Itron Security Manager (ISM)

Keep Your Data Safe

A new era of smart metering promises many exciting benefits, but comes with the imperatives of increased security and privacy protections. Automated meter reading and advanced metering infrastructure solutions rely on communications systems to transmit metering data, which could leave critical information open to theft and manipulation. An added concern, today's smart meters and endpoints have command interfaces that could be vulnerable to unauthorized reconfiguration and tampering, such as remote service disconnects at the customer premise. Lastly, as meter reading technology relies progressively more on networks, it could increasingly be the target of cyber attacks.

The Itron Security Manager (ISM) enables secure communications and data privacy between endpoints and authorized data collection systems. Utilizing industry-standard encryption technology, ISM uses cryptography to authenticate and encrypt two-way communications, providing the data confidentiality, integrity and authenticity critical for system security. Beyond cryptographic functions, the ISM acts as the centralized key manager. First, it manages the security keys, security state and security level for each of the endpoints. Second, ISM manages the import and export of security key files. If an endpoint security level is changed, ISM will generate additional keys for meter reading applications to update devices in the field. Third, ISM allows keys to be updated, as required by the utility's security policies, thus mitigating the risk of data theft and manipulation.

SPECIFICATIONS

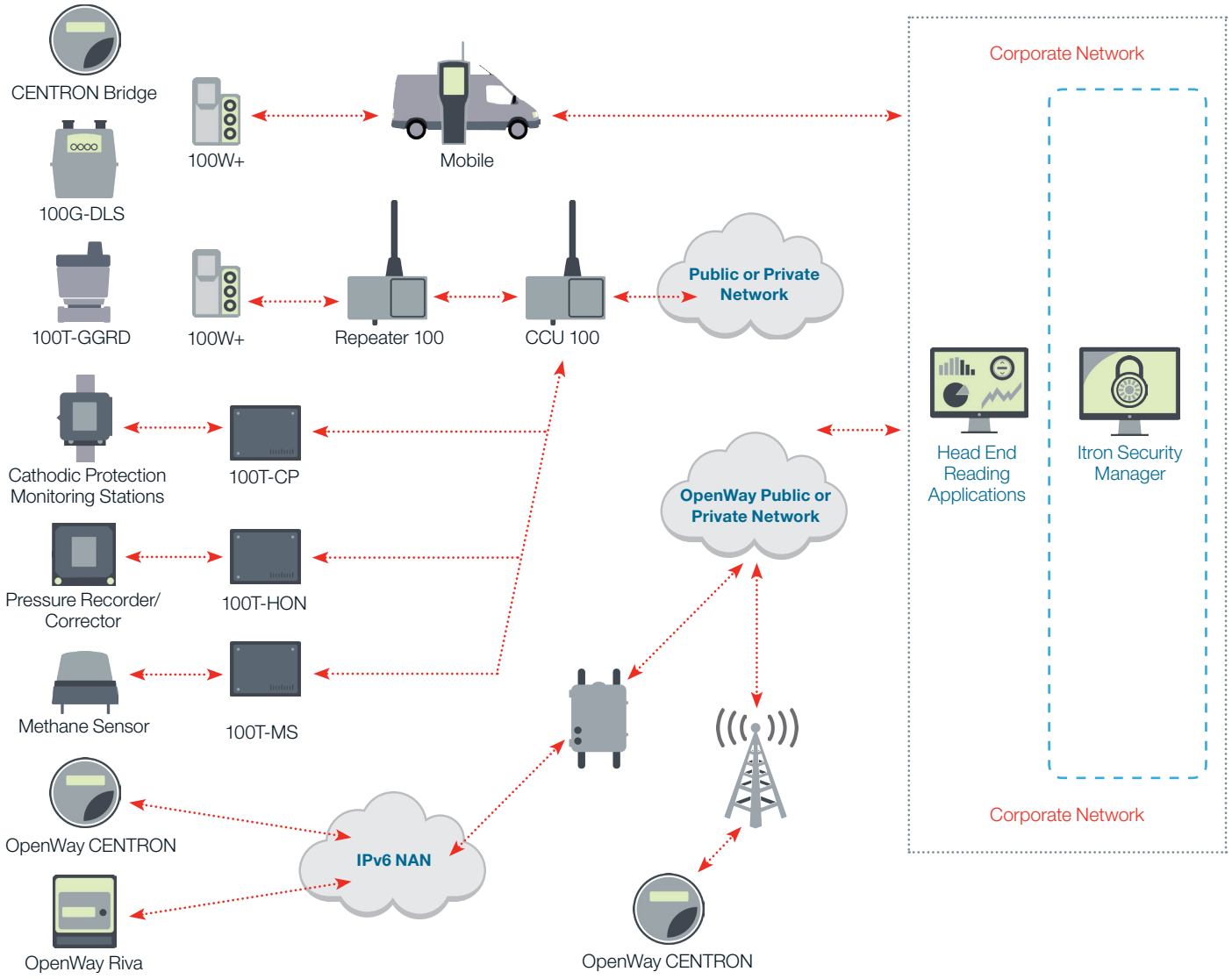

Figure 1: ISM Architecture

In addition to managing security keys, the ISM provides core system administration, such as creating accounts and roles, as well as assigning permissions. The administrative controls are used to lock down access and grant privileges only to personnel and data collection applications requiring ISM services.

FEATURES AND BENEFITS

- Supports Itron's AMI/AMR data acquisition applications: Fixed Network (FN), Field Deployment Manager (FDM), Field Collection System (FCS), MV-90 xi, Saturne and the OpenWay Collection Engine
- Delivers application layer security for Itron's communication protocols
- Ensures consumer data privacy and confidentiality through encryption
- Provides Advanced Encryption Standard (AES) symmetric key encryption and Elliptical Curve Encryption (ECC) asymmetric key encryption
- Secures communication channels between the head end and endpoints through authentication
- Stores and manages security keys with a secure, centralized database
  - System of record for all endpoint device keys
  - Manages key import, export and backup
  - Supports the generation and management of shared and unique keys for each endpoint
  - Facilitates security key exchanges, allowing utilities to update keys according to their security policy
  - Encrypts security keys stored in the database
- Allows data collection applications to request authentication and encryption through a cryptographic interface
- Utilizes NIST-approved encryption and authentication methods
- Supports multiple device types, each of which could use different encryption algorithms and contain different numbers and types of keys
- Provides event logging and reporting services for auditing
- Delivers a rich user interface for monitoring the system security status and errors
- Offers system administration functions to manage all user accounts and associated permissions
- Scales to match utility needs for high availability and high performance

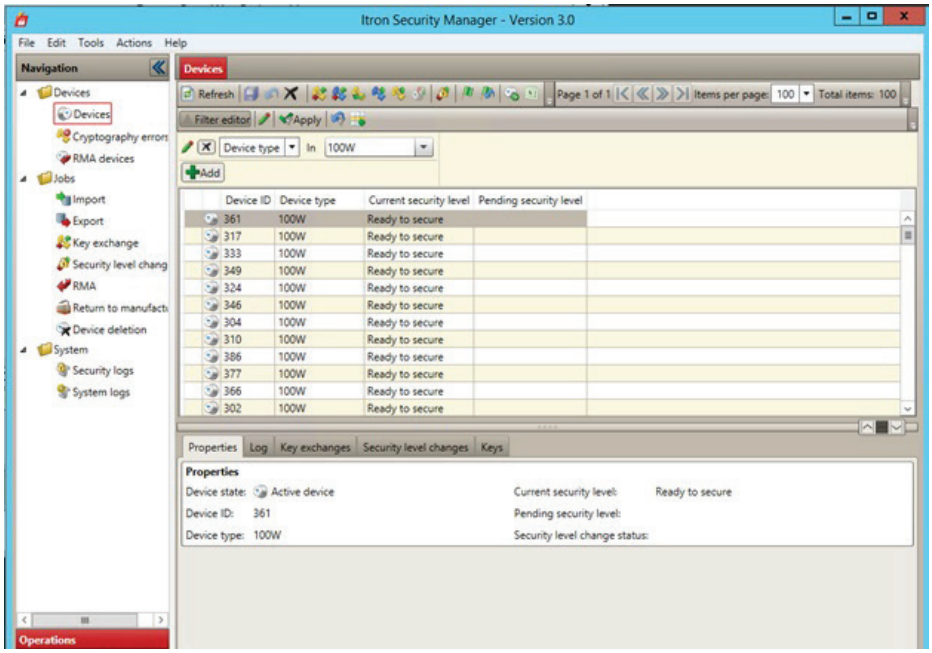

Figure 1.2: ISM Import Devices View

SUPPORTED APPLICATIONS

- Field Collection System (FCS) 2.5 or higher
- Field Deployment Manager (FDM) 3.6 or higher
- Mobile Collection Software 3.5 or higher
- Fixed Network (FN) 5.0 or higher
- Eclipse Enterprise 12.1
- OpenWay Collection Engine 6.0 or higher
- Saturne 4.8 or higher
- MV-90 xi 4.5 or higher

SPECIFICATIONS

- Database Platforms: SQL Server 2008 R2, Microsoft SQL Server 2012 and Oracle 11G
- Application Server Operating Systems: Windows Server 2012 R2
- Client Operating Systems: Windows Server 2012 R2, Windows 7
- Hardware Security Module Support: SafeNet Luna PCI-E 1700 for ChoiceConnect and the Thales nConnect 6000+ for OpenWay

ENDPOINTS

- 100G-DLS
- 100W+
- 100T-CP
- 100T-HON
- 100T-GGRD
- EM420i (GALVANI)
- CENTRON Bridge Meter
- OpenWay CENTRON II
- Gallus Net
- Gallus RF1 Net
- OpenWay Riva™

Join us in creating a more **resourceful world**.
To learn more visit **itron.com**

CORPORATE HQ
2111 North Molter Road
Liberty Lake, WA 99019 USA
Phone: 1.800.635.5461
Fax: 1.509.891.3355