xylem
Let's Solve Water

INTEGRATION GUIDE

AIT-10004-19

RNI Key Management Gateway

SENSUS
a xylem brand

Revision history

Rev No.	Date	Description
01	30-JUL-15	Initial version.
02	16-FEB-16	Updated for RNI 4.0.
03	5-OCT-16	Updated for RNI 4.1.
04	19-FEB-18	Updated for RNI 4.2.
05	28-FEB-18	Updated for RNI 4.3.
06	26-OCT-18	Updated for RNI 4.4.1.
07	25-FEB-19	Updated for RNI 4.5.0.
08	29-APR-19	Updated for RNI 4.5.1.
09	27-AUG-19	Updated for RNI 4.6.0.
10	29-OCT-19	Updated for RNI 4.6.1.
11	26-FEB-20	Updated for RNI 4.7.0.
12	30-APR-20	Updated for RNI 4.7.1.
13	28-AUG-20	Updated for RNI 4.8.
14	10-JUN-21	Updated for RNI 4.9.
15	25-OCT-21	Updated for RNI 4.10.
16	06-JUN-22	Updated for RNI 4.11.
17	02-DEC-22	Updated for RNI 4.12.
18	16-JUN-23	Updated for RNI 4.13. Added Key extraction file section.
19	15-NOV-23	Updated for RNI 4.14.

Copyright

Sensus
637 Davis Drive
Morrisville, NC 27560
1-800-638-3748
www.sensus.com

Document: RNI™ Key Management Gateway Integration Guide
Document Number: AIT-10004-19

Contents

Introduction

The Sensus **KeyManagement** web service gateway implements SOAP services to retrieve the SmartPoint module's encryption keys. This document presents the API for this gateway and is a guide for developing or customizing an application to integrate with it.

Scope

The **KeyManagement** gateway provides an API for extracting the SmartPoint module's encryption keys to perform field operations.

Target audience

The target audience is software integration engineers who are developing a customized web service client to extract the encryption keys.

Terminology

Word or Phrase	Definition
Field Tool (FT)	Device used in the field to send and receive information to and from an endpoint. Examples include Hand Held Device (HHD), FlexNet Micro Transceiver (FMT), ANSI Optical probe, serial MagLoop, etc.
DB	Database – currently both MS SQL and Oracle databases are supported.
Endpoint (EP)	Any FlexNet enabled device: meter, HAN device, etc.
FlexNetID	A unique identifier found in each endpoint. The FlexNet ID is guaranteed to be unique across all Sensus transceivers.
MeterID	An endpoint identifier that is unique within the customer domain and service type, but not guaranteed to be globally unique.
RNI	Regional Network Interface – A set of servers that connects the RF Meter network to external systems. Comprises five servers: Network Controller (NC), Database (DB), Web, Stats, and Map Server. Also includes an LDAP service hosted on one of the servers.
FlexNet Crypto Engine (FCE)	A service inside the RNI that manages and processes encryption keys.
SOAP	A data format for communicating with web services. Usually used with the HTTP protocol as a transport.
Web service	A collection of related web methods.
Web method	An operation that can be invoked remotely.

Notation

The conventions used in this document are as follows:

- Mandatory parts of the SOAP requests and responses are denoted in bold font and marked with an asterisk (e.g., **UserID***).
- *Italics* are used for emphasis.
- Highlights are used (sparingly) for statements of high importance.
- The `Consolas` font is used for proper nouns in the RNI system (i.e., words that must be typed as shown wherever applicable).

General considerations

The general considerations discussed in the following sections include web service protocols, security, and error reporting.

Web service protocols

The **KeyManagement** gateway supports SOAP 1.1 over HTTPS. Support for HTTPS is through the Apache reverse proxy in the RNI. The WSDL and Schema (.xsd) files required to use the service may be obtained upon request from Xylem/Sensus.

Security

Privacy

- The web service implementation does not support encryption in the SOAP payload. It relies on transport security (i.e., TLS) to guard against eavesdropping.

Authentication

- Supports per-request basic authentication as defined in the MultiSpeak message header.
-

Authorization

The user accessing the service must have a role assigned that is granted the permission “Key management, generate encryption files”.

Common security errors

Any authentication or authorization violations from processing a SOAP request result in a system error and cause entire request to fail. The following table shows the error messages returned in the SOAP fault.

	Error	Reasons
SYSTEM ERRORS	Userid and password are incorrect	The credentials provided in the request header are not valid.
	Userid and password attributes are not provided in the SOAP MsgHeader	The `UserId` and/or `Pwd` attributes are not provided in the SOAP MsgHeader. Authentication cannot proceed without these credentials.

Error reporting

Errors encountered during request processing are reported to the client through SOAP faults or error objects in the response.

SOAP fault

System and security errors are reported as SOAP faults and cause the entire request to fail.

Error object

Business errors are reported as error objects and do not cause the entire request to fail.

Customer ID

Since the RNI can be a shared management platform, each meterID or FlexNetID is resolved within the context of a customerID (a unique moniker for the utility that owns meters managed by the RNI). Thus, when any request or data for a meter is received, it must be identified by the (meterID or FlexNetID) + customerID tuple.

The following example shows a request with the `CustomerId` attribute.

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v1="http://www.sensus.com/keymanagementws/v1">
   <soapenv:Header>
      <v1:GetKeysRequestHeader UserID="testuser" Pwd="test123"
      SessionID="SSID1234"/>
   </soapenv:Header>
   <soapenv:Body>
      …
         <v1:MeterList>
            <!--Zero or more repetitions:-->
            <MeterRequest MeterId="1001M"
                          CustomerId="ACME"
                          ServiceType="Electric"
                          UniqueKey="true"/>
         </v1:MeterList>
      …
   </soapenv:Body>
</soapenv:Envelope>
```

The list of customer IDs associated with the authenticated (LDAP/AD) user should contain the `CustomerId` from the request.

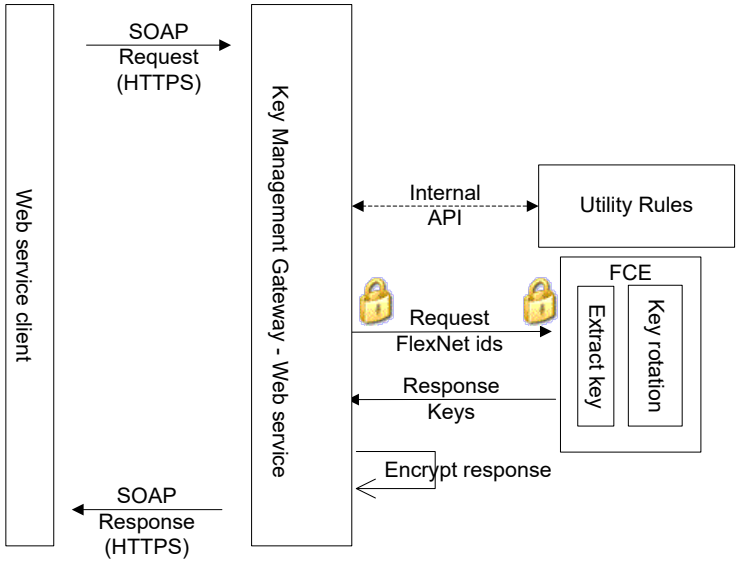
KeyManagement interface

Overview

The web service provides an Application Programming Interface (API) to extract encryption keys by meterID or FlexNetID. The web service process on the RNI/Gateway host executes as part of the FlexNet-gateway service.

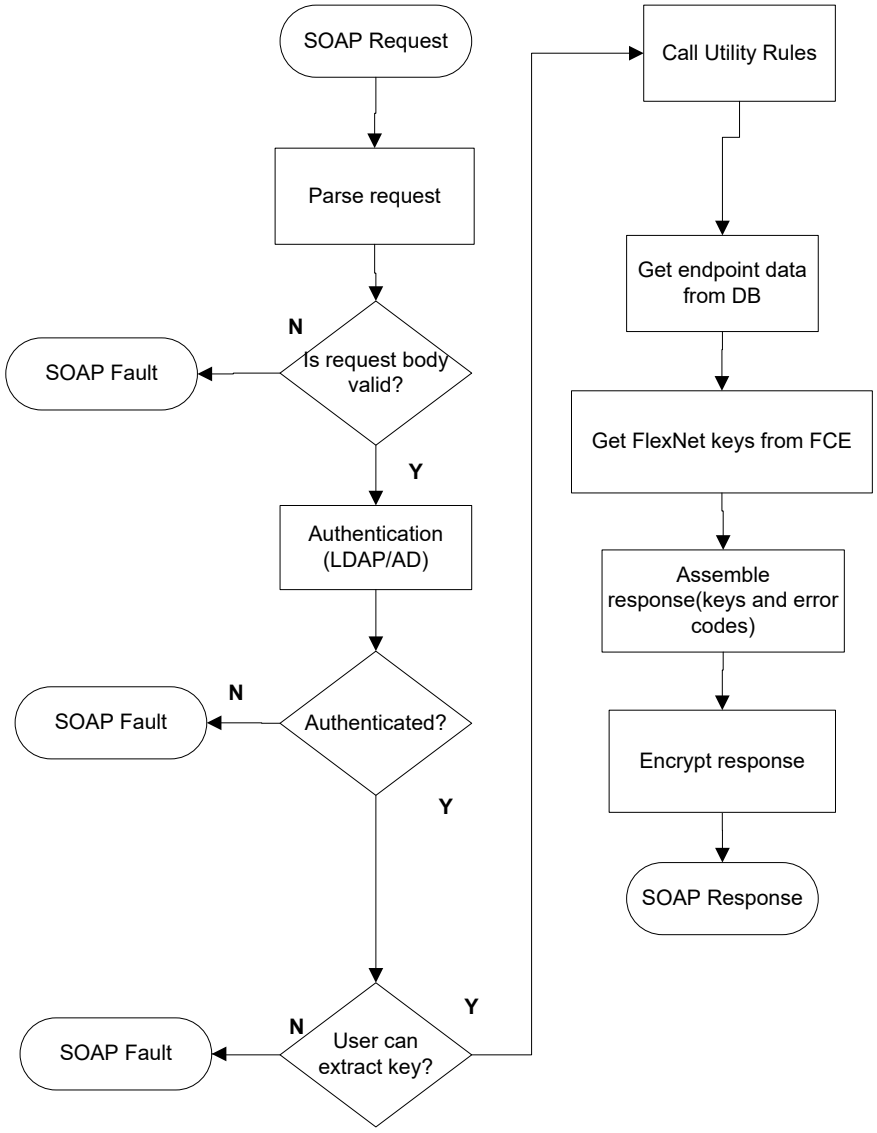
RNI component interaction

The following diagram shows key RNI components interaction.



Flow chart

This following image shows a flow chart for a generic operation in the KeyManagement web service.



Utility rules

The Utility Rules component provides the ability to apply business rules constraining the extraction of keys.

Currently, the only out-of-the-box rule is `MaximumKeysPerRequest` which limits the number of keys extracted per request. The maximum number of keys is a system-level setting defined by the `KeyManagement.MaximumKeyPerRequest` configuration property.

Web service methods

The web service provides two methods to extract encryption keys from the RNI, one by meterID (identifier for the meter) and the other by FlexNetID (identifier for the radio module on the meter).

External clients usually identify endpoints using meterID, while Sensus applications can use FlexNetID because they are aware of the radio. **Sensus recommends using meterID**.

Both methods send the encryption keys in a SOAP attachment. The content of the attachment is encrypted using AES-256.

The UserID in the request must be associated with the customerIDs of the requested meters and have the permission to extract keys. Otherwise, the request fails with a SOAP fault.

URL

The web service URL: https://<your gateway host name>/keymanagementws

GetKeys method

This web service method can be used to extract encryption keys by providing the FlexNetID.

Sample request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v1="http://www.sensus.com/keymanagementws/v1">
   <soapenv:Header>
      <v1:GetKeysRequestHeader UserID="testuser" Pwd="test123"
      SessionID="SES1234"/>
   </soapenv:Header>
   <soapenv:Body>
      <v1:GetKeysRequest>
         <v1:PassPhrase>test1234</v1:PassPhrase>
         <v1:includeSharedKey>true</v1:includeSharedKey>
         <v1:SmartPointRequestList>
            <!--Zero or more repetitions:-->
            <SmartPointRequest FlexNetId="2501" UniqueKey="true"/>
         </v1:SmartPointRequestList>
      </v1:GetKeysRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample response

Following is an example of a successful response with SOAP attachment, which contains the keys.

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <ns3:GetKeysResponse
      xmlns:ns3="http://www.sensus.com/keymanagementws/v1">
         <ns3:AuditInformation>
            <GeneratedBy>guestAdmin</GeneratedBy>
            <TimeGenerated>2010-10-19T16:02:47.165-04:00</TimeGenerated>
         </ns3:AuditInformation>
         <ns3:ErrorMessages/>
      </ns3:GetKeysResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

GetKeysByMeter method

This web service method can be used to extract encryption keys by providing the MeterID.

Sample request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v1="http://www.sensus.com/keymanagementws/v1">
   <soapenv:Header>
      <v1:GetKeysRequestHeader UserID="testuser" Pwd="test123"
      SessionID="SS1234"/>
   </soapenv:Header>
   <soapenv:Body>
      <v1:GetKeysRequestByMeter>
         <v1:PassPhrase>test1234</v1:PassPhrase>
         <v1:includeSharedKey>true</v1:includeSharedKey>
         <v1:MeterList>
            <!--Zero or more repetitions:-->
            <MeterRequest MeterId="1N6024013223" CustomerId="ACME"
            ServiceType="Electrical" UniqueKey="true"/>
         </v1:MeterList>
      </v1:GetKeysRequestByMeter>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample response

Following is the sample of a successful response with SOAP attachment, which contains the keys.

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <ns3:GetKeysResponse
      xmlns:ns3="http://www.sensus.com/keymanagementws/v1">
         <ns3:AuditInformation>
            <GeneratedBy>guestAdmin</GeneratedBy>
            <TimeGenerated>2010-10-19T16:02:47.165-04:00</TimeGenerated>
         </ns3:AuditInformation>
         <ns3:ErrorMessages/>
      </ns3:GetKeysResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Key extraction file

The responses to **GetKeys** and **GetKeysByMeter** both include a SOAP attachment.

MIME headers

Content-ID: FlexnetKeyResponse

Content-Type: text/plain

Format

The key extraction file may be in DAT or JSON format, depending on the version of RNI that you are using.

DAT format

The DAT format for key extraction is not human-readable, and it's a file format generated by RNI versions 4.12 and earlier. It is used by FieldLogic versions earlier than 7.5. This type of key extraction file has two logical sections—a global data section and an endpoint section.

Global data

This section starts with the tag `[Info]` followed by properties that are common to the entire response:

- **ExpirationDate** – This is in Epoch Time. The default value is 0 (i.e., never expire).
- **Shared** – The shared key, if requested.
- **PreviousShared** – The previous shared key, if the shared key was requested and a rotation is in progress.
- **CBCMACVerification** – Boolean value indicating whether cipher block chaining message authentication code verification is enabled. The default value is false.
- **RotateUniqueKeyAllowed** – Boolean value indicating whether unique key rotation is allowed. The default value is true.

Endpoint data

The global data section is followed by a series of endpoint data sections, each of them starting with a `[<FlexNetID>]` tag, for example, [612334234], and then the following properties corresponding to that endpoint:

- **Encrypted** – Boolean value indicating whether the endpoint is encrypted.
- **Unique** – The unique key for the endpoint. This is provided if available, even if the endpoint is not currently encrypted.
- **PreviousUnique** – The previous unique key if a rotation is in progress.
- **HAN** – The HAN key, if requested and applicable. If not supported, this property is always empty.

JSON format

The JSON format for key extraction is human-readable, and it's the default file format generated by RNI versions 4.13 and later. It is used by FieldLogic 7.5 and later. This type of key extraction file has two sections—the required header section and the tenant keys section.

Required header section

This section contains basic information that is not specific to the tenant or endpoint's encryption data. Following are the fields for this section:

- FileFormatVersion – This is the version of the file format. Currently the only applicable value is 1.
- CreationDate – The date that the file was created.
- ExpirationDate – The date that the file expires.
- CreatedBy – The user that created the file.
- Encryption – The encryption method used. Currently the only applicable value is PBE_AES256_GCM.
- Authentication – The authentication method used. Currently the only applicable value is HMAC_SHA256.

- Salt – A randomly generated hex string used as the salt for encryption. This ensures that each file generated is different even when the encryption data extracted is the same.
- Nonce –Currently not used. For future development.
- SignHash – Currently not used. For future development.
- RecipHash – Currently not used. For future development.

Tenant keys section

This section contains specific encryption data that is tenant-wide or endpoint-specific.

- TenantId – The ID of the tenant.
- TenantSharedKeys – This section contains the tenant shared keys, signed suspend command, whether CBCMACVerification is set, and whether RotateUniqueKeyAllowed is set.
- TData_Body – This section contains the encrypted unique keys and previous unique keys.

Other information

File authentication is added to prevent unauthorized users from modifying the encrypted data. The filename contains 24 hexadecimal characters enclosed in brackets and looks similar to Keys[0123456789ABCDEF01234567].json.

For earlier versions of FieldLogic, the RNI can be temporarily configured to use the old key export file format (DAT format) until all field tools have been upgraded to FieldLogic 7.5. However, this functionality will be removed in a future version of RNI.

To revert the RNI to using the older file format, the RNI administrator needs to add the following to flexnet.local.properties and then restart tgblistener:

fce.extractKeyFormatVersion=0

This generates the key export file in the original DAT file format instead of the new JSON file format.

Xylem |'zīləm|

1) The tissue in plants that brings water upward from the roots;

2) a leading global water technology company.

We're a global team unified in a common purpose: creating advanced technology solutions to the world's water challenges. Developing new technologies that will improve the way water is used, conserved, and re-used in the future is central to our work. Our products and services move, treat, analyze, monitor and return water to the environment, in public utility, industrial, residential and commercial building services settings. Xylem also provides a leading portfolio of smart metering, network technologies and advanced analytics solutions for water, electric and gas utilities. In more than 150 countries, we have strong, long-standing relationships with customers who know us for our powerful combination of leading product brands and applications expertise with a strong focus on developing comprehensive, sustainable solutions.

For more information on how Xylem can help you, go to www.xylem.com

xylem

Sensus
637 Davis Drive
Morrisville, NC 27560
Tel +1.800.638.3748
www.sensus.com