> Itron white paper

OpenWay® Signed Authorization for Local Communications Support

Katrina Hutchinson
Senior Product Manager

© 2011, Itron Inc. All rights reserved.

© 2011, Itron Inc. All rights reserved.

Introduction

With the release of SR 2.0 SP5.1, Itron will extend the Signed Authorization to include local communication. This will allow the utility to maintain the same level of security when communicating over the air or locally via the optical port or ZigBee® wireless communication module.

Overview

Upon release of SR 2.0 SP5.1, based on customer preference, all OpenWay meters will be configurable to require Signed Authorization for local meter communications via the optical port or ZigBee. This configurable setting will be a part of the meter's configuration as defined in the Collection Engine (CE). A new option in the Communications tab will allow customers to enable Signed Authorization for securing local communications.

Note: Upon activation of SR 2.0 SP5.1, the register will default to not require Signed Authorization.

Below is a description of each of the two options available.

Standard C12.18 Optical Security: Signed Authorization Not Required

When the meter is configured to not require Signed Authorization, the meter will continue to allow local communications using the Meter Passwords. When logging on to the meter via OpenWay Field Pro, the password used in the replica file will be used to logon to the meter or the user will be prompted to enter the password.

The OpenWay CENTRON meter supports up to five permission levels as described below:

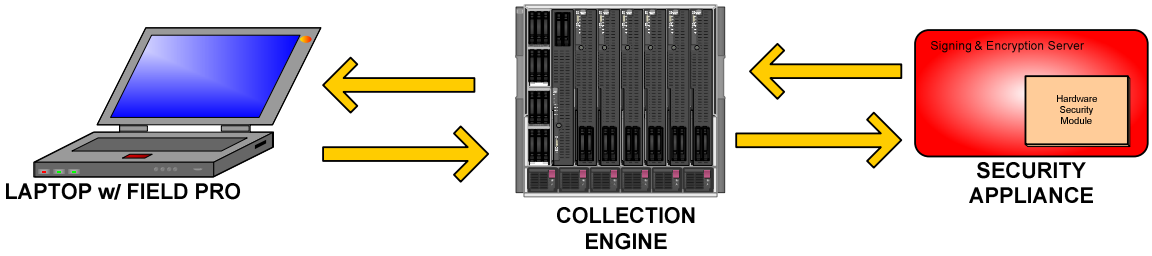
- **Level 4** – Full Access
- **Level 3** – Limited Access
- **Level 2** – Read Only + Access
- **Level 1** – Read Only Access
- **Level 0** – No Access

The meter supports configuration of up to 4 passwords one for each permission Level from 1 to 4..

Signed Authorization

If Signed Authorization is selected, the meter will require valid Credentials prior to allowing local communications. These Credentials must be obtained by OpenWay Field Pro from the CE, via a web service command, prior to use. The Credential will define:

- Signature validating credentials were obtained via Signed Authorization mechanisms
- Meter number the Credential is valid for
  - Individual meter – Used for creation of Credentials under RMA
  - All meters – Used for creation of Credentials for software tools
- Permission Level to use during communication
- Valid time period for Credential



© 2011, Itron Inc. All rights reserved.

Credential Exchange Methodologies

There are two methods of obtaining Credentials from the CE. These methods are outlined below.

Method 1: Certificate Exchange to Establish Trusted Relationship

This option requires that each computer capable of requesting Credentials has been loaded with a certificate that will be used to verify a trusted relationship between that computer and the CE. This certificate can be provided by the utility IT department or via a 3rd party, such as VeriSign.

If the utility IT department chooses to provide the certificate, this certificate must be loaded on all valid computers prior to requesting Credentials. If the utility chooses to utilize a 3rd party, the certificates provided by the 3rd party will allow all Microsoft supported computers to be considered "trusted" at time of purchase.

This option requires User IDs and passwords to be defined at the CE. These User IDs can be generically defined and do not have to be specific to each user.

Note: Users can be defined as "Service Mangers" which allows access to the CE for requesting Credentials only. Service Managers will not have access to the Collection User Interface.

Method 2: Windows Log In (Kerberos) - Active Directory Used to Validate Trusted Relationship

This option requires the use of Active Directory. The Active Directory users or groups must be uniquely defined in the CE role based security, one user name/group for each Active Directory entry. With this implementation passwords are managed by the Active Directory and or not required in the CE.

Collection Engine Settings

Once the utility decides the exchange methodology, the CE must be configured to define which method(s) will be used for Credential Exchange. The utility will also need to define the "Maximal Optical Signed Authorization by Endpoint Duration (minutes)" and the "Maximal Optical Signed Authorization Duration (Minutes)". These values are set in the System Settings, Security tab and define the maximum duration for Credentials for individual meters and all meters respectively.

In addition, when creating the User IDs, the utility will define which of the five optical password levels (as defined earlier) to use when communicating via Field Pro. This optical password information will be passed to the requesting computer as a part of the credential.

OpenWay Tools Settings

After the CE has been properly configured, the OpenWay Tools Administrator will need to properly configure OpenWay Field Pro using OpenWay Shop Manger. In Shop Manger, if Signed Authorization is required, the Signed Authorization option being utilized will be selected and the Authorization Server for that desired methodology will be entered. These values will be used in the replica file and loaded upon execution.

Each Credential request generated by Field Pro will be returned with the maximum duration as configured in the CE, "Maximal Optical Signed Authorization Duration (Minutes)", for a period up to 7 days.

© 2011, Itron Inc. All rights reserved.

Signed Authorization Business Process Overview

Once, implemented each utility will need to define the business process around loading each computer with Credentials as needed. Below is a general outline of the process once Signed Authorization over Optical is enabled.

Step	Action
1	Connect laptop to utility VPN. This can be accomplished by a hard connection locally at the utility or wireless outside of the utility.
2	Run the Field Pro application and request Credentials.
3	If Windows Logon is not used, enter the Collection Engine user Id and password.
4	Once Credentials are loaded, disconnect from VPN.
5	Resume normal Field Pro operations.

Return Material Authorization (RMA) Procedure

When Enhanced Optical security is required, meters being returned on RMA will need to include valid Credentials to allow Itron access to the meter for analysis. A unique application will be available as a part of OpenWay Tools to allow the creation of these Credentials. The web service call used to request the Credentials for RMAs will be different than the web service call used for requesting Credentials for OpenWay tools. The validity duration of the RMA Credentials will be as configured in the Collection Engine for a period up to 45 days. These Credentials will only be valid for Itron internal software only and not to be used by OpenWay Field Pro. The RMA Credentials will need to be generated individually by meter serial number.

Manufacturing Process

For all meters requiring Signed Authorization during manufacturing, Enhanced Optical security will have to be disabled temporarily as to allow the meters to complete the quality control (QC) verification process. In order to accomplish this, a new procedure will be introduced to disable Signed Authorization over optical communications for a period of 7 days for residential meters and 10 days for polyphase meters. This time period will ensure meters are accessible by Itron manufacturing during production. After the 7 or 10 day period has expired or the meter has been logged on to using Credentials the meters will only be accessible with proper Credentials received from the Collection Engine. To ensure a meter is currently utilizing Signed Authorization for local communications, once logged on, OpenWay Field Pro can be used to verify state.

© 2011, Itron Inc. All rights reserved.

Frequently Asked Questions

When the meter is configured to not require Signed Authorization, the meter will continue to allow local communications using the Meter Passwords. When logging on to the meter via OpenWay Field Pro, the password used in the replica file will be used to logon to the meter or the user will be prompted to enter the password.

Question		Answer
1	Are local security and over-the-air (OTA) security configured separately in the CE?	Yes, the Optical security and OTA security are separate. The Security tab is where the OTA security is set. The Communications tab is where the setting for Signed Authorization is set.
2	When requesting a Credential for “All Meters”, are many signed authorizations (one for each meter) or a single one provided?	The “All Meters” Credential is a single credential that is valid for all meters properly keyed with security information from appliances.
3	Will every laptop be able to service every meter in the population? If not, how can we best address portability of credentials across laptops should the work schedules/routes get shuffled from one field resource to another?	Every laptop that requires access to the meters will have to request Credentials. Credentials are not transferrable from one laptop to another.
4	Is the expiration/duration of credentials configurable within each CE Configuration group? Or is there a single credential duration setting in the CE for all groups?	Yes, the duration of Credentials is configurable at the CE for the “individual meter” and the “All meters” Credential. These settings are located in the System Settings Security tab as follows: Maximal Optical Signed Authorization by Endpoint Duration (minutes) and Maximal Optical Signed Authorization Duration (minutes)
5	How does the Time-based authorization information get down to the meter? Does the meter require connectivity to the CE in order to validate Credentials?	The Credential is sent from the Collection Engine to the Software (OW Tools) with a start time and end time. The Credential is signed so that when the meter receives the Credential it verifies based on signature that it is from a trusted source and then determines based on the meter’s current time if the Credential is valid. Only after these checks will the meter allow communications. The meter does not need to be connected to the CE in order to validate the Credential.
6	What happens if my meter is configured to require Signed Authorization and there are no keys injected in the meter?	When initial communication is established the meter will realize there are no keys present and allow communications using Meter Passwords.

© 2011, Itron Inc. All rights reserved.

7	What happens if my meter is configured to require Signed Authorization and there are unknown keys injected in the meter?	When Credential exchange occurs and the keys in the Credential and meter do not match, access to the meter will be prevented. In order to regain access to the meter, the keys will need to be updated or the meter will need to be reconfigured to not require Signed Authorization.
8	Are there any new events associated with Signed Authorization?	Yes, the Security Event now includes new data to indicate the following: • 23: Unrecognized Table ID in the Optical Signed Authorization Record. • 24: "START" time in the Optical Signed Authorization Record is ahead of the meter's time. • 25: "END" time in the Optical Signed Authorization Record is older than the meter's time. • 26: Unrecognized Password Level in the Optical Signed Authorization Record. • 27: Unrecognized Mfg Serial Number in the Optical Signed Authorization Record. • 28: The configuration bit of the Optical Signed Authorization changed from Enabled to Disabled. • 29: The configuration bit of the Optical Signed Authorization changed from Disabled to Enabled. • 30: The Optical Signed Authorization is Disabled for a Period of Time (in minutes). This parameter will include additional 2 bytes to indicate the Time Period. These events will be logged as a Security Event with the associated description ID as the data for the event.

© 2011, Itron Inc. All rights reserved.

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, water and heat 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

Due to continuous research, product improvement and enhancements, Itron reserves the right to change product or system specifications without notice. Itron is a registered trademark of Itron Inc. All other trademarks belong to their respective owners. © 2010, Itron Inc.
Publication 101008WP-01
011/11

© 2011, Itron Inc. All rights reserved.