**Itron White Paper**
*OpenWay® by Itron*

# OpenWay by Itron Security Overview

*Kip Gering / R. Eric Robinson*
*Itron Marketing / Itron Engineering*

## Executive Summary

The OpenWay® by Itron system was designed to meet the ever-changing requirements for advanced metering infrastructure (AMI) and smart grid initiatives in the energy and utility industries—industries Itron has served for over 25 years as a true market leader. Industry groups have only recently begun discussions on the security aspects of true two-way AMI systems that provide new levels of connectivity and involvement with end-use customers. Because of this new capability offered, AMI systems must provide a secure means for communication, as well as the command and control capabilities necessary for conservation and remote connect/disconnect operations.

## Intent of the Document

The purpose of this white paper is to discuss Itron's OpenWay security architecture and how this architecture is designed for scalability and a robust feature set. This paper focuses on the network security components—the Collection Engine to the meter register—in the context of the C12.22 architecture of OpenWay.

## Security Risk Analysis for Advanced Metering Systems

For utilities, AMI systems provide a new level of two-way connectivity with the end consumer—enabling advanced data acquisition, command and control and communication into the home. As a result, these AMI systems form the foundation of a digitized smart grid and must be protected. A system compromise can not only affect numerous customers but also create havoc with grid operations.

These capabilities also provide opportunities for a nefarious agent to attack the system. The attacker looking for fame or the terrorist looking to inflict harm will find remote disconnects switches and load control devices are exciting things to attack. The thief wanting to lower their energy bill would love an easy silent hack that reduced their meter readings.

A security risk analysis is an objective assessment of the effectiveness of existing security controls within a system. This risk assessment can be used to assess the probability, severity and reasoning of certain attacks and allows designers to implement proper controls for mitigation purposes. The development of a risk assessment includes listing the security assumptions, threat agents, motivations, threats, vulnerabilities, controls and assets in the system of interest. *Figure 1* on page 5 shows the interaction of some of these functions.

In a full OpenWay deployment, there are a variety of areas to attack:

- The meter itself.
- The RF communications between the network and the meter.
- The Cell Relay devices.
- The WAN communications with the Cell Relay.
- The OpenWay Collection Engine.

The likelihood of a component being attacked, the likelihood of that attack succeeding, and the overall impact of a successful attack are all different, and vary from component to component.

## OpenWay Security Overview

Itron believes that two-way AMI systems can be categorized as a *critical cyber asset* based on NERC CIP 002-001. NERC CIP 002-001 defines a *critical cyber asset* as any utility system that facilitates critical to automatic load shedding under a common control system capable of shedding 300 MW or more and uses a routable protocol outside of the Electronic Security Perimeter.

Based upon the critical nature of an AMI system and Itron's threat model, a secure AMI system must provide asymmetric cryptography to protect the integrity of control of the system. In addition, security features must be

included that ensure system availability and confidentiality of data. Itron has integrated a number of different security appliances to secure network communications, provide key management functions and monitor the network for attacks. These appliances also provide features that support administration, non-repudiation, access control, identification and auditing.

## OpenWay Security Architecture

Securing the OpenWay system involves being able to sign command messages, encrypt and decrypt messages, audit both the security activities and the events being returned by the meter, manage the keys and manage the larger set of security components deployed with the system. With this in mind, the security architecture for OpenWay includes the following specific security components:

### *Industrial Defender 300B Security Event Monitoring*

The Industrial Defender 300B component provides the ability to collect, correlate and analyze audit events to allow detection of intrusions and attacks. Examples of audit events include: device reprogramming, device authentication failure, signature verification failure, message decryption failure, home area network (HAN) traffic rate exceeding threshold, device firmware upgrade and spurious HAN and local area network (LAN) messages. These events are primarily generated at the meter or from wide area network (WAN) devices and sent to the OpenWay Collection Engine. The Collection Engine translates these lower level protocol alerts into API calls for submission to the security event monitor.

### *Certicom AMI 7100 Signing and Encryption Server*

The Signing and Encryption Server is responsible for securing command messages being sent from the Collection Engine to the meters. As a result, the number of keys managed for these messages is quite small, potentially as little as two keys that need active control. However, these keys must be very tightly controlled to ensure that the system is not compromised. The private signing key of the Collection Engine is never exposed in raw form, though there are facilities to back it up. To protect the keys, the Signing and Encryption Server includes an integral hardware security module (HSM). The HSM is FIPS 140-2 level 3 compliant, meaning that it is government-certified to protect the keys it contains against both physical and electronic attacks.

### *Certicom AMI 7200 Decryption and Key Update Server with Key Management Server*

This component provides rapid message decryption and comprehensive key management. Messages coming from the meters to the Collection Engine need to be quickly decrypted. In a large-scale OpenWay implementation, the system can decrypt more than 1,000 messages a second, each with its own unique key. While the messages are small, over the course of several hours, the system may need to decrypt messages using between 5 and 10 million unique AES keys. The solution must be able to quickly handle accessing millions of keys, decrypting thousands of messages and passing them on to the Collection Engine.

## Security Appliance Performance

The security architecture was designed specifically for OpenWay operational use cases centered on performing multiple functions such as meter data collection, demand response and remote disconnects simultaneously for 10 million meters or more. The appliances are also designed so one appliance can handle the storage and message traffic of a system with 10 million devices. Customers only need to install additional appliances for high availability and disaster recovery, not performance.

From a performance perspective, there are two general OpenWay system message schemes to consider:

**1) Message from the Collection Engine to the Meter**

Downstream messages from the Collection Engine to the meter are encrypted using an AES-128 bit key and signed using an ECC-256 bit key. For the Collection Engine, the security architecture allows for broadcast and multicast communications, where a single message from the Collection Engine can direct behavior for a large number, potentially millions, of meters simultaneously. This has the advantage over a point-to-point system in which every meter needs a message from the collection engine. For the OpenWay system, signature verification and decryption is

pushed out to the meters in a distributed fashion. The meter processes these security functions in milliseconds once the command is received. Thus, while each meter will need to validate the signature on the message to ensure its authenticity, those validations occur in parallel. The result is very little latency is ever added to a group operation no matter how many meters are involved. At the collection engine, the system can easily sign and encrypt 200 operations per second.

**2) Message from the Meter to the Collection Engine**

Upstream messages from the meter to the Collection Engine are encrypted with an AES-128 bit key. The OpenWay architecture is optimized such that an IP load balancer shapes the ingress traffic, distributing equally among the Collection Engine subcomponents for processing. The Collection Engine unwraps the network portion of the packet and passes the payload to the Certicom AMI 7200 Decryption and Key Update Server for processing. This appliance is scaled to decrypt 24,000 messages per second. From a scalability perspective, this maps out to over a million meters per minute processing.

### Meter Decryption and Encryption

Cryptographic processing at the meter is done using libraries provided by Certicom. These libraries include the algorithms recommended by the National Security Agency under their "Suite B" recommendations for commercial security. Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme.

## Collection Engine to Meter Communication within OpenWay

### Collection Engine to Meter Communication

The Collection Engine is responsible—in conjunction with the security appliances—for supporting the integrity of the control of the system. As a result, asymmetric cryptography is supported for command and control messages. Every node in the system has a set of asymmetric keys that are used for authentication and non-repudiation functions. Initial meter registration involves a key exchange process that establishes mutual authentication based upon a Diffie-Hellman exchange. When sending out messages, the C12.22 payload is signed and encrypted before being wrapped it in the C12.22 protocol. This is accomplished by the integrated Signing and Encryption appliance. As control over this operation is absolutely critical to ensuring control over the system, the Signing and Encryption Server will never expose the signing key. When the meter communicates information upstream to the Collection Engine, the C12.22 messages are encrypted to protect the confidentiality of data and decrypted by the DKUS appliance. An overview of this exchange is depicted in *Figure 1* below.

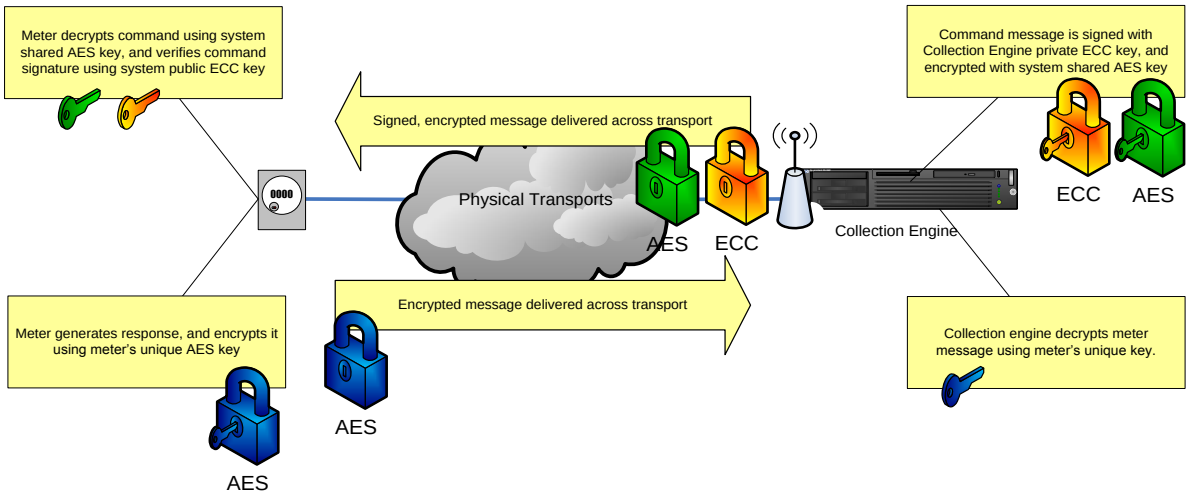


**Figure 1**

## RFLAN and Cell Relay Communications

The OpenWay radio frequency LAN (RFLAN) is a proprietary frequency-hopping RF network deployed in North America, utilizing the 900 MHz ISM band. Messages are transmitted in accordance with the ANSI C12.22 protocol, and are encrypted using 128-bit shared AES keys and signed using 256-bit ECC private keys.

The Collection Engine interfaces with meters through Cell Relays. Firewalls are recommended between portions of the system; however, the OpenWay architecture requires full two-way communication between the Collection Engine and the Cell Relay. The Collection Engine can be placed behind a firewall and still allow traffic on port 1153 (C12.22) to pass through. The Collection Engine needs to be able to access its database instance as well as the enterprise management system and the meter data management (MDM) application. These applications may be behind additional firewalls, or they may be on the same network as the Collection Engine itself, provided that the Collection Engine has full two-way access to the appropriate ports for data transfer. This initial communication is done using TCP/IP. As either the Collection Engine or the Cell Relay can initiate communications, both products must accept incoming C12.22 messages on TCP/IP port 1153. The Collection Engine listens on port 1153 for C12.22 communication and monitors the network for Web services calls.

## C12.22 and Meter Security

The C12.22 architecture plays an important role regarding the implementation of security. The major benefit of the design of a C12.22 network is that the Collection Engine interfaces at an application level protocol layer, enabling both session- and sessionless-based communication directly to the meter register. Unlike designs tied to a single communications network, with OpenWay the security architecture does need to change if the communication architecture changes. For example, an IP based network may provide IP communications and security to the NIC (Network Interface Card); however, after decrypting the message, another security function may be required for the NIC card to communicate using a C12.18 protocol for logging on to the register of the meter. An unfortunate consequence of this process is reduced reliability and the inability to perform simultaneous functions during the session.

OpenWay also benefits from the ability to perform broadcast and multicast communications to meters, minimizing the amount of messages that require encryption and processing, as opposed to sending multiple messages point to point to meters.

### Security Standards

OpenWay's security architecture is design to support NERC CIP requirements for critical cyber assets. In order to address this design criterion, OpenWay also supports the following security standards for security controls and functions.

- Designed to adhere to NSA Suite B requirements, including:
    - FIPS 197 approved encryption algorithms
    - FIPS 186-2 approved signature algorithms
    - FIPS 180-2 approved hashing algorithms
- Meets FIPS 140-2 Level 3 for cryptographic modules

## Summary

In summary, OpenWay's security architecture is tightly integrated with a set of Industrial Defender and Certicom appliances that are designed specifically for key security functions, without sacrificing the performance requirements that are needed for two-way command and control AMI and smart grid network operations. The Certicom AMI 7100 and 7200 appliances used with OpenWay provide customers the ability to meet NERC and FIPS requirements to protect their AMI network. In addition, these appliances exceed the operational requirements of OpenWay to support up to 10 million meters without the need for additional appliances or without impacting the system's performance managing upstream and downstream message processing. The Industrial Defender security event monitor completes OpenWay's security solution providing utilities insight into potential attacks against the system. OpenWay's architecture also reduces the complexity around security through the use of C12.22 and node-to-node communication between the Collection Engine and the meter register.

## Itron Inc.

Itron Inc. is a leading technology provider to the global energy and water industries. 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; as well as project management, installation, and consulting services. To know more, start here: www.itron.com

To know more, start here: www.itron.com

**Itron Inc.**
**Corporate Headquarters**
2111 North Molter Road
Liberty Lake, Washington 99019
U.S.A.
Tel.: 1.800.635.5461
Fax: 1.509.891.3355



Publication 100933WP-02
07/09