomorrow's energy needs.

Certicom is a vendor of choice due to the combination of expertise in secure distributed communications systems and commercially proven components vital to swift, secure deployment of your AMI network.

certicom™

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.

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

A Subsidiary of Research In Motion Limited RIM

certicom™

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)