SMART METER TEXAS

In-Home Device Guide

Table of Contents

Figures and Tables

1. Executive Summary

1.1 Purpose of the Document

The Smart Meter Texas (SMT) In-Home Device Guide is the primary In-Home Device document for the Texas market participants in territories covered by American Electric Power (AEP), CenterPoint Energy (CNP), Texas New Mexico Power (TNMP) and Oncor Electric Delivery. This document is a consolidation of all relevant In-Home Device documents and artifacts developed for the Texas market participants, and will be used as main source of information regarding the processes involved with the SMT In-Home Device implementation. As a "living" document, it will continually evolve based on upgrades to the SMT functionalities.

The aim of this In-Home Device Guide is to help the Texas market participants gain better understanding of the HAN functionalities, as well as the capabilities that are available to them within the SMT portal. Other items covered in detail are the In-Home Device Application Programming Interfaces (API) and the technical processes associated with in integrating In-Home Device systems with Smart Meter Texas.

This document does not cover the registration of Third-Party Service Providers (Third-Parties) nor the initiation of In-Home Device related customer agreements, which are the prerequisite requirements for Third-Parties to gain access to their customers' In-Home Devices.

1.2 Quick Reference

This In-Home Device Guide covers In-Home Device functions that are supported by SMT only. The following is a quick reference for the Texas market participants to locate the information:

Topics	Interested Party	Sections
In-Home Device functionalities supported via the SMT User Interface	Business Analysts	Sections 2, 3 and 4
In-Home Device Messaging Report	Technical Analysts, Business Analysts	Section 4
In-Home Device functionalities supported via Application Programming Interface (API)	Technical Analysts, Business Analysts	Sections 5 and 6
In-Home Device Messaging	Technical Analysts, Business Analysts	Section 5
In-Home Device Addressing of Messages	Technical Analysts, Business Analysts	Section 5
Examples of In-Home Device Messaging	Technical Analysts, Business Analysts	Section 5
How to Integrate with SMT (In-Home Device Integration with SMT)	DataPower / API Technical Integration Team	Section 6
Technical Requirements to Interface with SMT	DataPower / API Technical Integration Team	Section 7

Topics	Interested Party	Sections
Technical Requirements and Details on Authentication and Authorization	DataPower / API Technical Integration Team	Section 8
In-Home Device Testing with TDSPs	REPs of Records / In-Home Device Vendors	Section 9, Section 10
In-Home Device Interoperability Report	All Market Participants	Section 9, Section 10
In-Home Device Reprovisioning during Meter Exchange	All Market Participants	Section 11
In-Home Device Project Assumptions	Business Analysts	Section 12
Glossary of Terms	All Market Participants	Section 12

Table 1: Smart Meter Texas (SMT) In Home Device Guide Quick Reference

Section 2: TDSP Account Management – In-Home Device Permissions Functional Specification

This section is applicable to TDSP Administrators only. The In-Home Device Account Management describes how In-Home Device permissions are granted or revoked to their companies' users in the Portal. The In-Home Device Account Management functions can be performed via the SMT user interface.

Section 3: TDSP In-Home Device Provisioning Functional Specification

This section is applicable to TDSP Administrators and their authorized users with In-Home Device permission only. It describes how to add and remove In-Home Devices via the SMT user interface. The In-Home Provisioning processes describe how authorized users provision and deprovision In-Home Devices through the Portal. They also describe how authorized users are able to view In-Home Device provisioning information and In-Home Device history. In addition, this section explains how the Portal handles the different statuses of an In-Home Device throughout the provisioning process.

Section 4: In-Home Device Messaging Functional Specifications

This section describes the user interface which allows authorized users to retrieve message acknowledgments (message log) for a particular message type, Data Universal Numbering System (DUNS) and message creation date. This is the only In-Home Device Messaging function that can be performed via the SMT user interface.

Section 5: In-Home Device API Provisioning and In-Home Device API Messaging

This section lists and explains the following In-Home Device APIs that are available in SMT.

- In-Home Device Provisioning / Deprovisioning
- In-Home Device Utility Enrollment Group
- In-Home Device Messaging which includes:
  - Sending price signal
  - Sending simple text message
  - Cancel simple text message
  - Sending Load control event

- Cancel a Load control event
- Cancel all Load control events

Examples of In-Home Device Messaging APIs are provided for the following In-Home Device functions:

- sending a price signal,
- sending a simple text/display message,
- load control temperature setpoint,
- load control temperature offset, duty cycle, and update Utility Enrollment Group.

The addressing schemes will be discussed and explained in detail in this section. It explains the different addressing schemes that are available in SMT and how the users can send an In-Home Device message via point-to-point messaging or group messaging. The ESIID list and the GroupID list are discussed and examples of addressing are provided.

Section 6: In-Home Device API Starter Kit

This section provides the details of the In-Home Device API Starter Kit. The starter kit is a tool developed by SMT to help the Third-Party Service Providers integrate their In-Home Device function with SMT. The tool is based on soapUI and it can be utilized for the creation of In-Home Device APIs and allow users to edit the XML documents of the In-Home Device APIs.

The section will explain the process for how to request the Webservice description language (WSDL) files. After the Third-Party Service Providers integrated with SMT using the In-Home Device API Starter Kit, the WSDL files for In-Home Device related services will be provided by SMT upon request. These files can be utilized to build client applications to consume the SMT services for In-Home Devices.

Section 7: SMT In-Home Device Interface Security

This section describes Smart Meter Texas (SMT) interface security requirements necessary for In-Home Device API Starter Kit configuration set-up. It includes technical details required on API requests from the TDSP (i.e. user credential in SAML token that is part of SOAP header), and API requests from the Third-Party Service Providers (i.e. user credential passed in a UserName Token that is part of SOAP header). It also includes SMT requirements for CA issued certificates (SSL and Signer Cert) in its production environment.

Section 8: In-Home Device API Authentication and Authorization

This section discusses how the API authentication and authorization will be handled when direct web service request is made by the Third-Party Service Providers to Smart Meter Texas Portal (SMT) Enterprise Service Bus. Clients who communicate with SMT using the In-Home Device web service interface must support mutual authentication over SSL. DataPower and Tivoli components will authenticate users. Authorization is enforced by the SMT integration environment.

Section 9 and 10: In-Home Device Testing and Texas In-Home Device Test Report

Third-Party Service Providers and In-Home Device vendors should contact the TDSPs to initiate requests to perform In-Home Device testing.

This section discusses the TDSP processes in place to support In-Home Device Testing with Third-Party Service Providers and In-Home Device vendors. It describes the standardized method of testing and verifying In-Home Device functionality to ensure that In-Home Devices function as designed within the specifications detailed in the Smart Energy Profile 1.0 when operated on TDSPs AMS network.

The In-Home Device test cases that are executed during the ZigFesTx interoperability events are the basis of the test cases executed by the TDSPs in their In-Home Device validation program. Some TDSPs may have more test cases, and some have less, but all are based on the ZigFest test cases.

The Texas market ZigFests (i.e. ZigFesTx) are designed to give In-Home Device vendors access to production meters for Smart Energy Profile (SEP) 1.0 in-Home Device testing. It is open to any ZigBee member.

Section 11: In-Home Device Reprovisioning During Meter Exchange

This section describes how the In-Home Devices are reprovisioned to the new meter during the meter exchange process. The processes and procedures that the TDSPs perform during the meter exchange process are TDSP-specific, and these internal processes can affect the processing time on when the In-Home Devices are displayed in the new meter in the Smart Meter Texas portal.

Section 12: Appendices

This section lists the project assumptions and glossary of terms.

1.3 Available SMT In-Home Device Functions

Following are lists of available SMT In-Home Device functions accessible to different SMT Account types via User Interface (UI) or Application Programming Interface (API).

In-Home Device User Interfaces	Accessible To		
	TDSP	3rd Party*	Customer
Account Management (TDSP Admin Only)			
Grant In-Home Device Access	Yes	Yes	
Revoke In-Home Device Access	Yes	Yes	
Provisioning / Deprovisioning			
View Provisioning Status	Yes	Yes	Yes
Provisioning (add)	yes	Yes	Yes
Deprovisioning (remove)	Yes	Yes	Yes
Messaging			
View and Request Messaging History		Yes	

Table 2: List of In-Home Device Functions available in User Interface (UI)

In-Home Device API	Accessible To		
	TDSP	3rd Party*	Customer
Provisioning / Deprovisioning / UEG			
Provisioning (add)	Yes	Yes	

In-Home Device API	Accessible To		
	TDSP	3rd Party*	Customer
Deprovisioning (remove)	Yes	Yes	
Update Utility Enrollment Group (UEG) **		Yes	
Messaging			
Send Price Signal	Yes	Yes	
Send Simple Text/Display	Yes	Yes	
Cancel Simple Text/Display	Yes	Yes	
Send Load Control Event	Yes	Yes	
Cancel Load Control Event	Yes	Yes	
Cancel All Load Control Events	Yes	Yes	

Table 3: List of In-Home Device Functions available in Application Programming Interface (API)

Note*: Third-Party Service Providers require an Active In-Home Device Customer Agreement to perform these functions.

Note**: Before using the 'Update Utility Enrollment Group' function, you should verify with the TDSP and In-Home Device manufacturer if they support this functionality. Per SEP 1.0, the UEG function is available to In-Home Device / Load Control Devices that support the DRLC cluster.

Registered SMT customers (residential and non-residential) have the ability to provision (add) and deprovision (remove) their In-Home Devices via the SMT Portal User Interface. Refer to the Smart Meter Texas Customer user Guide for detailed step-by-step instructions how to add and remove an In-Home Device.

TDSPs have the ability to provision (add) and deprovision (remove) In-Home Devices via the SMT Portal User Interface and APIs.

Registered Third Party Service Providers have the ability to perform the following In-Home Device functions on Smart Meters associated with active In-Home Device related Customer Agreements:

- Provision (add) and Deprovision (remove) In-Home Device via the SMT User Interface and API
- Send Utility Enrollment Group via In-Home Device API
- Send Simple Text Message via In-Home Device API
- Send Pricing Message via the In-Home Device API
- Send Load Control Message via the In-Home Device API
- Request In-Home Device Status (Provision and Deprovision) Report API
- Request Messaging History Report via the SMT Portal User Interface

2. TDSP Account Management – In-Home Device Permissions Functional Specification

This section provides the business rules and the process description of granting or revoking In-Home Device Permissions via the SMT Portal.

NOTE: This section is applicable to TDSP Administrators only.

2.1 Business Rules

These are the In-Home Device Access Business Rules of the original Smart Meter Texas release and they are applicable to TDSP only.

Business Rules	
General Business Rules	
1	TDSP possesses the In-Home Device Rights for the ESI IDs under its DUNS.
2	TDSP administrators are granted all In-Home Device Rights automatically: View Provisioning Status, Provisioning, and Deprovisioning.
3	TDSP administrators can grant and revoke In-Home Device rights to TDSP users.
4	Account management is performed via portal screens.

Table 4: TDSP Account Management – In-Home Device Permissions Business Rules

2.2 User Experience

The following user interface allows TDSP Administrators to grant or revoke their users' In-Home Device Access permission.

2.2.1 UI-2.11.3.c User Account Details (View) - TDSP Only

Figure 1 is the user interface for TDSP Administrators to grant or revoke their users' In-Home Device Access Permission.

NOTE: Refer to the Smart Meter Texas (SMT) TDSP User Guide for step-by-step instructions on how to navigate to this user interface.

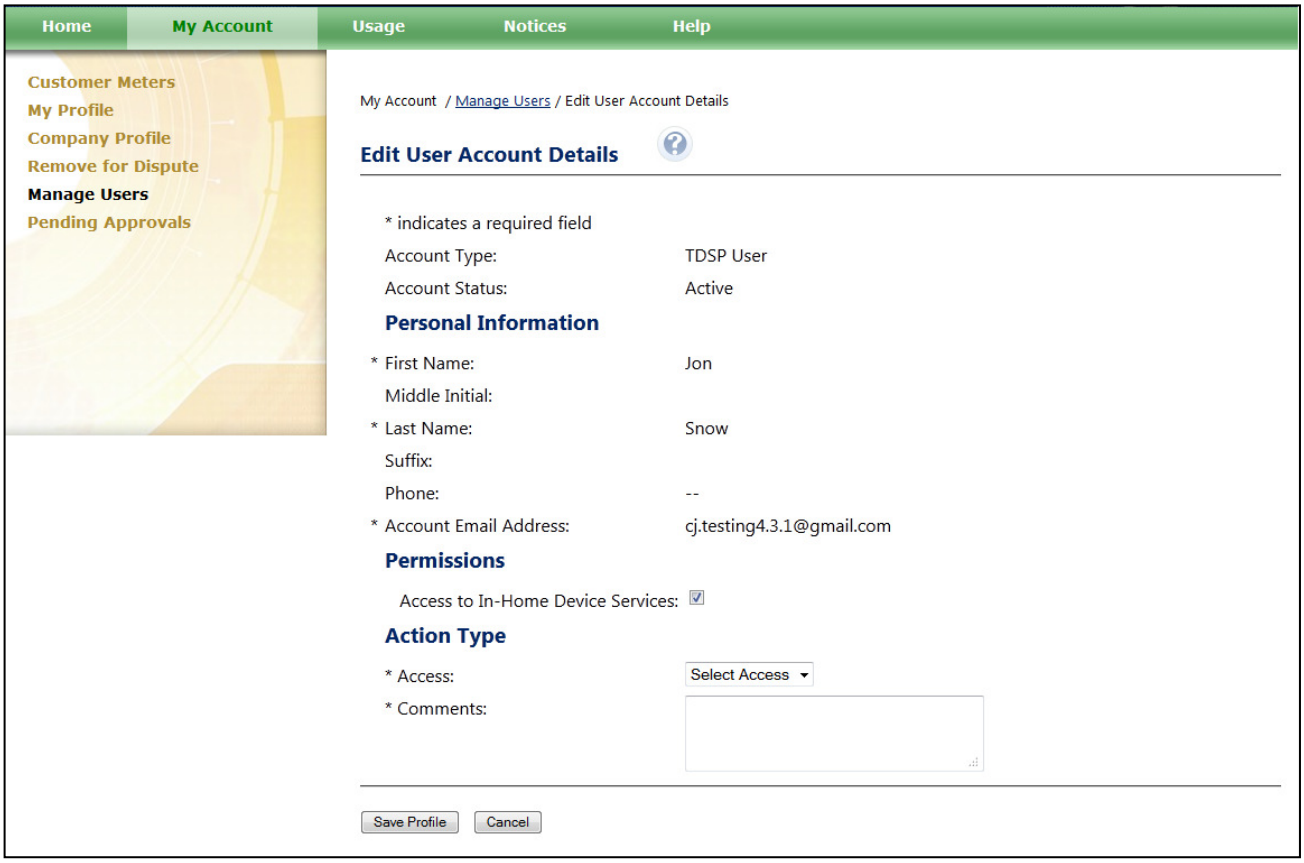


Figure 1: UI-2.11.3.c User Account Details (View) – TDSP

2.3 Process Flow Diagrams

2.3.1 Grant In-Home Device Access Process Flow

Here are the detailed process steps as shown in Figure 2: Grant In-Home Device Access (TDSP Only) Process Flow.

010. Enter Portal through Private URL

020. Navigate to My Account

030. User Action?

[N1] Authorized Meter, My Profile and Company Profile, go to 2.0 Account Management Processes

[N2] A TDSP Admin can grant In-Home Device Access to new users or existing users

[A1] Manage Users: Admin selects this link to grant access to an existing user

[A2] Pending Approval: Admin selects this link to grant access to new users

Note: 2.0 Account Management Processes is not shown but it pertains to managing user account and company profiles

040. Display Search Screen

050. Display List of users pending for approval

060. Select a particular user

070. Conduct Search

080. Display Search Results

090. Select a particular user

100. Display User Account Details Screen

110. Check the 'Access to In-Home Device Services' Control box

[N1] TDSPs can only provision, deprovision (it is implicit here that granting In-Home Device Access concedes the right to view provisioning status which applies for both user types)

120. Enable View, Provisioning, Deprovisioning Rights

[N1] This means that for this user the button View In-Home Devices in the Search Screen under my Account is enabled

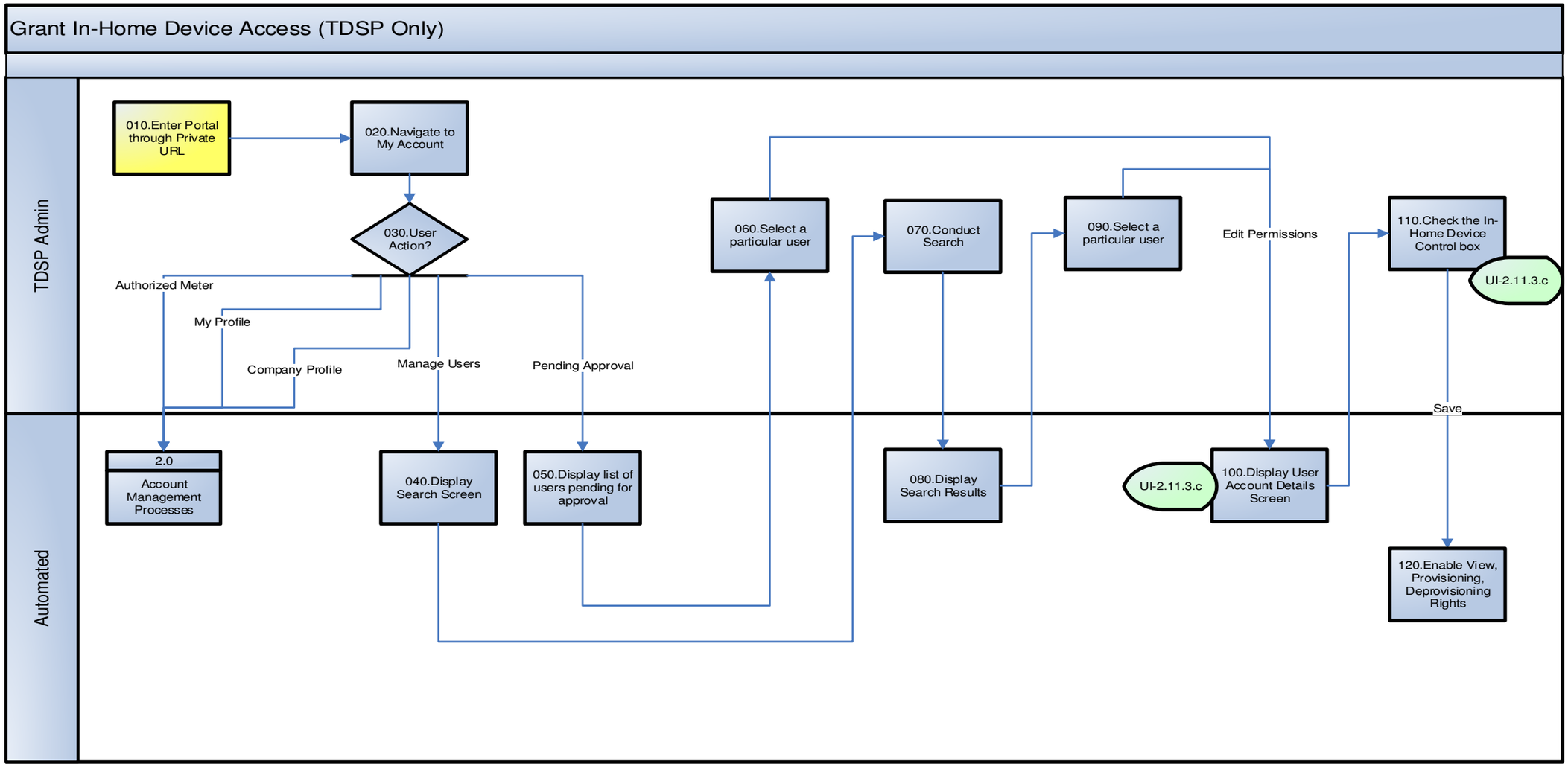


Figure 2: Grant In-Home Device Access (TDSP Only) Process Flow

2.3.2 Revoke In-Home Device Access Process Flow

Here are the detail process steps as shown in Figure 3: Revoke In-Home Device Access (TDSP Only) Process Flow.

010. Enter Portal through Private URL

020. Navigate to My Account

030. User Action?

[N1] Authorized Meter, My Profile, Company Profile and Pending Approval, go to 2.0 Account Management Processes

[N2] TDSP Admin can revoke In-Home Device Access only to existing users

[A1] Manage Users: Admin selects this link to revoke access to an existing user

Note: 2.0 Account Management Processes is not shown but it pertains to managing user account and company profiles

040. Display Search Screen

050. Conduct Search

060. Display Search Results

070. Select a particular user

080. Display User Account Details Screen

090. Uncheck the 'Access to In-Home Device Services' Control box

[N1] TDSPs can only provision and deprovision (it is implicit here that granting In-Home Device Rights concedes the right to view provisioning status which applies for both user types)

100. Disable User's In-Home Device Rights

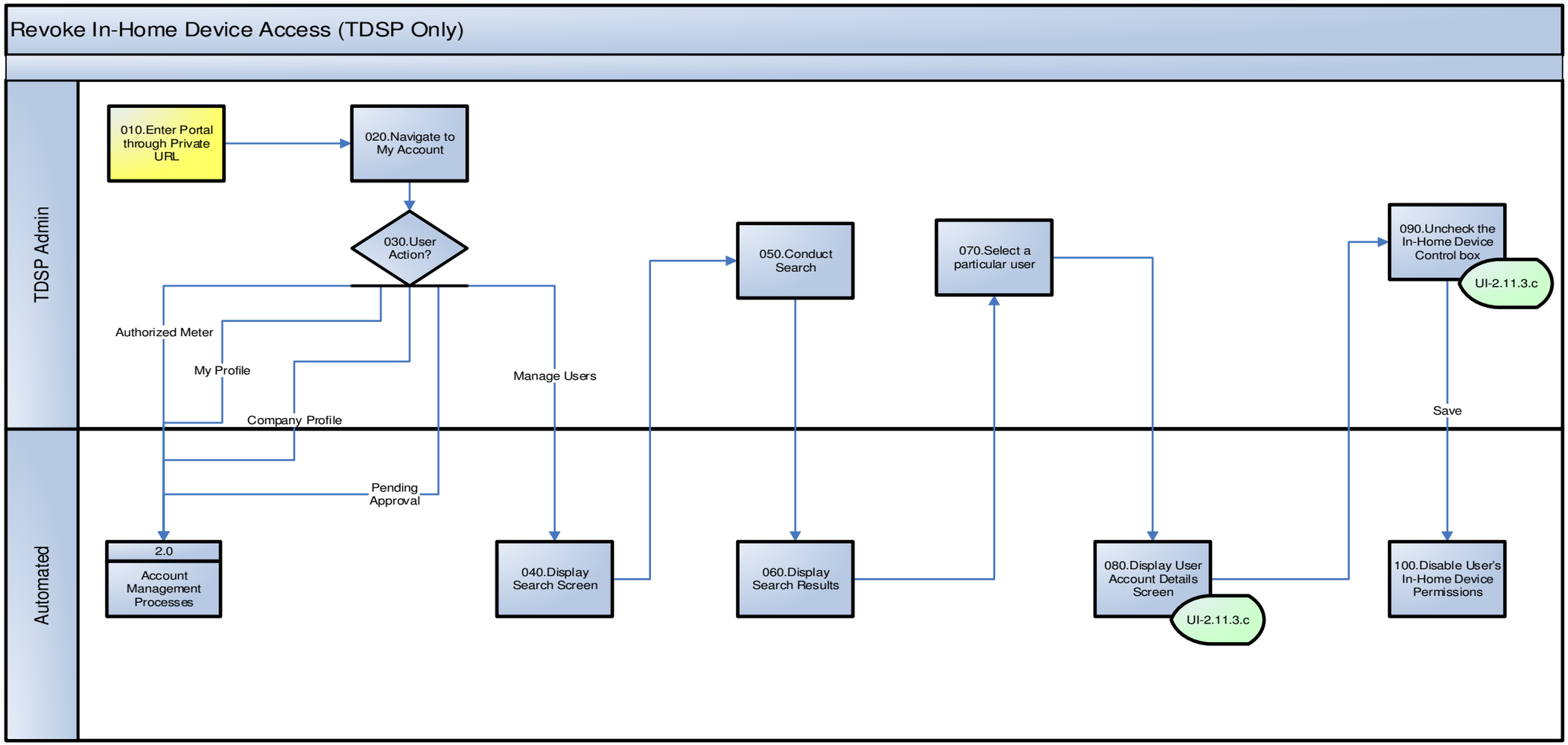


Figure 3: Revoke In-Home Device Access (TDSP Only) Process Flow

3. TDSP In-Home Device Provisioning Functional Specification

This section describes the process to provision (add) and deprovision (remove) In-Home Devices through the SMT Portal User Interfaces.

Authorized TDSP Users are able to provision (add) or deprovision (remove) In-Home Devices directly to customers' Smart Meters without the need to establish an In-Home Device Agreement with the customer.

Authorized Third-Party and REP Users need to establish an In-Home Device Agreement with customers in order to provision (add) In-Home Devices. They can only re-provision (re-add) or deprovision (remove) the devices associated with their Customer Agreements.

3.1 Business Rules

These are In-Home Device Provisioning Business Rules applicable to TDSP only.

Business Rules	
General Business Rules	
1	A meter can support a maximum of 5 slots
2	MAC address and Install Code will be displayed on the Portal
3	A device cannot be provisioned to the same meter (ESI ID) a second time
4	A device will be deprovisioned when there is a customer move-out but will remain provisioned when there is a ROR switch
5	Slots cannot be reserved for future provisioning
6	There is not a provisioning request expiration period. Devices in status provision request accepted, pending provisioning or meter ready will maintain that status until an authorized user manually deprovisions the device
7	All provisioning related time-stamps will be available online (through the UI) as long as an In-Home Device is provisioned (and kept through meter exchange)
8	TDSP Authorized Users have access to View provisioned devices, View provisioning details (MAC Address, Install Code, and Date-Time stamps for the different provisioning statuses) and View History of Provisioned Devices (a consolidated view of the details for devices that are provisioned or devices that were deprovisioned during the last 13 months)
9	Customers (Residential and Non-Residential) have access to View provisioned devices, View provisioning details and View History of Provisioned Devices
10	TDSP can deprovision any device under the ESI IDs he has access to, regardless of who provisioned it
11	TDSPs have to provide a reason code when deprovisioning a device
12	Deprovisioned devices and related time-stamps will be displayed online for 13 months after a HAN Device is deprovisioned

Table 5: In-Home Device Provisioning Business Rules

3.2 User Experience and SMT Procedures

Only the Administrators and authorized users of the TDSP may perform the following functions via the SMT Portal:

- Add (provision) In-Home Devices
- Remove (de-provision) In-Home Devices
- View In-Home Device Details
- View In-Home Device History
- View 3rd Party Agreements

The table below provides the document to the SMT TDSP User Guide for step-by-step procedures to navigate through these functions.

Topics	Refer to Document
Add In-Home Devices	SMT TDSP User Guide Section 9.2 Adding In-Home Devices
Remove In-Home Devices	SMT TDSP User Guide Section 9.3 Removing In-Home Devices
View In-Home Device Details	SMT TDSP User Guide Section 9.4 Viewing In-Home Device Details
View In-Home Device History	SMT TDSP User Guide Section 9.5 Viewing In-Home Device History
View Third-Party In-Home Device related Agreements	SMT TDSP User Guide Section 9.6 Viewing Third-Party Agreements
In-Home Device Messaging	SMT TDSP User Guide Section 9.7 Sending Messages to In-Home Devices

Table 6: In-Home Device Provisioning TDSP User Experience and SMT Procedures

3.3 Process Flow Diagrams

3.3.1 TDSP In-Home Device Provisioning Process Flow

Entry points:

From View Provisioning Status (Add an In-Home Device Button)

030. Display Provisioning Screen

040. Enter Device Information and Networking Details

[N1] This is the Install Code, MAC Address and Type of In-Home Device

[N2] Possible values for Type of In-Home Device:

- Unspecified
- In Home Display
- Load Control Device
- Programmable Thermostat
- Intelligent Gateway
- Home Plug Interface

050. Selection?

[A1] Add In-Home Device (Button is disable until user enters all required fields)

[A2] Cancel

080. Validate MAC Address and Install Code

[B1] Validations for MAC Address: Hexadecimal check - 0..1, A..F, a..f (only hex digits are allowed), No special characters ("." and "-" and spaces are also not allowed)

[B2] Manufacturer creates an install code for each individual device; these codes can be 48, 64, 96, or 128 bits in length

[B2] Regardless of code length, a 16-bit CRC value is appended to the end of the Installation code

090. MAC and IC Valid?

095. Display Error Message

[E1] The MAC Address or the Install Code is invalid, please revise your entries

100. Device already provisioned to that ESI ID?

[B1] A particular device with a particular combination of MAC Address and IC cannot be provisioned a second time to the same ESI ID.

110. Display Error Message

[E1] That Device is already provisioned to this ESI ID, you need to deprovision the device in order to reprovision

120. Allocate Slot/Update In-Home Device Main List – Set Device Status to Add Acknowledged

[N1] At this point the Portal Logs the provisioning activity at the user level

130. Update information on the In-Home Device Provisioning History Log

[N1] Every time a device changes its status the portal feeds the In-Home Device Provisioning History Log

140. Send Provisioning Request

[N1] Provisioning Request is sent to the corresponding TDSP

[N2] The Portal needs to add to the request the ESI ID and Meter Number

150. Receive Provisioning Request

160. Send Acknowledgment of Provisioning Request

180. TDSP In-Home Device Provisioning Process

[N1] TDSP External Process

190. Send Provisioning Status

200. Provisioning Status?

[N1] Depending on the provisioning status, the Portal will make the corresponding update:

[S1] Request Rejected

[S2] Pending *(This provisioning status is applicable to CNP only)*

[S3] Meter Ready

[S4] Provision Complete

[S5] Provision Failed

210. Clear Slot from In-Home Device Main List

[N1] When the request is rejected by the TDSP (it did not pass the TDSP validations), the device request should no longer appear on the Main List (it is not taking a slot), but it will now be displayed in the sub-screen according to step 270.

220. Update In-Home Device Main List- Set Device Status to Add Pending *(This provisioning status is applicable to CNP only)*

230. Update In-Home Device Main List- Set Device Status to Meter Ready

240. Update In-Home Device Main List- Set Device Status to Device Added

250. Before Meter Ready is received?

[Q1] Is the Provision Failed Message received before a Status of Meter Ready is received?

255. Ignore Failure Message, maintain Meter Ready Status

[N1] If the failure is received after meter ready the slot is still taken, so the Portal should ignore the message.

260. Clear Slot from In-Home Device Main List

[N1] When the provision failed massage is received before the meter ready status, the device request should no longer appear on the Main List (it is not taking a slot), but it will now be displayed in the sub-screen according to step 270.

270. List rejected/failed provisioning request in the In-Home Device List Sub-Screen

[N1] And also update information on the In-Home Device Provisioning History Log

[N2] The Statuses associated are:

-Add Rejected

-Add Failed

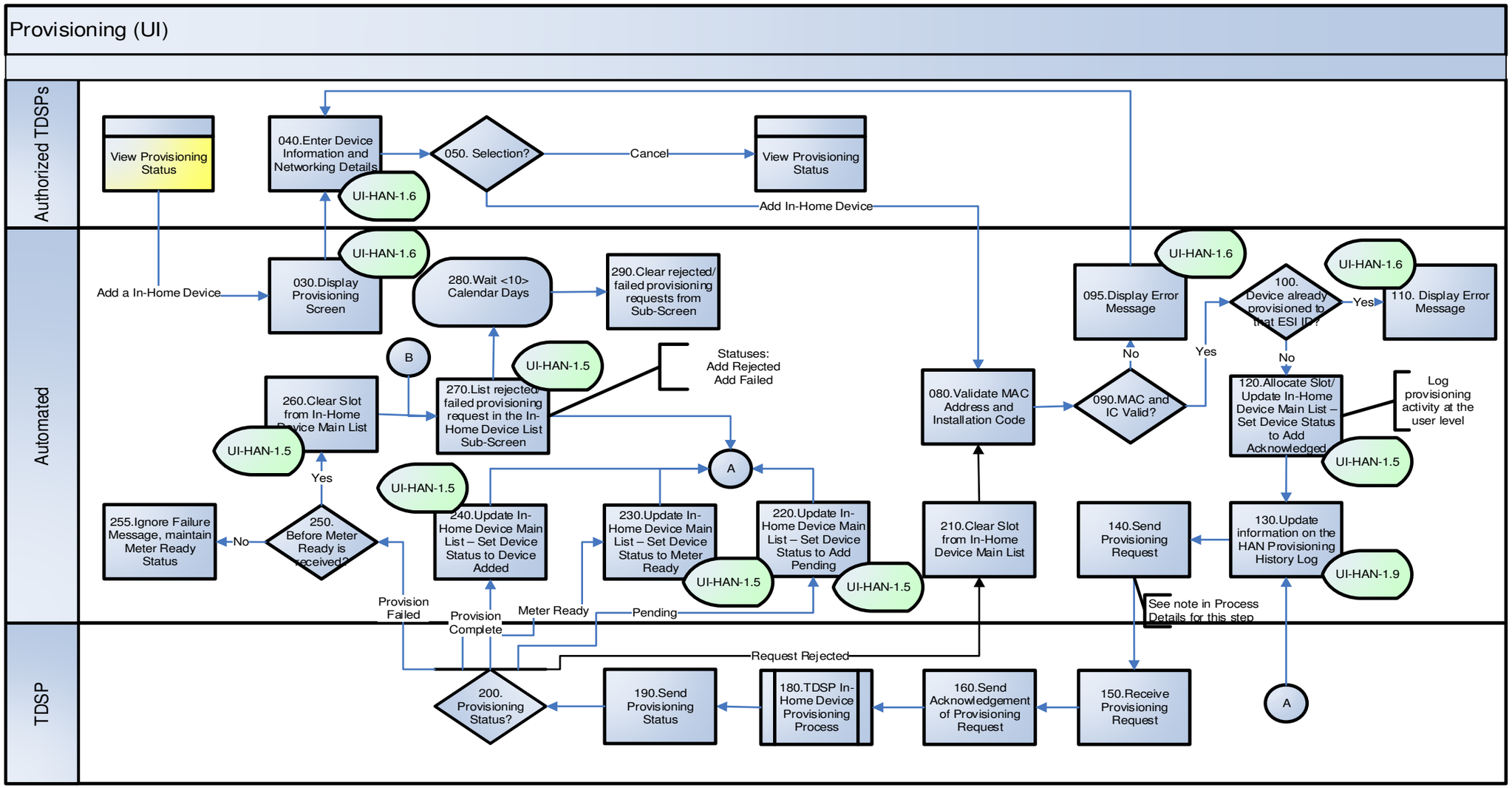
250. Wait <10> Calendar Days

[N1] Configurable period of time

260. Clear rejected/failed provisioned request from Sub-Screen

[N1] But information will remain in the In-Home Device Provisioning History Log

Figure 4: In-Home Device Provisioning Processes



Note: The *Pending* provisioning status is applicable to CNP only.

3.3.2 TDSP In-Home Device De-Provisioning Process Flow

Entry points:

From Provisioning/Deprovisioning process (Remove In-Home Device button)

010. Select Reason Code + Enter Optional Comments

[N1] User must select a reason code for deprovisioning

[N2] Possible Reason Codes differ based on User Type

For TDSPs the possible values are:

- REP Requested
- Customer Requested
- Malfunctioning Device
- Unsupported Device
- Request Add By Mistake
- Network Interference
- Other
- Customer Moving
- Customer No Longer Using the Device
- Troubleshooting / Problem Solving
- Make Room for a New Device
- Device No Longer Works

For REPs the possible values are:

- Customer Requested
- Malfunctioning Device
- Unsupported Device
- Request Add By Mistake
- Other

[N3] Comments are optional

[N4] Remove In-Home Device Button is disabled until user selects a reason code

040. Update In-Home Device List Screen – Set Device Status to Remove Acknowledged

[N1] Portal also logs deprovisioning activity at the user level

050. Update Information on the In-Home Device Provisioning History Log

060. Send Deprovisioning Request

[N1] With the deprovisioning request the Portal sends the ESI ID and Meter ID

070. Receive Deprovisioning Request

080. Send Acknowledgment of Provisioning Request

095. TDSP In-Home Deice Deprovisioning Process

100. Send Provisioning Status

110. Provisioning Status?

[S1] Request Rejected

[S2] Deprovisioning Pending *(This status is applicable to CNP only)*

[S2] Deprovision Failed

[S4] Deprovision Complete

120. Update In-Home Device List Screen – Set Device Status to Remove Pending *(This status is applicable to CNP only)*

130. Request Current Status Device to TDSP

[N1] Portal external process to query the TDSP and find out the correct status for that Device

135. List rejected/failed deprovisioned request in the In-Home Device List Sub-Screen / Update Status on Main Screen

[N1] Statuses would be:

-Remove Rejected

-Remove Failed

140. Clear Slot from In-Home Device Main List

150. List deprovisioned device in the In-Home Device List Sub-Screen

160. Wait <10> Calendar Days

170. Clear deprovision/failed deprovisioning devices from Sub-Screen

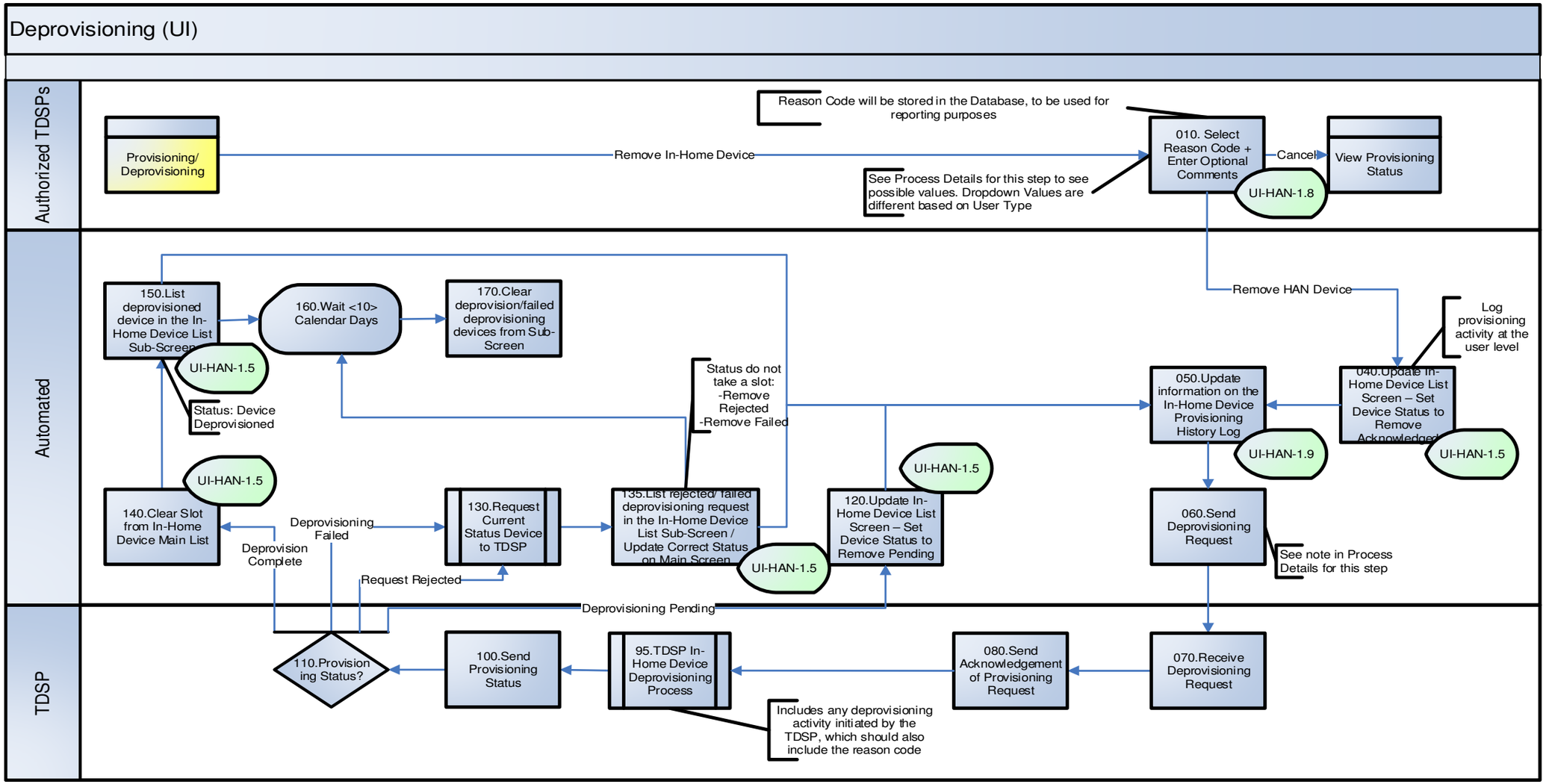


Figure 5: TDSP In-Home Device Deprovisioning Processes

Note: The *Pending* deprovisioning status is applicable to CNP only.

4. In-Home Device Messaging Functional Specifications

This section describes how an authorized user retrieves message acknowledgments (message log) from the SMT Portal user interfaces. The user interface allow users to filter the message log by the type of the message sent and the creation date of the message.

4.1 Business Rules

These are the Business Rules of the In-Home Device Messaging function in SMT.

Business Rules	
General Business Rules	
1	Third-Party Service Providers can send all types of messages through the API (display, load control, pricing)
2	The Third-Party will assign a message ID (32 bit) when they create a message. A particular Message ID could not have been used for the last 24 hours for the Portal to validate the request.
3	Third-Party Service Providers can cancel the messages they created. The Portal will not validate if the ESI IDs defined as original recipients still belong to this Third-Party Service Provider. The cancellation request will be sent to the TDSPs.
4	Message acknowledgment requests will always generate an asynchronous report

Table 7: In-Home Device Messaging Business Rules

NOTE: Rule #9 is the only business rule that applies to SMT Portal user interface. All the other business rules are applicable to the SMT APIs only.

4.2 User Experience and SMT Procedures

This section covers the user interfaces in the SMT Portal that allow the administrators and authorized users of the Third-Party Service Providers to request the In-Home Device Message Log report and to view the status of their message log report requests.

NOTE: the Report Request Status screen under the Usage tab shows all type of reports requested by the user, which includes both the In-Home Device Message Log Report request as well as Usage Report requests.

The table below provides the document to the SMT Third-Party User Guide for step-by-step procedures to navigate through these user interfaces.

Topics	Refer to Document
Request In-Home Device Message Log	SMT Third-Party User Guide Section 9.5 Requesting the In-Home Device Message Log

Table 8: Request In-Home Device Message Log Third-Party User Experience and SMT Procedure

4.3 Process Flow Diagrams

4.3.1 In-Home Device Messaging Processes – View Messaging Status

010. Enter Portal through Private URL

020. Navigate to My Account Tab/Land on Customer Meters

030. Select In-Home Devices Messages

040. Display Search Screen

050. Select Message Type (s)

[B1] User must select at least one message type in order to submit a request (user can select all message types)

060. Select DUNS (applicble to REPs acting as Third-Party only)

[B1] User must select at least one DUNS in order to submit a request (user can select all DUNS)

070. Select Date of Message

B1] User must select a Date of Message in order to submit a request

[N1] Submit Request button is disabled until user inputs all required fields (Message Type, DUNS, and Start Date)

100. Display Order ID Number with instructions to retrieve Log

[B1] Ad-hoc requests of data that will not be returned to the user in real time will always display an Order Number (ID)

[C1] The message to display will only contain a variable element: the X time. All other elements of the message will be static

[N1] The timing provided to the user at this time is an estimate. The message will also say that an e-mail will be sent once the request is complete

110. Add Report Request to Report Request Status Link on Usage Tab

[B1] The status of Ad-hoc requests of data with an Order Number will be displayed on the Portal

120. Process Data Request

[B1/C1] Processing of Ad-hoc Data Request is on a first come first served basis (no priorities assigned)

130. Publish Result File to FTP Site

[N1] Publish of the result file implies that in the Report Request Status Screen the request will be marked as complete

[B1] User will be able to download the report in CSV from the FTP site

140. Send e-mail to user that made request with Result File

[B1] A user that submits an ad-hoc request will receive an e-mail when the request is complete

[B2] The e-mail to the user will contain the result file requested, and a link to the page where the user can retrieve the report. The user will have to enter his User ID and Password to get authenticated

[M1] The report you requested is ready for retrieval. Click here to retrieve your report or go to the Report Request Status Link on the Usage Tab. You only have 10 calendar days to retrieve your report

150. Wait 10 days

[B1] Result Files will be available for download from the FTP site for up to 10 calendar days after the publish date

[B2] Status messages for unsuccessful requests will be kept for up to 10 calendar days after the publish date

160. Purge the Files/Status Messages

[N1] Result Files are no longer available for download. Status Messages are deleted. Complete and Unsuccessful requests are removed from the Report Request Status Screen

170. Wait for confirmation e-mail

180. Access Report Request Status Link on Usage Tab

[N1] Authenticated user accesses the Usage Tab and selects the Report Request Status Link

190. Display List of Requests

[B1] Portal displays the list of all requests submitted by the user in reverse chronological order. Date of Request is then one of the columns of the report and it contains day and time of the request in the following format: mm/dd/yy hh:mm:ss (24 hour clock)

[B2] Portal displays a maximum of 25 requests per page, user can page up or down to see the status of order requests

[B3] Requests are removed from the list 10 days after the publishing of the result (either successful or unsuccessful).

[B4] The list of requests displays the possible statuses for a request:

-Processing: the request is still processing

-Complete: means that there is some data available for download

-Unsuccessful: it means there is not data available for download (Specific error messages apply for situations). See step 550 for details

200. Status of Request?

[Q1] What is the status of the request?

210. Display processing message

[M1] Your request is being processed. You will receive an e-mail when your request is complete

220. Display Data Unavailable Message according to processing error

If there is no data available:

[E2] “Sorry, there is no data available for the date that you requested, please input a different date”

If there is some system error that prevents the portal from retrieving the data:

[E3] “Sorry, your request could not be processed, please try again later”

[B1] These error messages are displayed are displayed on the Report Request Status Link on the Usage Tab

230. 230.Display Link to FTP Site to access File

[B1] User will be able to download the result file by clicking on the link of the file

240. 240.Go to FTP Site to Access Result File

[N1] User downloads the result file in CSV

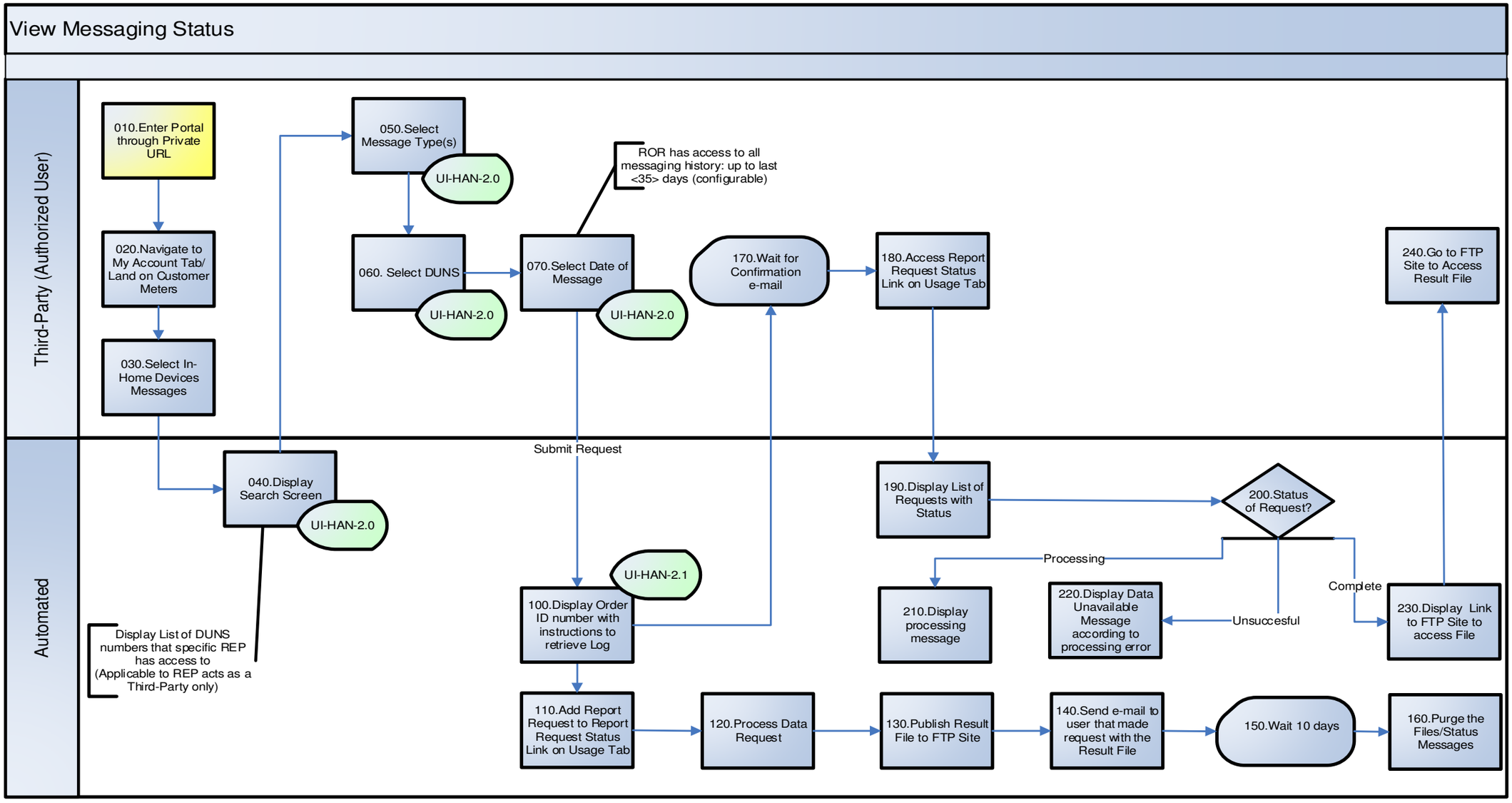


Figure 6: HAN Messaging Processes – View Messaging Status

4.4 File Formats

All files will be provided to the users in CSV format. We should be able to provide at least the fields marked as required

Element	Required	Description
TDSPDUNSNumber	Yes	DUNS Number
RequestID	No	Request ID generated by the Portal
MessageID	No	Message ID assigned by the REP
ESIID	Yes	
MeterSerialNumber	No	
DeviceMACAddr	No	Identifies the HAN Device if device-level status is available.
EventCategoryID	Yes	Allowed values are: STM - SimpleMessage CSM - CancelSimpleMessage LCE - LCEvent CLE - CancelLCEvent CAL - CancelAllLCEvents PRM - PriceMessage,
StatusCode	Yes	Allowed values are: RQA: Request Accepted and sent to TDSP ACK: Acknowledgment from TDSP that the message request has been received PEN – Pending CON – Confirmed STR – Request/Event Started OPT – Opt Out FLR – Failure SNT – Message Sent COM – Completed CAN – Canceled
StatusDesc	No	Additional status description text provided by the TDSP
StatusTimestamp	Yes	The timestamp for the status information. Ideally, this is the timestamp derived from the meter/ESI.

Table 9: In-Home Device Messaging Log – File Format

5. In-Home Device API Provisioning and In-Home Device API Messaging

5.1 SMT In-Home Device Interface Overview

Figure 7 presents the system context diagram for SMT with In-Home Device functionality highlighted.

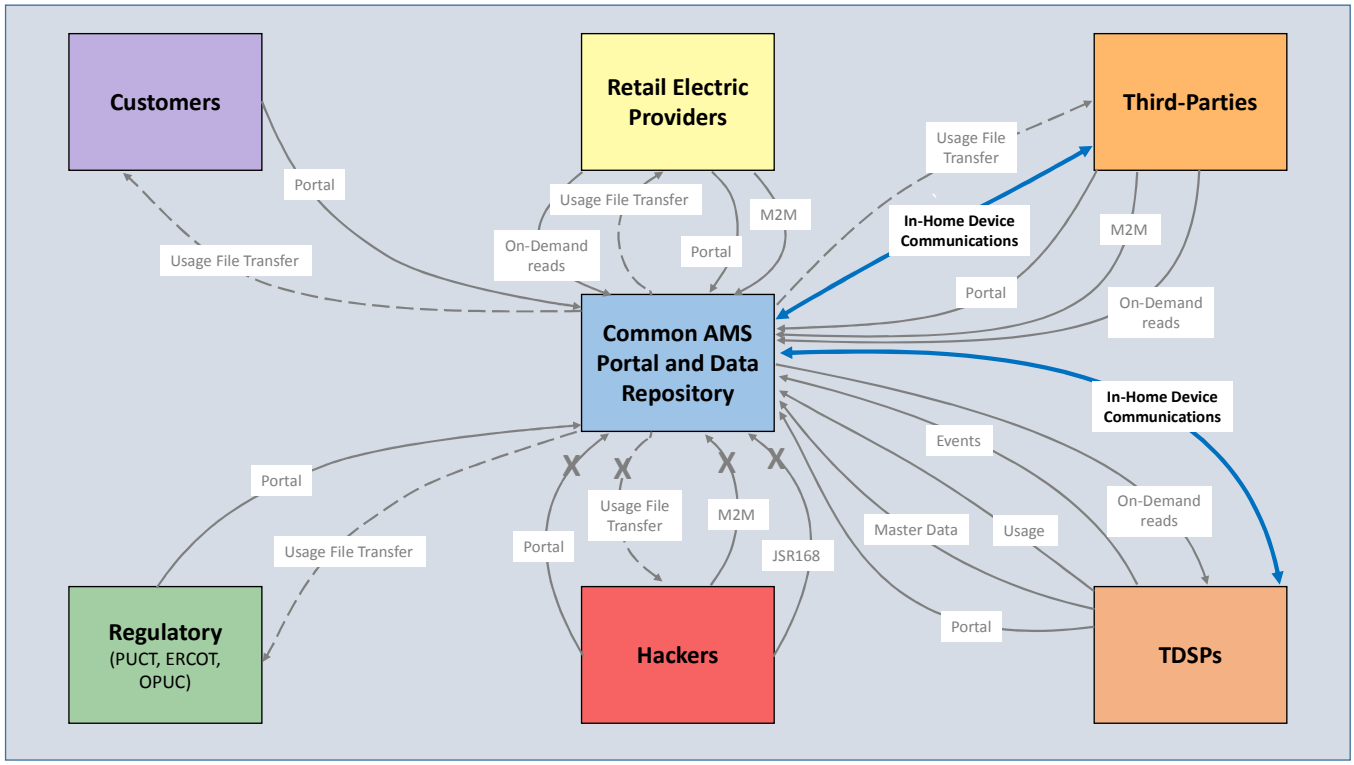


Figure 7: System context diagram with In-Home Device highlighted

SMT provides In-Home Device provisioning, deprovisioning and Smart Energy messaging functions via Application Programming Interfaces. SMT will perform validations of the requests and act as a pass-through to TDSP systems that implement In-Home Device functionality.

These interfaces (as well as front-end interfaces) may be used by the following types of requstors as of Release 4.3 of the project:

- Third-Parties
- REPs acting as a Third-Party

5.1.1 Interface Overview

Table 10 shows the set of In-Home Device interface requests, acknowledgements, status updates and responses. An interface number is associated with each type of message.

Interface Message Description	Response	Invocation Type
Provisioning HAN Device Request	Provision Request Acknowledgement	Synchronous
Deprovisioning HAN Device Request	Provision Request Acknowledgement	Synchronous
Simple Messaging Request	Messaging Request Acknowledgement	Synchronous
Cancel Simple Message Request	Messaging Request Acknowledgement	Synchronous
Load Control Messaging Request	Messaging Request Acknowledgement	Synchronous
Cancel Load Control Message Request	Messaging Request Acknowledgement	Synchronous
Cancel All Load Control Message Request	Messaging Request Acknowledgement	Synchronous
Price Signal Request	Messaging Request Acknowledgement	Synchronous
Update Enrollment Group Request	Messaging Request Acknowledgement	Synchronous

Table 10: List of SMT In-Home Device Interfaces

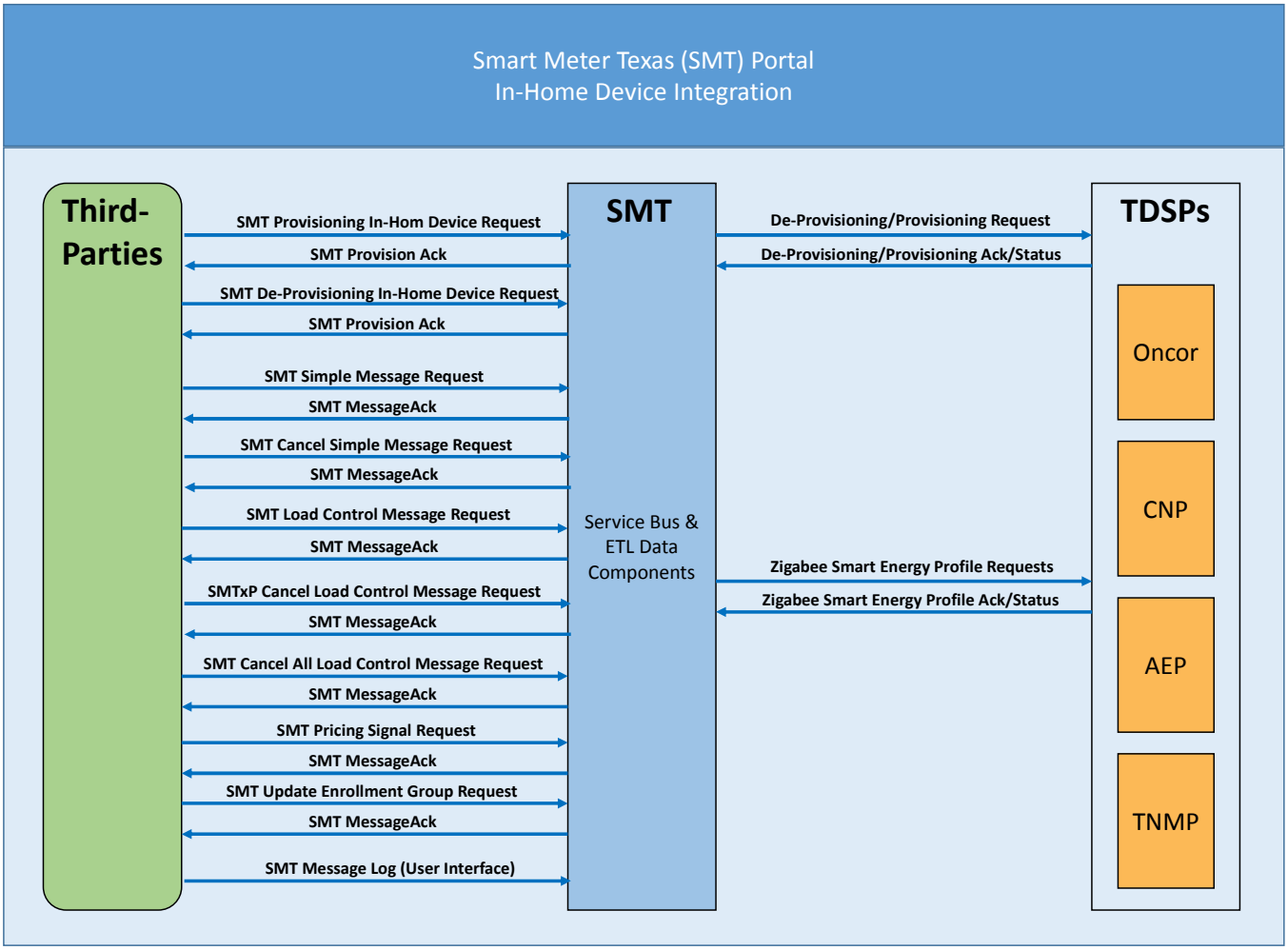


Figure 8: System interface view of all Current release interfaces

5.1.2 Interface Security

Requestors who communicate with SMT using the In-Home Device web service will be on 2-way SSL, the interface must support mutual authentication over SSL. To support authentication, SMT requires user credentials to be passed in Username Token that is part of SOAP header. Token data is used to map the sender of a request to a system account.

When a Username token is sent, the User Name element identifies the system account. The SMT security infrastructure will validate the request sender by verifying the WS-Security signature using the signer certificate from the SMT certificate store. It will also validate that the system account is authorized to access data associated with the DUNs number provided in the Requester Type element of the SMT Header. If the digital signature and DUNs number pass validations and the user can be authenticated, the web service request is passed to the ESB. Otherwise, a SOAP fault is issued.

Tokens are placed into the soap Header. A sample soap Header containing a User token appears below:

```
<soapenv:Header>
  <wsse:Security xmlns:wsse=
  "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
   <wsse:UsernameToken>
    <wsse:Username>Entity_Sytem_Account</wsse:Username>
   </wsse:UsernameToken>
  </wsse:Security>
</soapenv:Header>
```

Note that examples found in subsequent sections will use an empty soap Header in lieu of this. Instructions for the setup of accounts and security credentials will be made available through the SMT help desk. The SMT help desk can be reached on 1- 888-616-5859.

5.1.3 Assumption of Central Time

Requestors have the ability to specify the current time and/or start times for display of messages, load control events and price signals. SMT assumes that all time values input through the API are in Central Standard or Central Daylight Time and converts it to UTC (Coordinated Universal Time).

An example for how Central time values should be formatted appears below:

```
<StartTime>2009-12-01T16:00:00</StartTime>
```

UTC values should be formatted as follows:

```
<StartTime>2009-12-01T16:00:00Z</StartTime>
```

Example: Output when Current time is entered as CT or UTC

Current Time Input (CT)	Output in Zulu	Current Time Input (Zulu)	Output in Zulu
2010-12-32T00:00:00	2011-01-01T06:00:00Z	2011-01-01T00:00:00Z	2011-01-01T00:00:00Z
2010-13-38T00:00:00	2011-02-07T06:00:00Z	2011-02-07T00:00:00Z	2011-02-07T00:00:00Z
2066-13-45T00:00:00	2067-02-14T06:00:00Z	2067-02-14T00:00:00Z	2067-02-14T00:00:00Z
2010-13-29T00:00:00	2011-01-28T06:00:00Z	2011-01-28T00:00:00Z	2011-01-28T00:00:00Z
2000-12-12T00:00:00	2000-12-12T06:00:00Z	2000-12-12T00:00:00Z	2000-12-12T00:00:00Z
2015-03-15T00:00:00	2015-03-15T06:00:00Z	2015-03-15T00:00:00Z	2015-03-15T00:00:00Z
2009-02-15T00:00:00	2009-02-15T06:00:00Z	2009-02-15T00:00:00Z	2009-02-15T00:00:00Z
2009-01-01T00:00:00	2009-01-01T06:00:00Z	2009-01-01T00:00:00Z	2009-01-01T00:00:00Z
2009-02-29T00:00:00	2009-03-01T06:00:00Z	2009-03-01T00:00:00Z	2009-03-01T00:00:00Z
2008-02-29T00:00:00	2008-02-29T06:00:00Z	2008-02-29T00:00:00Z	2008-02-29T00:00:00Z
2008--02-29T24:59:62	2008-03-01T07:00:02Z	2008-03-01T01:00:02Z	2008-03-01T01:00:02Z
2010-12-32T24:59:61	2011-01-02T07:00:01Z	2011-01-02T01:00:01Z	2011-01-02T01:00:01Z
2011-12-10T26:62:62	2011-12-11T09:03:02Z	2011-12-11T03:03:02Z	2011-12-11T03:03:02Z
2010-12-32T24:59:61	2011-01-02T07:00:01Z	2011-01-02T01:00:01Z	2011-01-02T01:00:01Z
2010-12-32T24:65:41	2011-01-02T07:05:41Z	2011-01-02T01:05:41Z	2011-01-02T01:05:41Z

5.1.4 Meter Serial Numbers

All SMT interfaces require a MeterSerialNumber element. SMT will accept the manufacturer's serial number or a fully-qualified TDSP meter serial number in this element (if you are an authorized TDSP user), or all zeros (if you are a Third-Party Service Provider or REP acting as a Third-Party).

An example of a manufacturer's serial number appears below:

```
<MeterSerialNumber>6039657245</MeterSerialNumber>
```

Some TDSPs add a manufacturer code to the manufacturer's serial number to guarantee uniqueness.

CenterPoint places the manufacturer code before the serial number.

```
<MeterSerialNumber>I6039657245</MeterSerialNumber>
```

Oncor appends the manufacturer code to the end of the serial number.

```
<MeterSerialNumber>6039657245LG</MeterSerialNumber>
```

SMT can accept either format and validates the value in combination with the ESIID value provided.

5.1.5 Request Priorities

Requestors have the ability to specify a request priority as part of a SMT Header and within display of messages, load control events and price signals. These elements have been defined with the goal of minimizing future changes. However, prioritization is not implemented in the current release.

5.1.6 Handling Optional Integers

Optional integers are specified for the following interface elements:

- Provisioning request – DeviceClusterSupport
- Load Control event – CoolingTemperationOffset
- Load Control event – HeatingTemperatureOffset
- Load Control event – CoolingTemperationSetPoint

- Load Control event – HeatingTemperatureSetPoint
- Load Control event – AverageLoadAjustPercent
- Load Control event – DutyCycle
- Price Signal – PriceRatio
- Price Signal – GenerationRatio
- Price Signal – AlternateCostUnit
- Price Signal – Generation Price

Requestors must remove the optional tags or must specify an integer value when submitting a request.

5.2 Common SMT-TDSP Interface Definitions

5.2.1 Schema Definitions

All provisioning and deprovisioning requests use the following schema definition:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpprovisiondevice">
```

All messaging requests use the following schema definition:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
```

5.2.2 SMT Request Header Information

SMT messages use a common request header element in the SOAP Body element. An example request header appears below.

```
<Header></Header>
<Body>
 <processProvisionDevice xmlns="http://schemas.esb.ams.com/smtxpprovisiondevice">
 <ProvisioningRequest xmlns="">
 <RequestID>123</RequestID>
 <RequesterType>3</RequesterType>
 <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
 <RequesterID>ADMIN2</RequesterID>
 <RequestPriority>M</RequestPriority>
 <CallbackUri></CallbackUri>
 … <!-- Additional elements within the body appear below-->
</Body>
```

All requests sent to SMT will contain header information list in Table 11

Element	Mandatory	Type	Description
RequestID	N	string(32)	Unique request identifier. Every request sent to SMT will be assigned a RequestID. Requestors may assign their own unique value for a Request ID as part of the request sent to SMT, however it is discouraged because the value is not guaranteed to be unique across all requestors. SMT always generates its own unique value and use it for communications with TDSP systems. The SMT-generated value will be returned to the requestor in a request acknowledgement.
RequesterType	Y	Int	Requester Type indicator. Accepted values are: 0 REP; 1 TDSP; 2 Customer; 3 Third-party; 4 Host; 5 Supplemental
RequesterAuthenticationID	Y	string(9,16)	Requestors and TDSPs should input their primary DUNS number
RequesterID	Y	string	System Account ID of the Requestor
RequestPriority	Y	string(1)	Priority of request. Accepted values are: H – High M – Medium L – Low
CallbackUri	N	string(256)	(For future use as a callback mechanism with the requestor.)

Table 11: SMT-TDSP interface header information

5.3 In-Home Device Provisioning and Deprovisioning

This section describes the device slot management and discusses the interfaces used to Provision and Deprivision In-Home Devices.

5.3.1 Slot Management

A meter may have up to 5 devices provisioned to it. Each device takes a slot. Meter slot management rules are as follows:

- A slot is allocated when a valid provisioning request is accepted by SMT.
- A slot is de-allocated if the TDSP returns a failure status associated with a provisioning request.
- A slot is de-allocated when the TDSP returns a completion status for a deprovisioning request.
- If a deprovisioning request fails, slot allocation is unchanged.

5.3.2 Provisioning In-Home Devices (TDSP Users Only)

TDSP submits the device provisioning request through the front-end web services API (Requests can also be entered via the SMT user interface). SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester is authorized to provision devices to that ESIID, that the correct meter serial number was supplied, that a slot is available, and that device is not already provisioned or in a provisioning request pending status to the ESIID. If a provisioning request passes business validation checks, SMT assigns a unique identifier, saves the request, and sends an acknowledgement. The request status at this point will be Add Acknowledged[1]. If the request fails any of these checks, a failure is returned in a Request Acknowledgement in the form of request rejected.

When the request is sent, the TDSP will initially send an acknowledgment back to SMT - either a successful acknowledgement with the status of add acknowledged or a failure with a status of request failed. There can be two add acknowledged Status for a provisioned request but the acknowledgement will have different description one indicating that SMT received the request and the other indicating that the TDSP received the request. The TDSP may perform initial validation.

The TDSP may perform additional validations on the provisioning request as stated above. If failure occurs, the TDSP will return the failure status to SMT. Otherwise, the provisioning request is executed and the execution status is returned as Meter Ready. In some cases, the customer will have to take some type of action (such as pushing a button) in order to provision that In-Home Device. The manufacturer's instructions should provide further details. Once the device has completed its joining process, the TDSP will return a successful status of device added or a failure with add failed.

Figure 9 shows the interface exchanges for provisioning an In-Home Device.

[1] All provisioning and deprovisioning status are visible through the Portal UI.

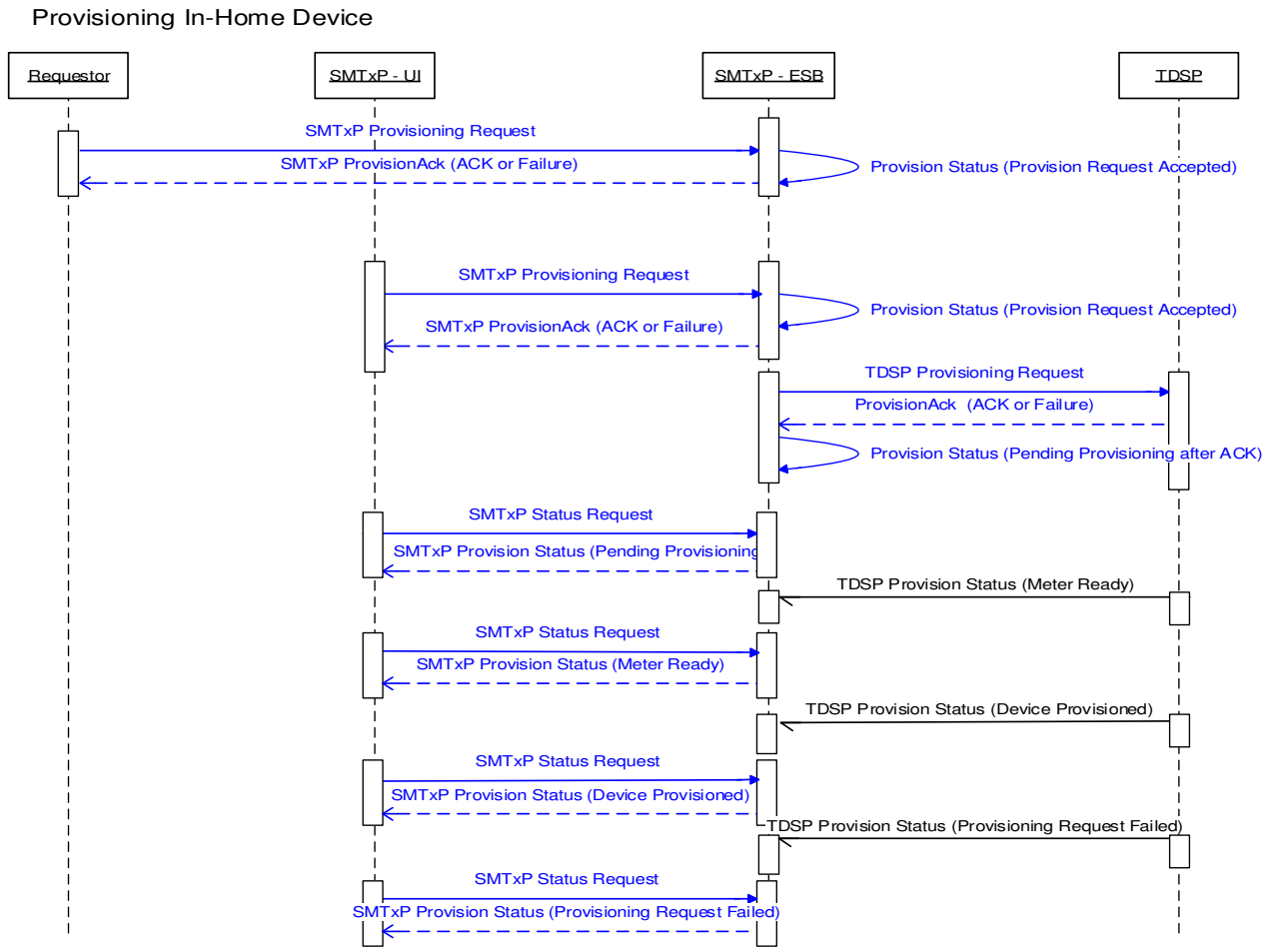


Figure 9: Provisioning an In-Home Device

SMT will only allow one In-Home Device to be provisioned per request.

A sample provisioning request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpprovisiondevice">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
  </wsse:Security>
 </soapenv:Header>
  <soapenv:Body>
   <smt:processProvisionDevice>
    <SMTxPProvisioningRequest>
     <!--Optional  RequestID removed -->
```

```
        <RequesterType>3</RequesterType>
        <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
        <RequesterID>ADMIN2</RequesterID>
        <RequestPriority>M</RequestPriority>
        <!--Optional: CallbackUri removed -->
        <DeviceProvisionRequestList>
          <DeviceProvisionRequest>
            <ESIID>00000000000000001</ESIID>
            <MeterSerialNumber>00000000000000000</MeterSerialNumber>
            <DeviceMACAddr>101BC50070000502</DeviceMACAddr>
            <DeviceInstallCode>83FED3407A939723A5C639B26916D505C3B5</DeviceInstallCode>
            <!--Optional: DeviceClusterSupport removed -->
            <!—Optional: DeviceClass removed -->
            <DeviceText>Living Room PCT</DeviceText>
          </DeviceProvisionRequest>
        </DeviceProvisionRequestList>
      </SMTxPProvisioningRequest>
    </smt:processProvisionDevice>
  </soapenv:Body>
</soapenv:Envelope>
```

When sending a device provisioning request, the SMT request will include:

A request header.
Display request information below.

Provisioning request information formatted as described in Table 12

Element	Mandatory	Type	Description
ESIID	Y	string(17,64)	Energy Service Interface identifier
MeterSerialNumber	Y	string(30)	TDSP Meter manufacturer serial number
DeviceMACAddr	Y	string(16)	Device MAC Address
DeviceInstallCode	Y	string(36)	Device Installation Code
DeviceClusterSupport	N	Int	Sum of 1 - Messaging, 2 - Load Control, 4 Pricing, 0 - unspecified (max integer value = 7), default=0
DeviceClass	N	string(5)	Bitmap values. Bit position(right to left) as 1=InHomeDisplay, 2=LoadControlDevice, 3=ProgrammableThermostat, 4=IntelligentGateway. The SMT API will accept a string(5) value. Characters must be a "0" or a "1". ACK=FLR is returned if this value deviates from these rules.
DeviceText	N	string(256)	User-friendly label for device identification

Table 12: Device provisioning request information.

5.3.3 Deprovisioning In-Home Devices

Requestor submits the device deprovisioning request through the front-end web services API. (Requests can also be entered via the SMT user interface.) SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester is authorized to deprovision the devices to that ESIID, that the correct meter serial number was supplied and that the device is not already deprovisioned or in a deprovisioning request pending status to the ESIID. If a deprovisioning request passes business validation checks, SMT assigns a unique identifier, saves the request, and sends an acknowledgement. The request status at this point will be remove acknowledged[2]. If the request fails any of these checks, a failure is returned in a Request Acknowledgement in the form of request rejected.

When the request is sent, the TDSP will initially send an acknowledgment back to SMT - either a successful acknowledgement with the status of remove acknowledged or a failure with a status of request failed. There can be two remove acknowledged Status for a deprovisioned request but the acknowledgment will have different description one indicating that SMT received the request and the other indicating that the TDSP received the request. The TDSP may perform initial validation.

The TDSP would perform additional validations on the deprovisioning request if applicable as stated above. If failure occurs, the TDSP will return the failure status to SMT. Otherwise, the deprovisioning request is executed and the execution status is returned. Once the device has completed its deprovisioning process, the TDSP would return a successful status of device removed or a failure with remove failed.

Figure 10 shows the interface exchanges for deprovisioning an In-Home Device.

[2] All provisioning and de-provisioning status are visible through the Portal UI.

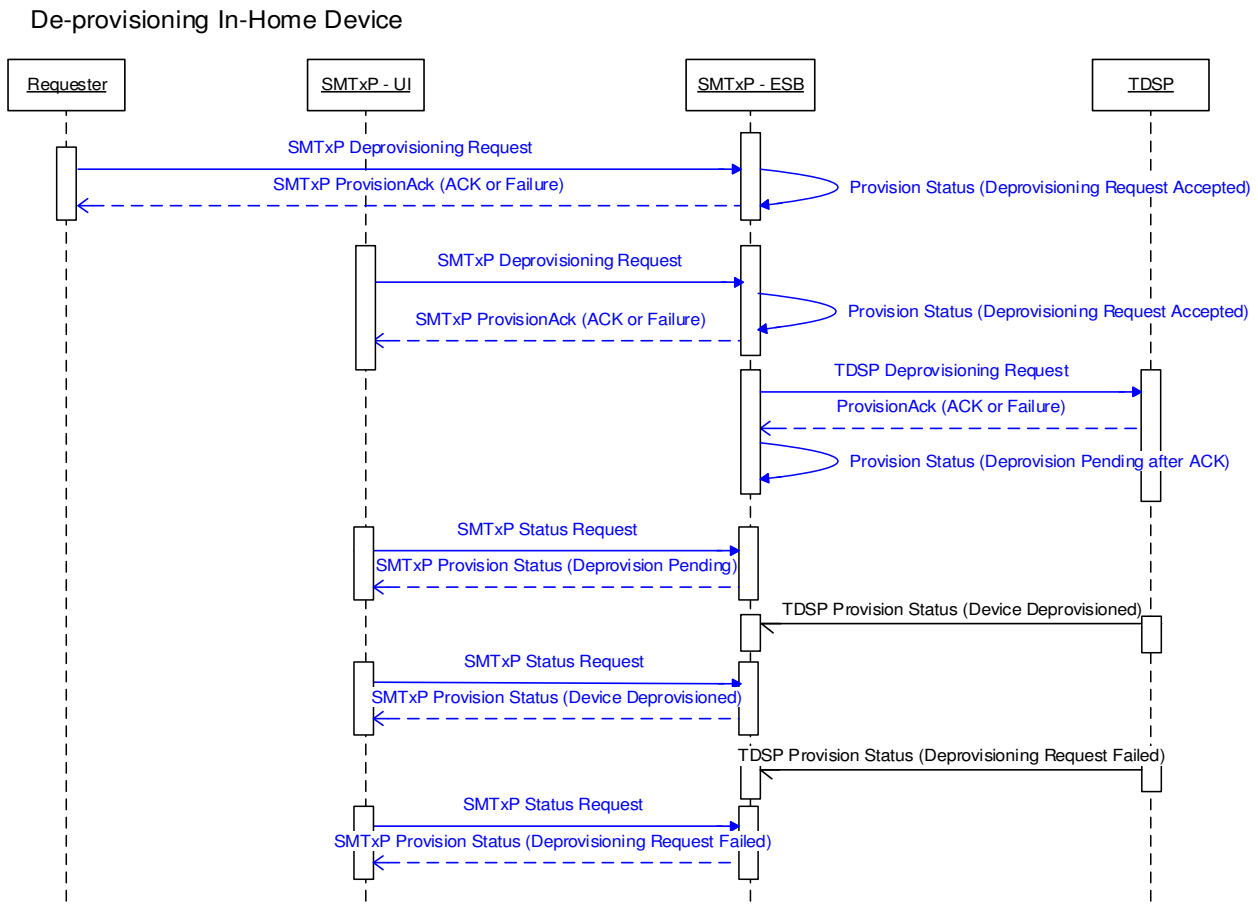


Figure 10: Deprovisioning an In-Home Device

SMT will only allow one In-Home Device to be deprovisioned per request.

A sample deprovisioning request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpprovisiondevice">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
  </wsse:Security>
 </soapenv:Header>
  <soapenv:Body>
   <smt:processDeProvisionDevice>
    <SMTxPDeProvisionRequest>
     <!--Optional  RequestID removed -->
     <RequesterType>3</RequesterType>
```

```
        <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
        <RequesterID>ADMIN1</RequesterID>
        <RequestPriority>L</RequestPriority>
        <!--Optional: CallbackUri removed -->
        <DeviceDeprovisionRequestList>
          <DeviceDeprovisionRequest>
            <ESIID>00000000000000001</ESIID>
            <MeterSerialNumber>00000000000000098</MeterSerialNumber>
            <DeviceMACAddr>101BC50070000502</DeviceMACAddr>
            <ReasonCode>3</ReasonCode>
            <ReasonComment>Customer requested deprovisioning</ReasonComment>
          </DeviceDeprovisionRequest>
        </DeviceDeprovisionRequestList>
      </SMTxPDeProvisionRequest>
    </smt:processDeProvisionDevice>
  </soapenv:Body>
</soapenv:Envelope>
```

When sending a device deprovisioning request, the SMT request will include a Request Header. Display request information as described in Table 13

Element	Mandatory	Type	Description
ESIID	Y	string(17,64)	Energy Service Interface identifier
MeterSerialNumber	Y	string(30)	TDSP Meter manufacturer serial number
DeviceMACAddr	Y	string(16)	Device MAC Address
ReasonCode	Y	string(1)	Deprovisioning reason code are : 1 = RepRequested 2 = CustomerRequested, 3 = MalfunctioningDevice, 4 = UnsupportedDevice, 5 = RequestProvByMistake, 6 = NetworkInterference 7 = Other
ReasonComment	N	string(64)	Reason description for deprovisioning

Table 13: Device deprovisioning request information

5.3.4 Device Provisioning and Deprovisioning Request Acknowledgement

When a provisioning or deprovisioning request is sent to SMT, an appliance on the SMT perimeter performs XML validation. If the request fails validation, a SOAP fault is returned. If the request passes XML validation, it is passed to the SMT Enterprise Service Bus to process. The SMT ESB performs business validations and returns a Provisioning Request Acknowledgement

A sample provisioning acknowledgement appears below.

```
<soapenv:Envelope xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
```

```
<soapenv:Header/>
<soapenv:Body>
  <sm:processProvisionDeviceResponse xmlns:sm=
    "http://schemas.esb.ams.com/smtxpprovisiondevice">
     <SMTxPProvisionAck>
```

Element	Mandatory	Type	Description
RequestID	Y	string(32)	Unique Request ID which is generated by SMT
RequestStatus	Y	string(3)	Values returned are: ACK - Acknowledgement indicating the request was accepted for further processing. FLR - Failure, indicating the request was not accepted for processing
RequestStatusDesc	N	string(64)	Request Status Description

Table 14: Device provisioning/deprovisioning acknowledgement header record

If a request is sent with invalid addressing information, the invalid information will returned as one or more invalid request elements. The elements of an invalid request record appear in Table 15..

Element	Mandatory	Type	Description
ESIID	Y	string(17,64)	Energy Service Interface identifier
MeterSerialNumber	Y	string(30)	TDSP Meter manufacturer serial number
DeviceMACAddr	N	string(16)	Device MAC Address
Reason	N	string(128)	Reason of Failure at individual ESIID

Table 15: Device provisioning and deprovisioning status record

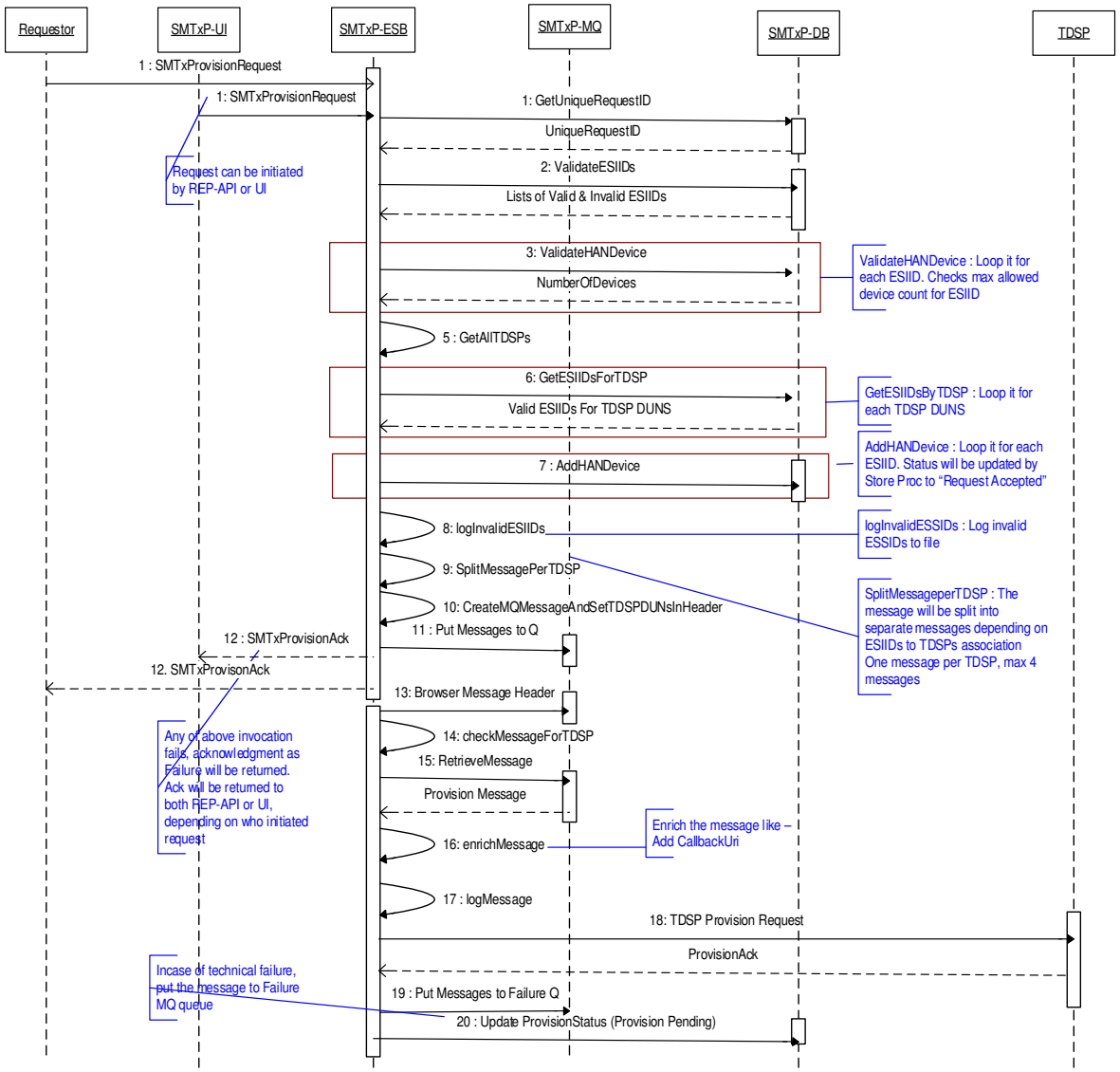


Figure 11: Deprovisioning an In-Home Device.

5.3.5 Update Utility Enrollment Group Request

NOTE: Verify that the TDSP and the In-Home Device Manufacturer support the Utility Enrollment Group functionality before initiating the request.

The following shows the interface exchanges for updating the Utility Enrollment Group value on an In-Home Device.

Requestor submits the update UEG request through the front-end web services API. SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.

- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester is authorized to deprovision the devices to that ESIID, that the correct meter serial number was supplied and that the device is not already deprovisioned or in a deprovisioning request pending status to the ESIID. If a deprovisioning request passes business validation checks, SMT assigns a unique identifier, saves the request, and sends an acknowledgement. The request status at this point will be remove acknowledged[1].if the request fails any of these checks, a failure is returned in a Request Acknowledgement in the form of request rejected.

When the request is sent, the TDSP will initially send an acknowledgment back to SMT - either a successful acknowledgement with the status of remove acknowledged or a failure with a status of request failed. The TDSP may perform initial validation.

The TDSP would perform additional validations on the update UEG request if applicable as stated above. If failure occurs, the TDSP will return the failure status to SMT. Otherwise, the deprovisioning request is executed and the execution status is returned. Once the device enrollment group has been set, the TDSP would return a status.

A sample Update UEG Request message appears below:

```
<soapenv:Body wsu:Id="id-7" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
   <smt:processUpdateUEGDevice>
     <SMTxPUpdateUEGRequest>
       <!--Optional:-->
       <RequestID/>
       <RequesterType>3</RequesterType>
       <RequesterAuthenticationID>799530915</RequesterAuthenticationID>
       <RequesterID>reliantuser01</RequesterID>
       <RequestPriority>H</RequestPriority>
       <!--Optional:-->
       <CallbackUri>cnn.com</CallbackUri>
       <DeviceUpdateUEGRequestList>
         <!--1 to 100 repetitions:-->
         <DeviceUpdateUEGRequest>
           <ESIID>10089010201473984801 00</ESIID>
           <MeterSerialNumber>61330847</MeterSerialNumber>
           <DeviceMACAddr>1234567890234534</DeviceMACAddr>
           <UtilityEnrollmentGroup>200</UtilityEnrollmentGroup>
         </DeviceUpdateUEGRequest>
       </DeviceUpdateUEGRequestList>
     </SMTxPUpdateUEGRequest>
   </smt:processUpdateUEGDevice>
 </soapenv:Body>
</soapenv:Envelope>
```

A request header.

Display request information as described in the table below.

Element	Mandatory	Type	Description
ESIID	Y	string(17,64)	Energy Service Interface identifier
MeterSerialNumber	Y	string(30)	TDSP Meter manufacturer serial number
DeviceMACAddr	Y	string(16)	Device MAC Address
UtilityEnrollmentGroup	Y	integer(1)	0 to 255

Table 16: Update UEG request information

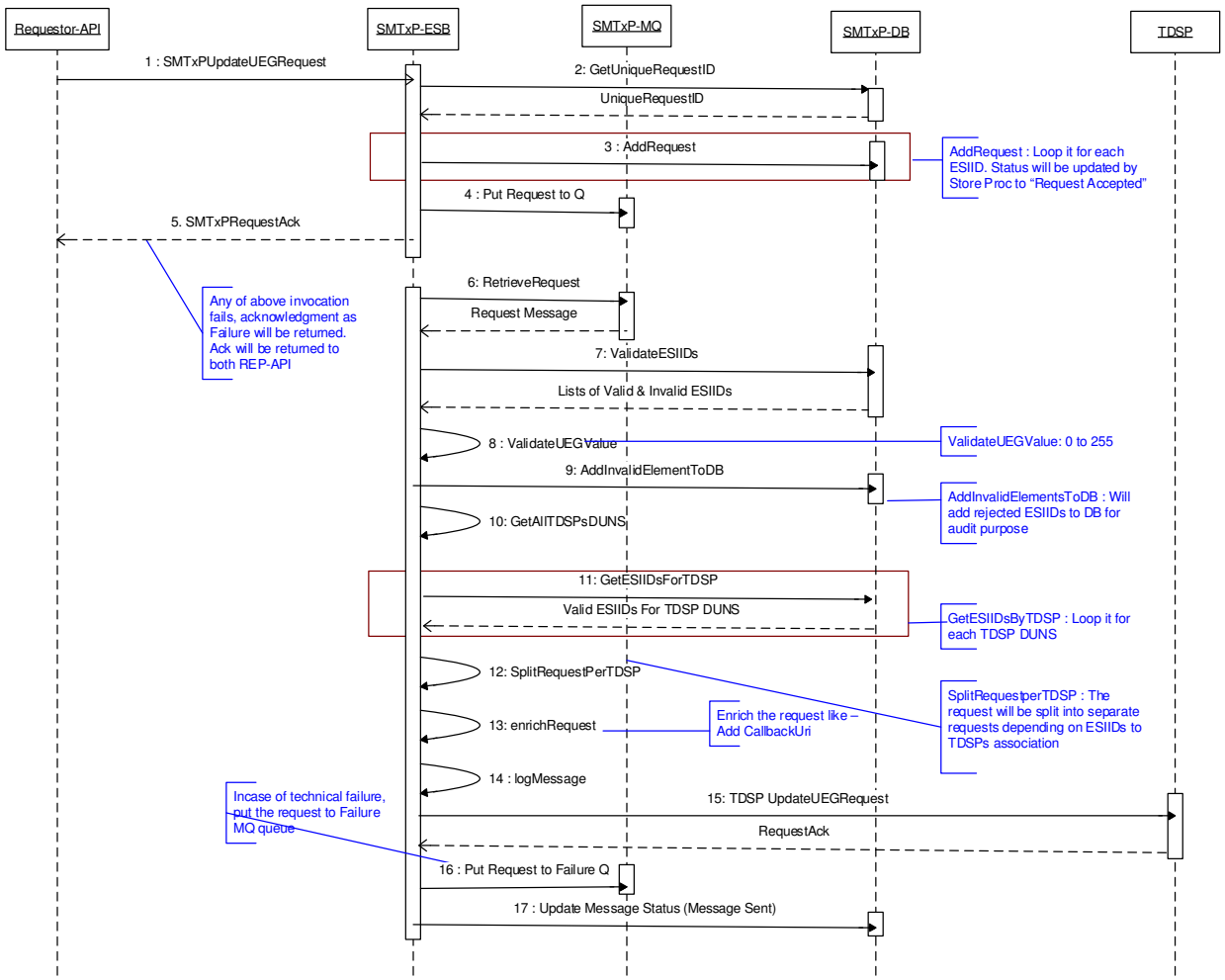


Figure 12: Update Utility Enrollment Group Request

5.3.6 Update UEG Request Acknowledgement

When an update UEG request is sent to SMT, an appliance on the SMT perimeter performs XML validation. If the request fails validation, a SOAP fault is returned. If the request passes XML validation, it is passed to the SMT Enterprise Service Bus to process. The SMT ESB performs business validations and returns a Update UEG Request Acknowledgement.

A sample update UEG acknowledgement appears below.

```
<soapenv:Body wsu:Id="id-10" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <tds:processDeviceUpdateUEGStatus>
      <UpdateUEGStatusResponse>
        <!--Optional:-->
        <StatusID>313745</StatusID>
        <TDSPDUNSNumber>957877905</TDSPDUNSNumber>
        <DeviceUpdateUEGStatusList>
          <!--Zero or more repetitions:-->
          <DeviceUpdateUEGStatus>
            <ESIID>1008901020147398480100</ESIID>
            <MeterSerialNumber>61330847</MeterSerialNumber>
            <DeviceMACAddr>1234567890234534</DeviceMACAddr>
            <EventCategoryID>UEG</EventCategoryID>
            <StatusCode>COM</StatusCode>
            <!--Optional:-->
            <StatusDesc>Testing By Eswar</StatusDesc>
            <StatusTimestamp>2011-08-10T16:01:12Z</StatusTimestamp>
            <!--Optional:-->
            <ReasonCode>Eswar</ReasonCode>
            <!--Optional:-->
            <ReasonComment>Eswar</ReasonComment>
          </DeviceUpdateUEGStatus>
        </DeviceUpdateUEGStatusList>
      </UpdateUEGStatusResponse>
    </tds:processDeviceUpdateUEGStatus>
  </soapenv:Body>
</soapenv:Envelope>
```

Element	Mandatory	Type	Description
RequestID	Y	string(32)	Unique Request ID which is generated by SMT
RequestStatus	Y	string(3)	Values returned are: ACK - Acknowledgement indicating the request was accepted for further processing. FLR - Failure, indicating the request was not accepted for processing
RequestStatusDesc	N	string(64)	Request Status Description

Table 17: Update UEG acknowledgement header record

If a request is sent with invalid addressing information, the invalid information will returned as one or more invalid request elements. The elements of an invalid request record appear in Table 18.

Element	Mandatory	Type	Description
ESIID	Y	string(17,64)	Energy Service Interface identifier
MeterSerialNumber	Y	string(30)	TDSP Meter manufacturer serial number
DeviceMACAddr	N	string(16)	Device MAC Address

Element	Mandatory	Type	Description
Reason	N	string(128)	Reason of Failure at individual ESIID

Table 18: Update UEG acknowledgement record.

5.3.7 In-Home Device Status API

The current status of In-Home Devices can be obtained from the SMT database via the In-Home Device Status Report API. This API can be used to make a request for a daily comprehensive list of all In-Home Devices with their current status. It also can be used to retrieve 3 incremental In-Home Device status reports in the current day. The figure below shows the interaction between the API and the requester.

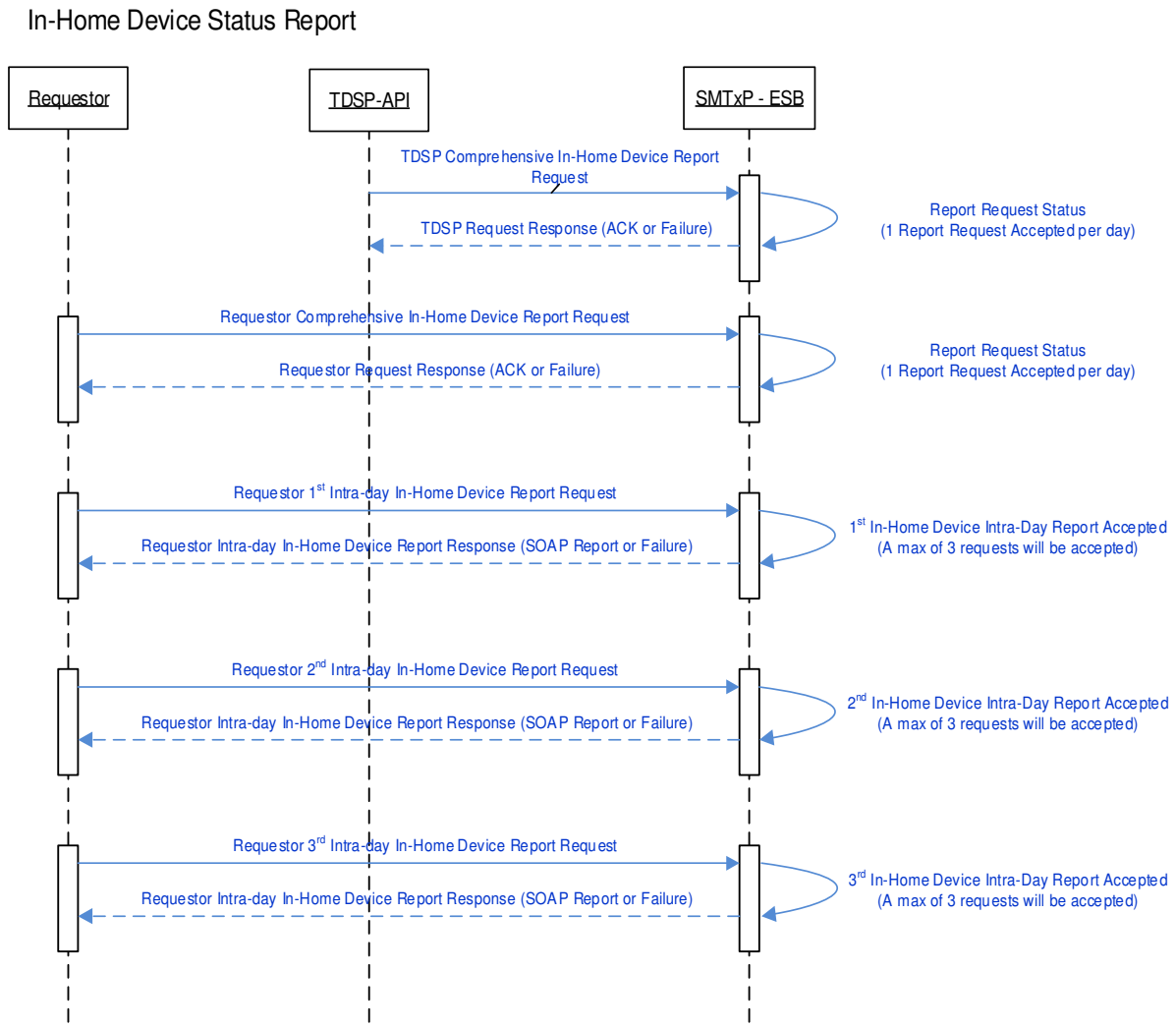


Figure 13: In-Home Device Status Report Request flow

5.3.7.1 Comprehensive In-Home Device Status Report Request Details

A Requestor or TDSP submits the comprehensive In-Home Device Status Report request through a web services API. SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester has not sent a previous request for the comprehensive report this day. If the user's request is the first one for the day, the user is added to the list of recipients and a success is returned in the form of request accepted. If the request fails the count check, a failure message is returned in the Request Acknowledgement in the form of "User already registered".

A sample comprehensive In-Home Device Status Report request appears below.

```
<soapenv:Envelope xmlns:smt="http://schemas.esb.ams.com/smtxphanstatus"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
  </soapenv:Header>
  <soapenv:Body wsu:Id="id-4" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
    <smt:processSMTxPHANStatusComprehensiveRequest>
      <SMTxPHANStatusRequest>
        <!--Optional:-->
        <RequestID></RequestID>
        <!--Optional:-->
        <RequesterType>3</RequesterType>
        <!--Optional:-->
        <RequesterAuthenticationID>799530915</RequesterAuthenticationID>
        <!--Optional:-->
        <RequesterID>HANREPADMIN</RequesterID>
        <!--Optional:-->
        <RequestPriority>H</RequestPriority>
        <!--Optional:-->
        <CallbackUri/>
        <!--Optional:-->
        <RequestType>ONETIME</RequestType>
      </SMTxPHANStatusRequest>
    </smt:processSMTxPHANStatusComprehensiveRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

When sending a comprehensive In-Home Device Status Report request, the SMT request will include the request information is described below in Table 20.

Element	Mandatory	Type	Description
RequestID	N	string(32)	Unique request identifier. Every request sent to SMT will be assigned a RequestID. The requestor may assign their own unique value for a Request ID as part of the request sent to SMT, however it is discouraged because the value is not guaranteed to be unique across all requestors. SMT always generates its own unique value and use it for communications with TDSP systems. The SMT-generated value will be returned to the requestor in a request acknowledgement.
RequesterType	N	Int	Requester Type indicator. Accepted values are: 1 TDSP; 3 Third-party
RequesterAuthenticationID	N	string(9,16)	Third-Parties and TDSPs should input their primary DUNS number
RequesterID	Y	string	System Account ID of the Requestor
RequestPriority	N	string(1)	Priority of request. Accepted values are: H – High M – Medium L – Low
CallbackUri	N	string(256)	(For future use as a callback mechanism with the requestor.)
RequestType	Y		Indicates this is a request for a comprehensive report. 'ONETIME' is the accepted value.

Table 19: Comprehensive In-Home Device Status Report Request

5.3.7.2 Incremental In-Home Device Status Report Request Details

A Requestor or TDSP submits the incremental In-Home Device Status Report request through a web services API. SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester has not sent more than three requests for the day. If the request is the first request for the day, a report is returned containing report data for the time period between the start of the day and the current time of the request. If the request is the second request for the day, a report is returned containing report data for the time period between the first request of the day and the current time of the second request. If the request is the third request for the day, a report is returned containing report data for the time period between the second request of the day and the current time of the third request. If the request fails the count check, a failure message is returned in a Request Acknowledgement in the form of "Fail – Request exceeding 3".

A sample incremental In-Home Device Status Report request appears below.

```
<soapenv:Envelope xmlns:smt="http://schemas.esb.ams.com/smtxphanstatus"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
  </soapenv:Header>
  <soapenv:Body wsu:Id="id-6690098" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd">
    <smt:ProcessSMTxPHANStatusSyncResponse>
      <SMTxPHANStatusSyncRequest>
        <RequestID></RequestID>
        <!--Optional:-->
        <RequesterType>3</RequesterType>
        <!--Optional:-->
        <RequesterAuthenticationID>799530915</RequesterAuthenticationID>
        <!--Optional:-->
        <RequesterID>HANREPADMIN</RequesterID>
        <!--Optional:-->
        <RequestPriority>H</RequestPriority>
        <!--Optional:-->
        <CallbackUri/>
      </SMTxPHANStatusSyncRequest>
    </smt:ProcessSMTxPHANStatusSyncResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

When sending an incremental In-Home Device Status Report request, the SMT request will include the request information is described below in Table 20.

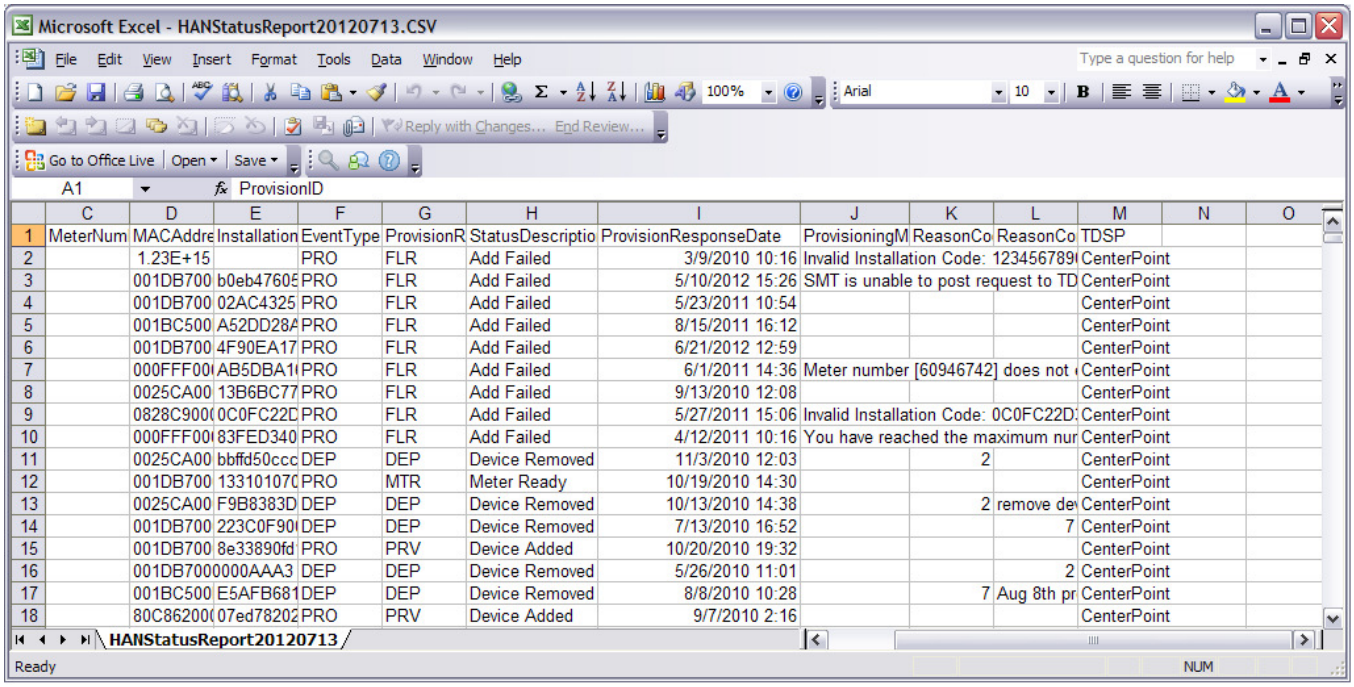
Element	Mandatory	Type	Description
RequestID	N	string(32)	Unique request identifier. Every request sent to SMT will be assigned a RequestID. The requestor may assign their own unique value for a Request ID as part of the request sent to SMT, however it is discouraged because the value is not guaranteed to be unique across all requestors. SMT always generates its own unique value and use it for communications with TDSP systems. The SMT-generated value will be returned to the requestor in a request acknowledgement.
RequesterType	N	Int	Requester Type indicator. Accepted values are: 1 TDSP; 3 Third-party
RequesterAuthenticationID	N	string(9,16)	Requestors and TDSPs should input their primary DUNS number
RequesterID	Y	string	System Account ID of the Requestor
RequestPriority	N	string(1)	Priority of request. Accepted values are: H – High M – Medium L – Low
CallbackUri	N	string(256)	(For future use as a callback mechanism to the requestor.)

Table 20: Incremental In-Home Device Status Report Request

5.3.8 In-Home Device Status Report Format

The comprehensive report will be placed in the FTP folder of the Requestor or TDSP. The report will remain in the FTP folder for a period of 10 days and will be deleted afterwards.

A sample comprehensive In-Home Device Status Report appears below:



	C	D	E	F	G	H	I	J	K	L	M	N	O
1	MeterNum	MACAddre	Installation	EventType	ProvisionR	StatusDescriptio	ProvisionResponseDate	ProvisioningM	ReasonCo	ReasonCo	TDSP		
2		1.23E+15		PRO	FLR	Add Failed	3/9/2010 10:16	Invalid Installation Code: 123456789			CenterPoint		
3		001DB700	b0eb4760	PRO	FLR	Add Failed	5/10/2012 15:26	SMT is unable to post request to TD			CenterPoint		
4		001DB700	02AC4325	PRO	FLR	Add Failed	5/23/2011 10:54				CenterPoint		
5		001BC500	A52DD28A	PRO	FLR	Add Failed	8/15/2011 16:12				CenterPoint		
6		001DB700	4F90EA17	PRO	FLR	Add Failed	6/21/2012 12:59				CenterPoint		
7		000FFF00	AB5DBA1	PRO	FLR	Add Failed	6/1/2011 14:36	Meter number [60946742] does not			CenterPoint		
8		0025CA00	13B6BC77	PRO	FLR	Add Failed	9/13/2010 12:08				CenterPoint		
9		0828C900	0C0FC22D	PRO	FLR	Add Failed	5/27/2011 15:06	Invalid Installation Code: 0C0FC22D			CenterPoint		
10		000FFF00	83FED340	PRO	FLR	Add Failed	4/12/2011 10:16	You have reached the maximum nur			CenterPoint		
11		0025CA00	bbffd50ccc	DEP	DEP	Device Removed	11/3/2010 12:03		2		CenterPoint		
12		001DB700	133101070	PRO	MTR	Meter Ready	10/19/2010 14:30				CenterPoint		
13		0025CA00	F9B8383D	DEP	DEP	Device Removed	10/13/2010 14:38		2	remove de	CenterPoint		
14		001DB700	223C0F90	DEP	DEP	Device Removed	7/13/2010 16:52			7	CenterPoint		
15		001DB700	8e33890fd	PRO	PRV	Device Added	10/20/2010 19:32				CenterPoint		
16		001DB7000000AAA3		DEP	DEP	Device Removed	5/26/2010 11:01			2	CenterPoint		
17		001BC500	E5AFB681	DEP	DEP	Device Removed	8/8/2010 10:28		7	Aug 8th pr	CenterPoint		
18		80C86200	07ed7820	PRO	PRV	Device Added	9/7/2010 2:16				CenterPoint		

Figure 14: Comprehensive In-Home Device Status Report

The incremental In-Home Device Status Report response is a synchronous SOAP message. The message will contain In-Home Device status representing three different increments in the current day. The increments are broken down by response:

- Response 1: contains report data for the time period between the start of the day and the current time of the first request.
- Response 2: contains report data for the time period between the first request of the day and the current time of the second request.
- Response 3: contains report data for the time period between the second request of the day and the current time of the third request.

A sample incremental In-Home Device Status Report appears below:

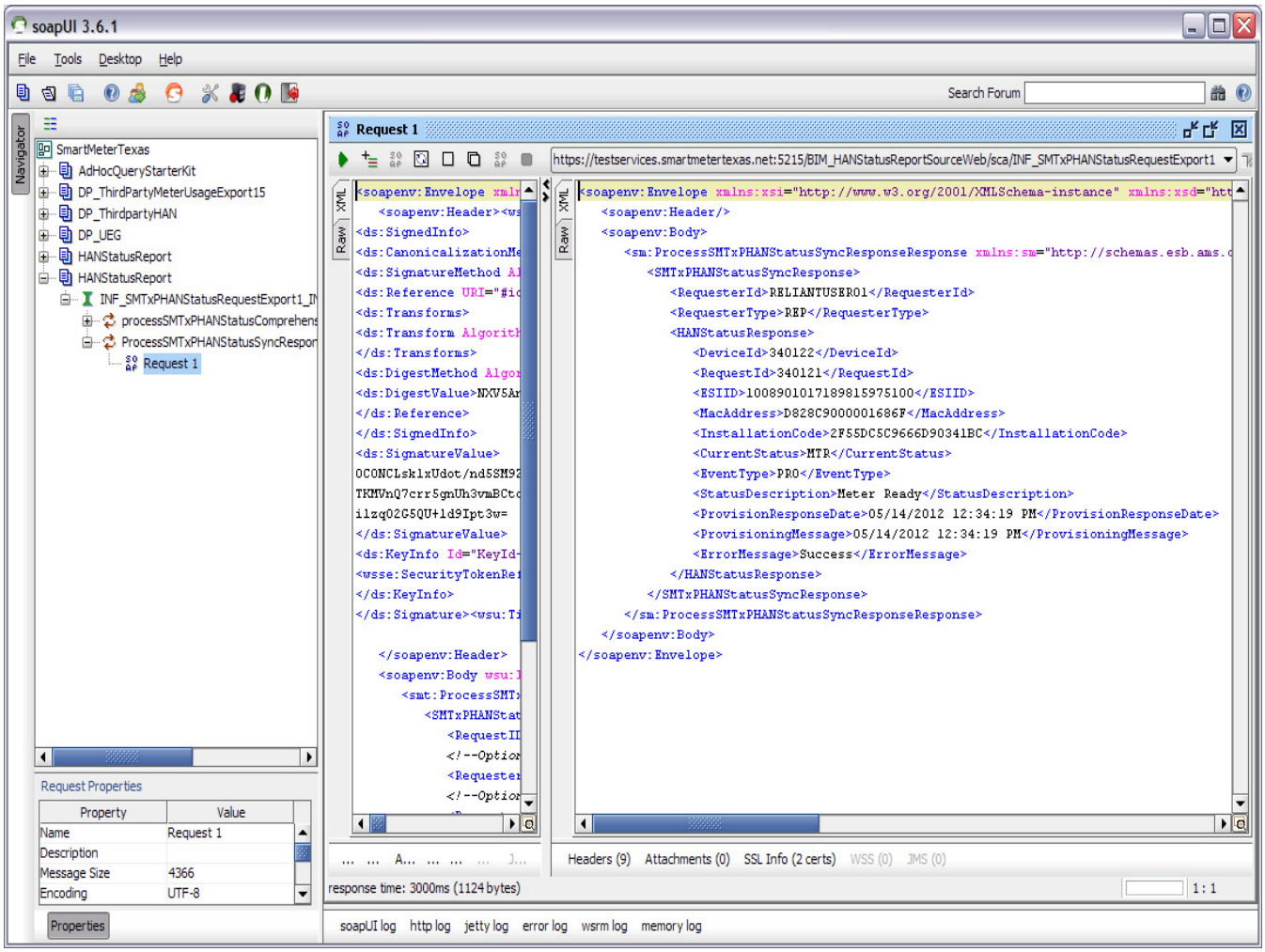


Figure 15: Incremental In-Home Device Status Report

5.4 In-Home Device Messaging

This section presents information concerning the submission of Smart Energy Profile message requests in the Smart Meter Texas portal.

5.4.1 Addressing of Zigbee Smart Energy Messages

SMT utilizes the Address Block group in the In-Home Device Messaging API's to validate the destination of the Zigbee Smart Energy Messages.

The table below**Error! Reference source not found.** describes the contents of each Address-Block element.

Element			Mandatory	Type	Description
Address List			N		Collection of address elements
	Address	ESIID	Y	string(64)	Energy Service Interface identifier CNP requires that the ESIID field be populated with the target ESIID(s) for Point-to-Point Messaging Oncor and AEP require that the ESIID field be populated with the target ESIID(s)
		Meter Serial Number	Y	string(30)	TDSP Meter manufacturer serial number CNP requires that the Meter Serial Number field be populated with the target Meter Serial Number for Point-to-Point Messaging Oncor/AEP require that the Meter Serial Number field be populated with the target Meter Serial Number(s)
		Device MAC Addr	N	string(16)	All TDSPs require that the Device MAC Addr field be populated with BLANK value.

Table 21: Address blocks element information

The Address block includes a collection of address elements. SMT's Address block validation logic requires that the collection of ESIID/Meter address elements be populated in the In-Home Device Messaging API's to accept the In-Home Device Message. If it is not populated, SMT will generate an exception back to the requester.

5.4.2 Addressing of Messages with ESIIDs

The figure below presents an example of how message addressing will be handled when a requester includes ESIIDs with a message. On the left, the requester has provided three ESIIDs – 1 ESIID and meter serial number each for TDSP 1, TDSP 2 and TDSP 3. SMT creates 3 copies of the message and adds information as required for the message. If appropriate, SMT will evaluate the ESIID list and route and create messages to go to appropriate TDSPs.

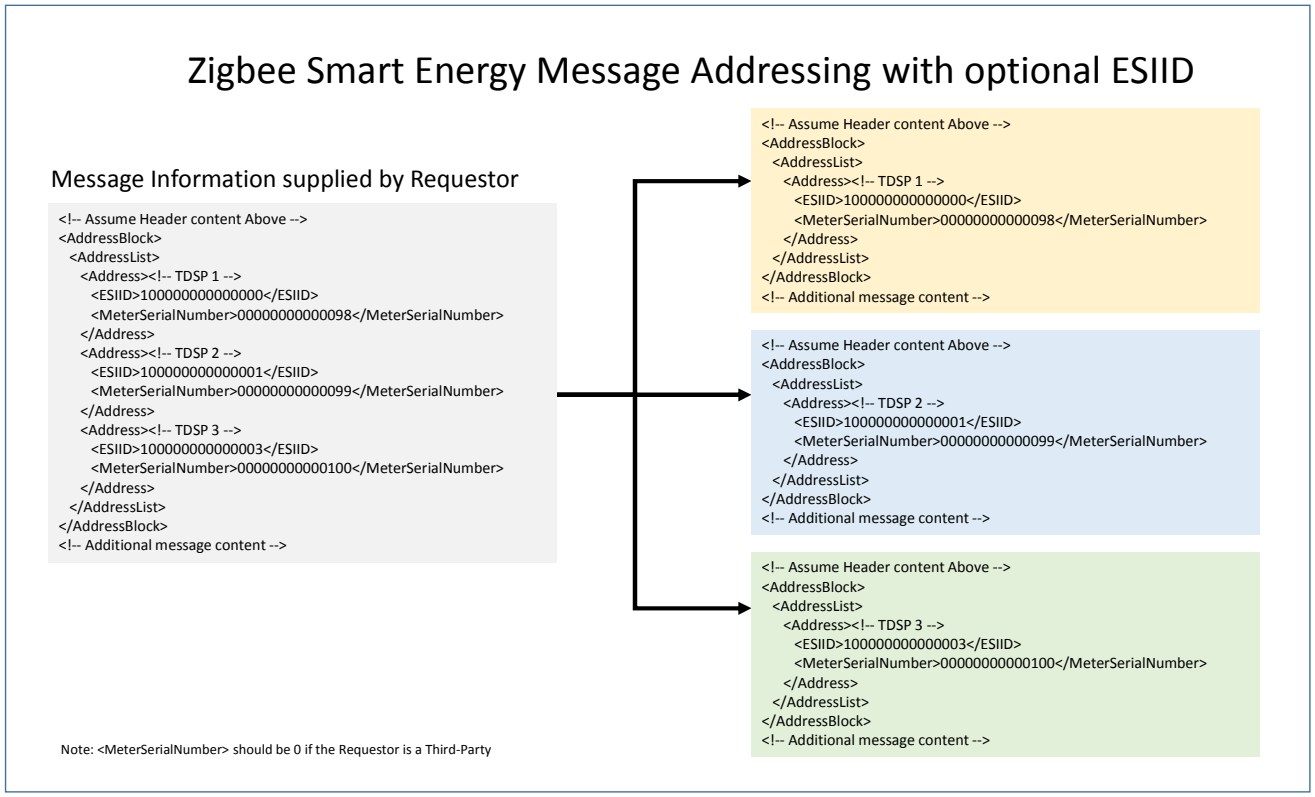


Figure 16: Message addressing with ESIIDs

SMT will limit the number of address elements to 10,000. Requests with more than 10,000 address elements will be rejected.

5.4.3 Simple Text/Display Messaging

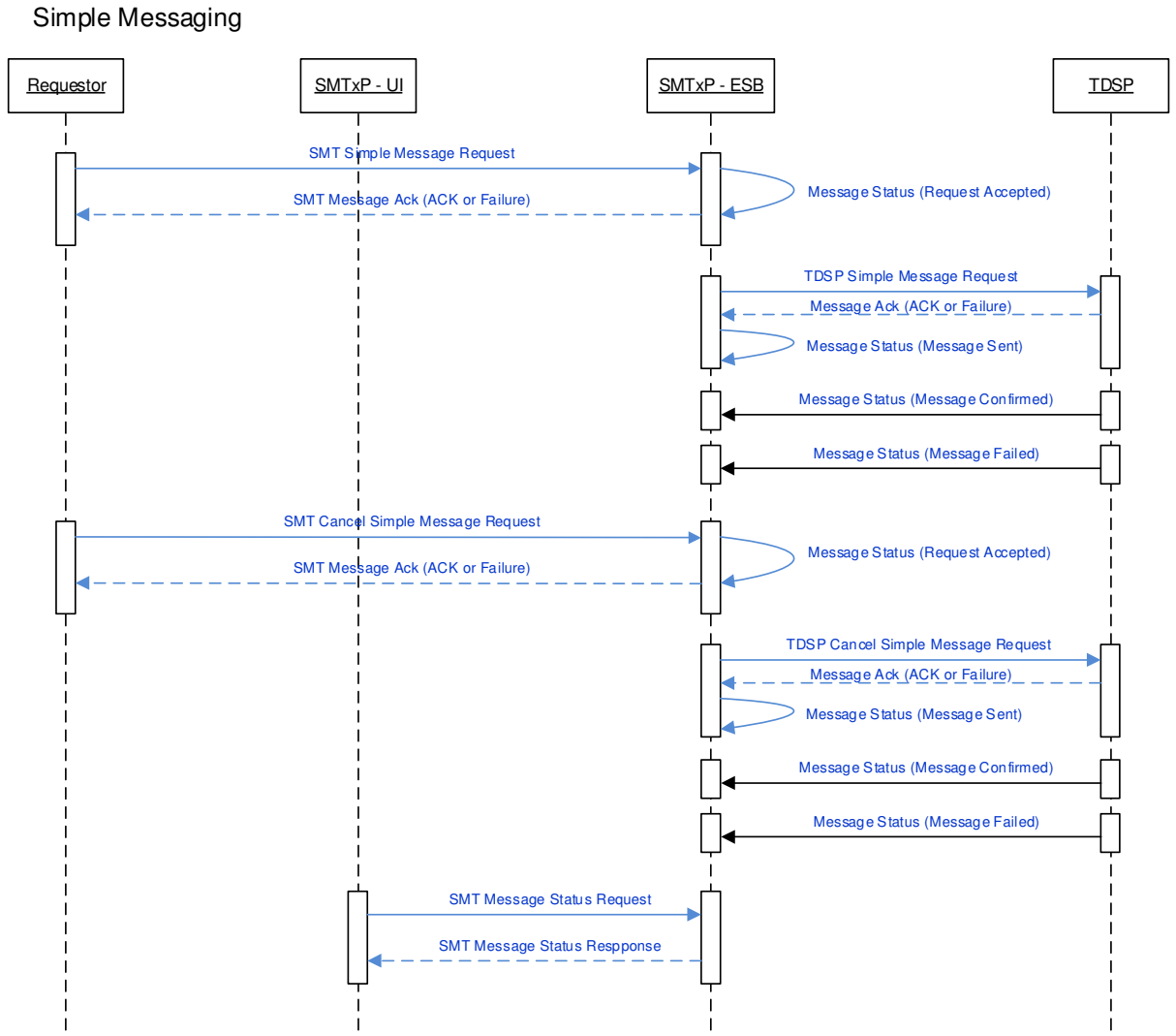


Figure 17: Sending and Cancelling Simple text/display Messages

The above figure shows the interface exchanges for sending and canceling simple text/display messages.

Requestor submits simple text message request via the SMT API. SMT performs two levels of validations:

- XML validation is performed by SMT. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester is authorized to send a text message. If the simple text messaging request passes business validation checks, SMT assigns a unique identifier, saves the request, and returns an acknowledgement to the requestor. If the request fails any of these checks, a failure is returned in a Request Acknowledgement in the form of request rejected.

SMT will create a copy and send to the respective TDSPs based on the addressing schemes. When the request is sent, the TDSP may perform initial validation on the simple text messaging request and then acknowledge the

request or return a failure. The request status becomes *Request Acknowledged by TDSP* when the TDSP returns an acknowledgement or *Request Failed* if a failure condition is returned.

The TDSP will perform additional validations on the simple text messaging request after returning the acknowledgement. If a failure occurs, the TDSP will return the failure status to SMT. Otherwise, the simple text messaging request is executed and the execution status is returned. In either case, SMT will store the simple text messaging request status that is returned.

The failure status will be different for each TDSP and depends on the failure condition.

5.4.3.1 Sending Simple Text/Display Messages

A sample simple text message request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
 </wsse:Security>
</soapenv:Header>
 <soapenv:Body>
  <smt:processSimpleMessaging>
   <SMTxPSimpleMessageRequest>
    <!--Optional  RequestID removed -->
    <RequesterType>3</RequesterType>
    <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
    <RequesterID>ADMIN2</RequesterID>
    <RequestPriority>L</RequestPriority>
    <!--Optional: CallbackUri removed -->
    <AddressBlock>
     <!--Optional: GroupID removed -->
     <AddressList>
      <!--0 to 10000 repetitions:-->
      <Address>
       <ESIID>00000000000000001</ESIID>
       <MeterSerialNumber>00000000000000098</MeterSerialNumber>
       <DeviceMACAddr>101BC50070000502</DeviceMACAddr>
      </Address>
     </AddressList>
    </AddressBlock>
    <SimpleMessageBlock>
     <MessageID>123</MessageID>
     <StartTime>2000-01-01T00:00:00Z</</StartTime>
     <DurationTime>20</DurationTime>
     <Message>Welcome to the Smart Meter Texas Portal!</Message>
     <MCTransmission>0</MCTransmission>
```

```
            <MCPriority>0</MCPriority>
            <MCConfirmation>0</MCConfirmation>
          </SimpleMessageBlock>
        </SMTxPSimpleMessageRequest>
      </smt:processSimpleMessaging>
    </soapenv:Body>
  </soapenv:Envelope>
```

When sending a request to display a simple text message, the SMT request will include:

- A message header
- An address block
- Display request information as described in Table 22**Error! Reference source not found.**.

Element	Mandatory	Type	Description
MessageID	Y	Int	Message Identifier, Requestor issued
StartTime	Y	dateTime	The time at which the message becomes valid. Requestor provides value. For "now", use 2000-01-01T00:00:00Z
DurationTime	Y	Int	SEP defines a range from 0 to 0xFFFF. In Release 1, the maximum number of minutes allowed is 255.
Message	Y	string(80)	As per SEP
MCTransmission	Y	Int	Values are per SEP: 0 Secured/normal 1 InterPAN 2 Secured & InterPAN In Release 1, SMT will only allow a value of 0.
MCPriority	Y	Int	Values are per SEP: 0 Low 1 Medium 2 High 3 Critical
MCConfirmation	Y	Int	Values are per SEP: 0 confirmation not required 1 confirmation required

Table 22: Smart Energy text display request information

5.4.3.2 Canceling Simple Text/Display Messages

SMT will perform validations, save the request, and send a cancellation acknowledgement. The message status for the cancellation at this point will be *request Accepted*. If there is a failure, the status will be request rejected.

SMT will formulate cancellation requests and send it to the TDSPs. The TDSP is will acknowledge the message or return a failure .The request status becomes *Request Acknowledged by TDSP* when the TDSP returns an acknowledgement or *Failure* if a failure condition is returned.

The TDSP may return additional Status regarding the request later. SMT will store the simple text messaging request cancellation Status that are returned. The format of the cancel text message is described in Table 11.

A sample simple text message cancellation request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
  </wsse:Security>
 </soapenv:Header>
  <soapenv:Body>
   <smt:processCancelSimpleMessage>
    <SMTxPCancelSimpleMessageRequest>
     <!--Optional  RequestID removed -->
     <RequesterType>3</RequesterType>
     <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
     <RequesterID>ADMIN2</RequesterID>
     <RequestPriority>L</RequestPriority>
     <!--Optional: CallbackUri removed -->
     <AddressBlock>
      <!--Optional: GroupID removed -->
      <AddressList>
       <!--0 to 10000 repetitions:-->
       <Address>
        <ESIID>00000000000000001</ESIID>
        <MeterSerialNumber>00000000000000098</MeterSerialNumber>
        <DeviceMACAddr>101BC50070000502</DeviceMACAddr>
       </Address>
      </AddressList>
     </AddressBlock>
     <CancelSimpleMessageBlock>
      <MessageRequestID>123</MessageRequestID>
      <MCTransmission>0</MCTransmission>
      <MCPriority>0</MCPriority>
      <MCConfirmation>0</MCConfirmation>
     </CancelSimpleMessageBlock>
    </SMTxPCancelSimpleMessageRequest>
   </smt:processCancelSimpleMessage>
  </soapenv:Body>
</soapenv:Envelope>
```

When sending a request to cancel display of a simple text message, the SMT request will include:

- A message header
- An address block
- Display cancelation request information as described in the table below.

Element	Mandatory	Type	Description
MessageRequestID	Y	string(32)	This is the SMT-generated value sent in the header of the original text display request.
MessageID	Y	Int	This message id assigned by the requester in the original display text request.
MCTransmission	Y	Int	Values are per SEP: 0 Secured/normal 1 InterPAN 2 Secured & InterPAN SMT will only allow a value of 0.
MCPriority	Y	Int	Values are per SEP: 0 Low 1 Medium 2 High 3 Critical
MCConfirmation	Y	Int	Values are per SEP: 0 confirmation not required 1 confirmation required

Table 23: Smart Energy text display cancelation information

5.4.4 Load Control Messaging

A requestor submits a load control event request to be displayed through the SMT API. SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester is authorized to send a load control event to addressed devices. If the load control event request passes business validation checks, SMT assigns a unique identifier, saves the request, and sends an acknowledgement. The request status at this point will be *Request Accepted*. If the request fails any of these checks, a failure is returned in a Request Acknowledgement in the form of request rejected.

SMT will create a copy and send to the respective TDSPs based on the addressing schemes. When the request is sent, the TDSP may perform initial validation on the load control event request and then to acknowledge the request or return a failure indicator.

The TDSP will perform additional validations on the load control event request after returning the acknowledgement. If a failure occurs, the TDSP will return the failure status to SMT. Otherwise, the load control event request is executed and the execution status is returned. In either case, SMT will store the load control event request status that is returned.

The figure below shows the interface exchanges for creating load control events.

Load Control Messaging

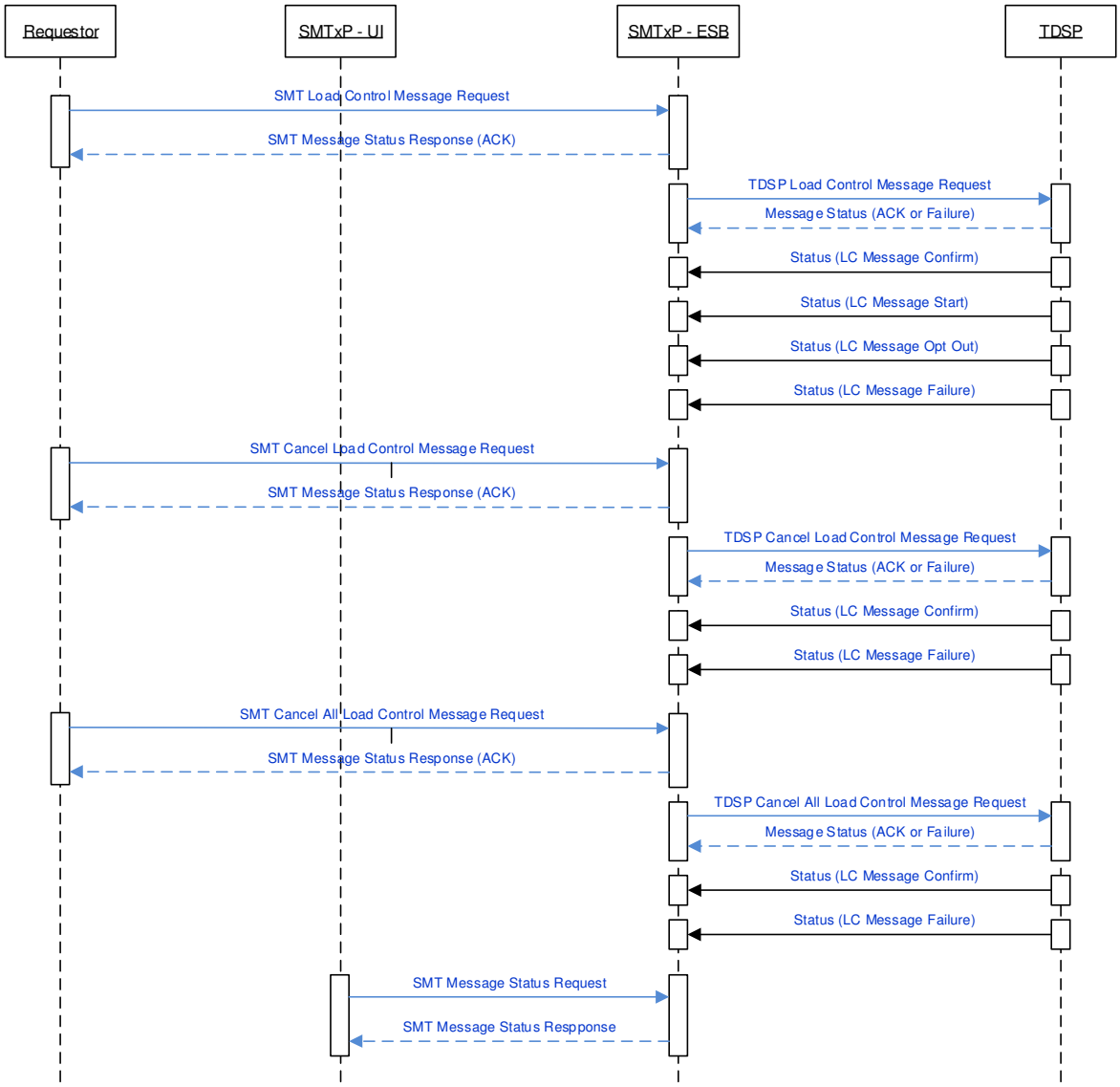


Figure 18: Creating and canceling load control events

Figure 18 also shows the process by which load control events are cancelled. The requester can cancel a single event or cancel all load control events through the front-end web services API. SMT will perform validations, save the request, and send a cancellation acknowledgement. The message status for the cancellation at this point will be *Message Accepted*. (Change this)

SMT will formulate the appropriate cancellation request and send it to the TDSPs. The TDSPs will acknowledge the message or return a failure. SMT will log acknowledgements from all TDSPs. The TDSP may return additional status regarding the request later.

5.4.5 Creating a Load Control Event

A sample load control event request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
 </wsse:Security>
</soapenv:Header>
 <soapenv:Body>
  <smt:processLoadControlEvent>
   <SMTxPLoadControlEventRequest>
    <!--Optional  RequestID removed -->
    <RequesterType>3</RequesterType>
    <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
    <RequesterID>ADMIN2</RequesterID>
    <RequestPriority>L</RequestPriority>
    <!--Optional: CallbackUri removed -->
    <AddressBlock>
     <!--Optional: GroupID removed -->
     <AddressList>
      <!--0 to 10000 repetitions:-->
      <Address>
       <ESIID>00000000000000001</ESIID>
       <MeterSerialNumber>00000000000000098</MeterSerialNumber>
      </Address>
     </AddressList>
    </AddressBlock>
    <LCMessageBlock>
     <EventID>135</EventID>
     <StartTime>2000-01-01T00:00:00Z</StartTime>
     <DurationTime>180</DurationTime>
     <DeviceClass>0000000000000000</DeviceClass>
     <UtilityEnrollmentGroup>0</UtilityEnrollmentGroup>
     <CriticalityLevel>4</CriticalityLevel>
     <EventControl>0</EventControl>
    </LCMessageBlock>
   </SMTxPLoadControlEventRequest>
  </smt:processLoadControlEvent>
 </soapenv:Body>
</soapenv:Envelope>
```

When sending a request to create a load control event, the SMT request will include:

- A message header
- An address block
- Load control request information as described in the table below.

Element	Mandatory	Type	Description
EventID	Y	Int	Event identifier, unique within messages. Requestor assigned EventID
StartTime	Y	dateTime	The time at which the message becomes valid. Requestor provided value. For "now", use 2000-01-01T00:00:00Z
DurationTime	Y	Int	As per SEP: allowed values are 1 to 1440
DeviceClass	Y	string(16)	This is a bitmap value as related to Table D.2 in Section D.2.2.3.1.1.1 in revision 15 of the Smart Energy Profile Spec (page 143). That table defines a bit map for Load Control the device class. Bit 0 (right-most bit) controls HVAC compressors or furnaces. Bit 1 controls Strip and baseboard heaters..... Bit 11 controls Generation systems. Bits 12-15 are reserved. The SMT API will accept a string(16) value. Counting characters from the right, characters 1-12 must be a "0" or a "1". ACK=FLR is returned if this value deviates from these rules.
UtilityEnrollmentGroup	Y	Int	Per SEP: Range 0 - 255
CriticalityLevel	Y	Int	Per SEP: Range of 1-9
CoolingTemperationOffset	N	Int	Per SEP
HeatingTemperatureOffset	N	Int	Per SEP
CoolingTemperationSetPoint	N	Int	Per SEP, Range -27315 to 32766 & 32768
HeatingTemperatureSetPoint	N	Int	Per SEP, Range -27315 to 32766 & 32768
AverageLoadAdjustPercent	N	Int	As per SEP: Range of -100 to 100 or 128(0x80) which indicates the field is not used.
DutyCycle	N	Int	As per SEP: Range of 0 to 100 & 255 for NULL
EventControl	Y	Int	Values are per Zigbee: 0 – do not randomize start time, do not randomize end time 1 – randomize start time, do not randomize end time 2 – do not randomize start time, randomize end time 3 – randomize start and end times

Table 24: Smart Energy Load control request information

5.4.6 Canceling a Load Control Event

A sample load control event cancelation request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
  <soapenv:Header>
    <wsse:Security xmlns:wsse=
      "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
```

```
 <wsse:UsernameToken>
  <wsse:Username>REP_Sytem_Account</wsse:Username>
 </wsse:UsernameToken>
 </wsse:Security>
</soapenv:Header>
 <soapenv:Body>
  <smt:processCancelLCEvent>
   <SMTxPCancelLoadControlEventRequest>
    <!--Optional  RequestID removed -->
    <RequesterType>3</RequesterType>
    <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
    <RequesterID>ADMIN2</RequesterID>
    <RequestPriority>L</RequestPriority>
    <!--Optional: CallbackUri removed -->
    <AddressBlock>
     <!--Optional: GroupID removed -->
     <AddressList>
      <!--0 to 10000 repetitions:-->
      <Address>
       <ESIID>00000000000000001</ESIID>
       <MeterSerialNumber>00000000000000098</MeterSerialNumber>
       <DeviceMACAddr>101BC50070000502</DeviceMACAddr>
      </Address>
     </AddressList>
    </AddressBlock>
    <CancelLCMessageBlock>
     <LCMessageID>?</LCMessageID>
     <EventID>135</EventID>
     <StartTime>2000-01-01T00:00:00Z</</StartTime>
     <DeviceClass>0000000000000000</DeviceClass>
     <UtilityEnrollmentGroup>0</UtilityEnrollmentGroup>
     <CancelControl>0</CancelControl>
    </CancelLCMessageBlock>
   </SMTxPCancelLoadControlEventRequest>
  </smt:processCancelLCEvent>
 </soapenv:Body>
</soapenv:Envelope>
```

When sending a request to cancel a load control event, the SMT request will include:

- A message header
- An address block
- Load control cancellation request information as described in Table 25.

If a load control event is cancelled for a specific load control event then the event id should be included in the load control cancellation request information.

If a load control event is cancelled for a set of ESIIDs, those ESIIDs and meter serial numbers will be included in individual AddressBlock elements with an AddressBlockList element. See section 6 for more information on these elements.

In the current release, CNP will cancel all load cancel events if no specific load control event id is included in the request.

Element	Mandatory	Type	Description
LCRequestID	Y	string	Original RequestID of the LC Message
EventID	Y	string(32)	EventID of issued event that needs to be cancelled
EffectiveTime	Y	dateTime	The time at which the message becomes valid. Requestor provides value. For "now", use 2000-01-01T00:00:00Z
DeviceClass	Y	string(16)	This is a bitmap value as related to Table D.3 in Section D.2.2.3.2.1. in revision 15 of the Smart Energy Profile Spec (page 148). That table defines a bit map for Load Control the device class. Bit 0 (right-most bit) controls HVAC compressors or furnaces. Bit 1 controls Strip and baseboard heaters..... Bit 11 controls Generation systems. Bits 12-15 are reserved. The SMT API will accept a string(16) value. Counting characters from the right, characters 1-12 must be a "0" or a "1". ACK=FLR is returned if this value deviates from these rules.
UtilityEnrollmentGroup	Y	Int	Per SEP: Range 0 - 255
CancelControl	Y	Int	As per SEP: 0 do not randomize 1 randomizes

Table 25: Smart Energy Load control cancellation request information

5.4.7 Canceling all Load Control Events

A sample request to cancel all load control events appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
  </wsse:Security>
 </soapenv:Header>
 <soapenv:Body>
   <smt:processCancelAllLCEvents>
     <SMTxPCancelAllLoadControlEventRequest>
       <!--Optional  RequestID removed -->
       <RequesterType>3</RequesterType>
       <RequesterAuthenticationID>111111111</RequesterAuthenticationID>
       <RequesterID>ADMIN2</RequesterID>
```

```
        <RequestPriority>L</RequestPriority>
        <!--Optional: CallbackUri removed -->
        <AddressBlock>
          <!--Optional: GroupID removed -->
          <AddressList>
            <!--0 to 10000 repetitions :-->
            <Address>
              <ESIID>00000000000000001</ESIID>
              <MeterSerialNumber>00000000000000098</MeterSerialNumber>
            </Address>
          </AddressList>
        </AddressBlock>
        <CancelAllLCEventMessageBlock>
          <CancelControl>0</CancelControl>
        </CancelAllLCEventMessageBlock>
      </SMTxPCancelAllLoadControlEventRequest>
    </smt:processCancelAllLCEvents>
  </soapenv:Body>
</soapenv:Envelope>
```

When cancelling all load control events, the SMT request will include:

- A message header.
- An address block
- Load control cancellation request information as described in the table below.

Element	Mandatory	Type	Description
CancelControl	Y	Int	Values are per Zigbee: 0 do not randomize 1 randomize

Table 26: Smart Energy Request information for canceling all load control events

5.4.8 Sending Price Signals

The requestor submits a price signal request to be passed through the SMT API. SMT performs two levels of validations:

- XML validation is performed by an appliance on the SMT perimeter. If the request fails validation, a SOAP fault is returned.
- If XML is formatted correctly, business validations are performed by SMT. SMT validates that the requester is authorized to send pricing signals to the devices. If the price signal request passes business validation checks, SMT assigns a unique identifier, saves the request, and sends an acknowledgement. The request status at this point will be *Request Accepted*. If the request fails any of these checks, a failure is returned in a Request Acknowledgement in the form of request rejected.

SMT will create a copy and send to the respective TDSPs based on the addressing schemes when the request is sent, the TDSP may perform minimal validation on the price signal request and then will acknowledge the request or return a failure.

Figure 19 shows the interface exchange for sending a price signal message.

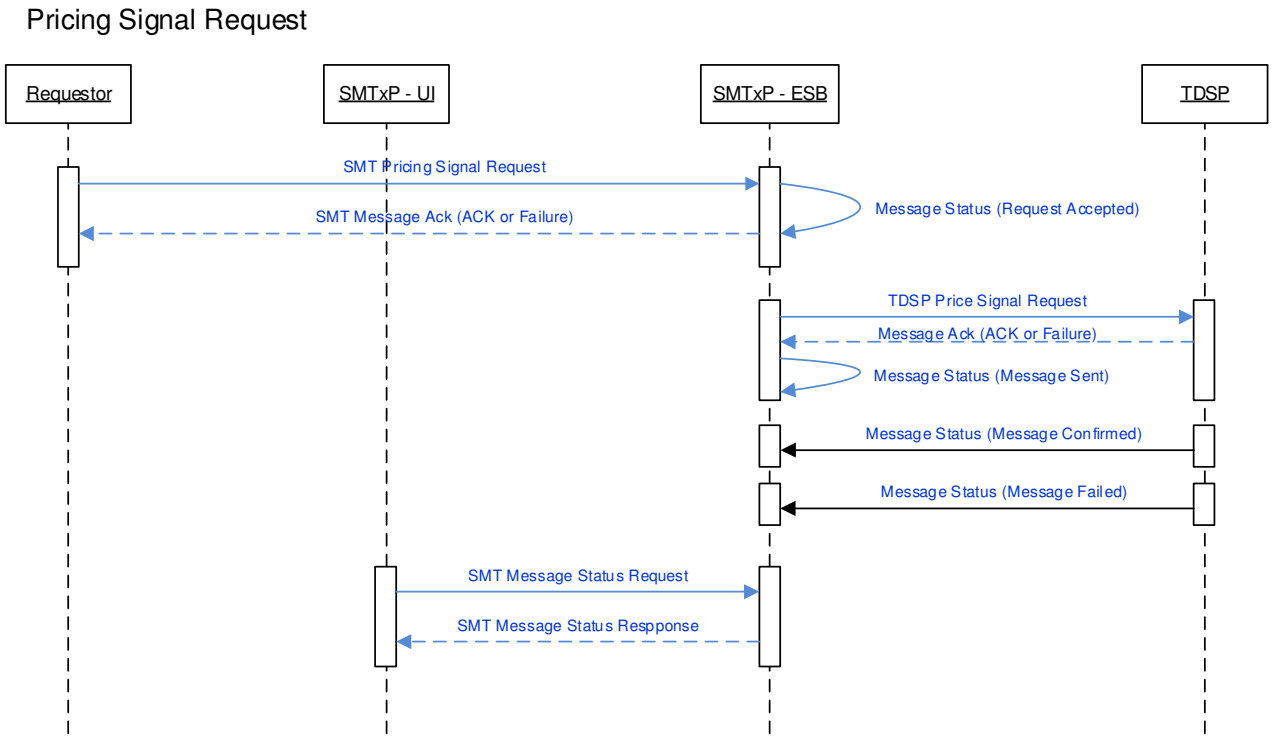


Figure 19: Sending a price signal request.

5.4.9 Sending Price Signal Request

A sample price signal request appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
 <soapenv:Header>
  <wsse:Security xmlns:wsse=
   "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <wsse:UsernameToken>
   <wsse:Username>REP_Sytem_Account</wsse:Username>
  </wsse:UsernameToken>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body>
   <smt:processPricingMessage>
     <SMTxPPriceSignalRequest>
       <!--Optional  RequestID removed -->
       <RequesterType>3</RequesterType>
       <RequesterAuthenticationID>1234567890123</RequesterAuthenticationID>
       <RequesterID>ADMIN2</RequesterID>
```

```
<RequestPriority>L</RequestPriority>
<!--Optional: CallbackUri removed -->
<AddressBlock>
  <!--Optional: GroupID removed -->
   <AddressList>
    <!--0 to 10000 repetitions:-->
     <Address>
       <ESIID>12345678901234567</ESIID>
       <MeterSerialNumber>1234567890123456789012</MeterSerialNumber>
       <DeviceMACAddr> ABCD123456789012</DeviceMACAddr>
     </Address>
  </AddressList>
</AddressBlock>
<PriceMessageBlock>
  <ProviderID>123456789</ProviderID>
  <RateLabel>Rate Label-1</RateLabel>
  <IssuerEventID>123456789</IssuerEventID>
  <CurrentTime></CurrentTime>
  <UOM>0</UOM>
  <Currency>USD</Currency>
  <PriceTier>1</PriceTier>
  <PriceTrailingDigit>4</PriceTrailingDigit>
  <RegisterTier>1</RegisterTier>
  <StartTime>2000-01-01T00:00:00Z</</StartTime>
  <Duration>180</Duration>
  <Price>12545</Price>
  <GenerationPrice>12400</GenerationPrice>
</PriceMessageBlock>
</SMTxPPriceSignalRequest>
</smt:processPricingMessage>
</soapenv:Body>
</soapenv:Envelope>
```

When sending a price signal request, the SMT request will include:

- A message header
- An address block
- Display request information as described in the table below.

Element	Mandatory	Type	Description
ProviderID	Y	Int	Provider ID (limited to 9 digits) – Requestor will provide a unique number for Provider. Discussion of using the first 9 digits of the requestor's DUNS possibly, or a different identifier chosen by requestor.
RateLabel	Y	String(12)	Rate Label
IssuerEventID	Y	Int	Issuer Event ID – Mandatory in SEP, unique identifier controlled by requestor for message.
CurrentTime	Y	dateTime	Current Time – API will include current time field as mandatory for requestor and TDSP.

Element	Mandatory	Type	Description
UOM	Y	Int	Unit Of Measure – Per SEP.
Currency	Y	String(3)	Currency (USD= US Dollars) - Use ISO 4217, US Dollar=USD=840, use character value.
Price Tier	Y	Int	Price Tier – Requestor will provide. As per SEP - 0 means no Tiers, values 1 thru 6 indicate a Price Tier. Tier 1 is the least expensive. Tier 6 is the most expensive.
Price Trailing Digit	Y	Int	Price Trailing Digit – Requestor will provide. As per SEP - number of digits to right of the decimal point in the price field.
Register Tier	Y	Int	Register Tier (4 bits Unsigned – Range 0 to 15) -As per SEP - Table D.31 in spec. 0 means no tier related. Register Tier values of 1 thru 6 allowed.
Start Time	Y	dateTime	The time at which the message becomes valid. REP provided value. For “now”, use 2000-01-01T00:00:00Z
Duration	Y	Int	Duration (in minutes) - Requestor will provide. As per SEP, 16 bits, a max value of 0xffff (=65535) would mean stay in place until changed, by a subsequent Price message.
Price	Y	Int	Price – Requestor will provide. As per SEP.
Price Ratio	N	Int	Price Ratio per SEP.
GenerationPrice	N	Int	Generation Price per SEP.
GenerationRatio	N	Int	Generation Price Ratio per SEP.
AlternateCostDelivered	N	Int	Alternate Cost Delivered per SEP.
AlternateCostUnit	N	Int	Alternate Cost Unit per SEP.
AlternateCostTrailingDigit	N	Int	Alternate Cost Trailing Digit per SEP.

Table 27: Smart Energy price signal request information

Per SEP - Nested and overlapping Publish Price commands are not allowed. The current active price will be replaced if new price information is received by the ESI.

5.4.10 Smart Energy Messaging Request Acknowledgement

When a SEP messaging request is sent to SMT, an appliance on the SMT perimeter performs XML validation. If the request fails validation, a SOAP fault is returned. If the request passes XML validation, it is passed to SMT. SMT ESB performs business validations and returns a Messaging Request Acknowledgement

A sample messaging acknowledgement appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header/>
  <soapenv:Body>
    <sm:processLoadControlEventResponse xmlns:sm="http://schemas.esb.ams.com/smtxpmessaging">
      <SMTxPMessageAck>
        <RequestID>2930</RequestID>
        <RequestStatus>Success</RequestStatus>
```

```
        <RequestStatusDesc>Request Accepted</RequestStatusDesc>
      </SMTxPMessageAck>
    </sm:processLoadControlEventResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

The Smart Energy message acknowledgement contains header information and zero or more invalid request elements. The Smart Energy messaging acknowledgement header record includes the 3 elements described in the table below.

Element	Mandatory	Type	Description
RequestID	Y	string(32)	Unique Request ID which is generated by SMT
RequestStatus	Y	string(3)	Values returned are: ACK - Acknowledgement indicating the request was accepted for further processing. FLR - Failure, indicating the request was not accepted for processing
RequestStatusDesc	N	string	Request Status Description

Table 28: Smart Energy messaging request acknowledgement header record

If a Smart Energy messaging request is sent with invalid addressing information, the invalid information will be returned as one or more invalid request elements. The elements of an invalid request record appear in the table below.

Element	Mandatory	Type	Description
ESIID	Y	string(17,64)	Energy Service Interface identifier
MeterSerialNumber	Y	string(30)	TDSP Meter manufacturer serial number
DeviceMACAddr	N	string(16)	Device MAC Address
Reason	N	string(128)	Reason of Failure at individual ESIID

Table 29: Smart Energy messaging acknowledgement invalid request element record

5.5 In-Home Device Messaging Examples

5.5.1 Simple Message Example

The following example illustrates how to send a simple message that starts immediately for a duration of 30 minutes. No confirmation (0) is required for this simple message.

```
<SimpleMessageBlock>
  <MessageID>58158</MessageID>
  <StartTime>2000-01-01T00:00:00Z</StartTime>
  <DurationTime>30</DurationTime>
  <Message>Simple Message Test</Message>
  <MCTransmission>0</MCTransmission>
```

```
    <MCPriority>0</MCPriority>
    <MCConfirmation>0</MCConfirmation>
  </SimpleMessageBlock>
```

5.5.2 Simple Message Block

The following is a brief explanation of the elements of the Simple Message block.

SimpleMessageBlock		Y	segment	
	MessageID	Y	int	An unique number assigned to the simple message by the requestor. For example, requestor can increment the number each time request is submitted
	StartTime	Y	dateTime	Examples: 2000-01-01T00:00:00Z this start time is used whenever you want the message to start immediately. 2012-02-23T14:15:00Z to start Feb 23, 2012 at 8:15 AM CST. The 2 zeros on the end represent seconds and rarely other than 00 used. The 14:15 is UTC or Greenwich Mean Time – CST +6hr). You have the option of using local time, leaving out the Z at the end. See the next line for an example which is commented out. 2012-02-23T17:00:00 example using local time to start Feb 23, 2012 at 5:00 PM CST It is recommended to use UTC time with the Z at the end
	DurationTime	Y	int	Duration of the simple message in minutes - from 1 minute to 1440 minutes (1 day)
	Message	Y	string(80)	String containing the message to be delivered (max 80 characters)
	MCTransmission	Y	int	No SMT logic behind this element, not used, enter 0
	MCPriority	Y	int	Per SEP: 0 Low, 1 Medium, 2 High, 3 Critical, but no SMT logic behind this element
	MCConfirmation	Y	int	Per SEP: 0 confirmation not required, 1 confirmation required. When the recipient enters confirmation on the HAN Device, a meter event log will be created

5.5.3 Load Control Messaging Temperature Set Point

The following example illustrates how to send a load control message to set the cooling temperature setpoint to 30 deg C (3000 in the example below) and the heating temperature setpoint to 15 deg C (1500 in the example below). Since the start time has been set to 2000-01-01T00:00:00Z, this load control event will be started immediately for a duration of 30 minutes. All In-Home Devices, regardless of the utility enrollment group they are assigned to, will receive the event as the Utility Enrollment Group in the load control event has been set to 0.

Duty Cycle is 255 or NULL which means that the load control switches will not react to this load control event.

```
  <LCMessageBlock>
    <EventID>12348911</EventID>
    <StartTime>2000-01-01T00:00:00Z</StartTime>
    <DurationTime>30</DurationTime>
    <DeviceClass>0000111111111111</DeviceClass>
```

```
  <UtilityEnrollmentGroup>0</UtilityEnrollmentGroup>
  <CriticalityLevel>1</CriticalityLevel>
  <CoolingTemperationSetPoint>3000</CoolingTemperationSetPoint>
  <HeatingTemperatureSetPoint>1500</HeatingTemperatureSetPoint>
  <DutyCycle>255</DutyCycle>
  <EventControl>0</EventControl>
</LCMessageBlock>
```

5.5.4 Load Control Messaging Temperature Offset

The following example illustrates how to send a load control message to set the cooling temperature offset 2 deg C (20 in the example below) and the heating temperature offset 3 deg C (30 in the example below). Since the start time has been set to 2012-02-23T14:15:00Z, this load control event will be started Feb 23, 2012 at 8:15 AM CST. The 2 zeros on the end represent seconds and rarely other than 00 used. The 14:15 is UTC or Greenwich Mean Time – CST +6hr). The duration of the load control event is 45 minutes. All In-Home Devices, regardless of the utility enrollment group they are assigned to, will receive the event as the Utility Enrollment Group in the load control event has been set to 0.

Duty Cycle is 255 or NULL which means that the load control switches will not react to this load control event.

```
<LCMessageBlock>
  <EventID>12348911</EventID>
  <StartTime>2012-02-23T14:15:00Z</StartTime>
  <DurationTime>45</DurationTime>
  <DeviceClass>0000111111111111</DeviceClass>
  <UtilityEnrollmentGroup>0</UtilityEnrollmentGroup>
  <CriticalityLevel>1</CriticalityLevel>
  <CoolingTemperationOffset>20</CoolingTemperationOffset>
  <HeatingTemperatureOffset>30</HeatingTemperatureOffset>
  <DutyCycle>255</DutyCycle>
  <EventControl>0</EventControl>
</LCMessageBlock>
```

5.5.5 Load Control Messaging Temperature Offset (with Duty Cycle)

The following example illustrates how to send a load control message to set the cooling temperature offset 2 deg C (20 in the example below) and the heating temperature offset 3 deg C (30 in the example below). Since the start time has been set to 2012-02-23T14:15:00Z, this load control event will be started Feb 23, 2012 at 8:15 AM CST. The 2 zeros on the end represent seconds and rarely other than 00 used. The 14:15 is UTC or Greenwich Mean Time – CST +6hr). The duration of the load control event is 45 minutes. All In-Home Devices, regardless of the utility enrollment group they are assigned to, will receive the event as the Utility Enrollment Group in the load control event has been set to 0. Duty Cycle is 255 or NULL which means that the load control switches will not react to this load control event.

In addition, the Duty Cycle is 50 which means that the load control switches will react to this load control event. The switches will be on 50% of the time, and off 50% of the time.

```
<LCMessageBlock>
  <EventID>12348911</EventID>
  <StartTime>2012-02-23T14:15:00Z</StartTime>
  <DurationTime>45</DurationTime>
  <DeviceClass>0000111111111111</DeviceClass>
  <UtilityEnrollmentGroup>0</UtilityEnrollmentGroup>
  <CriticalityLevel>1</CriticalityLevel>
  <CoolingTemperationOffset>20</CoolingTemperationOffset>
  <HeatingTemperatureOffset>30</HeatingTemperatureOffset>
  <DutyCycle>50</DutyCycle>
  <EventControl>0</EventControl>
</LCMessageBlock>
```

5.5.6 Load Control Message Block

The following is a brief explanation of the elements of the Load Control Message block.

LCMessageBlock		Mandatory?	Description
	EventID	Y	An unique number assigned to the load control event by the requestor. For example, requestor can increment the number each time request is submitted
	StartTime	Y	Examples: 2000-01-01T00:00:00Z this start time is used whenever you want the event to start immediately. 2012-02-23T14:15:00Z to start Feb 23, 2012 at 8:15 AM CST. The 2 zeros on the end represent seconds and rarely other than 00 used. The 14:15 is UTC or Greenwich Mean Time – CST +6hr). You have the option of using local time, leaving out the Z at the end. See the next line for an example which is commented out. 2012-02-23T17:00:00 example using local time to start Feb 23, 2012 at 5:00 PM CST It is recommended to use UTC time with the Z at the end
	DurationTime	Y	Duration of the event in minutes - from 1 minute to 1440 minutes (1 day)

LCMessageBlock		Mandatory?	Description
	DeviceClass	Y	0000111111111111 - each of the 12 ones represents a device class such as an IHD, PCT, pool pump, exterior lighting, etc. This example selects all device classes). The leading four zeros are for possible future use. This is a bitmap value as related to Table D.2 in Section D.2.2.3.1.1.1 in revision 15 of the Smart Energy Profile Spec (page 143). That table defines a bit map for Load Control the device class. Bit 0 (right-most bit) controls HVAC compressors or furnaces. Bit 1 controls Strip and baseboard heaters..... Bit 11 controls Generation systems. Bits 12-15 are reserved. The SMT API will accept a string(16) value. Counting characters from the right, characters 1-12 must be a "0" or a "1". ACK=FLR is returned if this value deviates from these rules.
	UtilityEnrollmentGroup	Y	HAN Device can be assigned to a specific UEG other than zero. UEG 0 is sent to all HAN Devices. Other UEG specified indicates only those HAN Devices assigned to that specific UEG will react to the load control event. Allowed values 0 to 255 only
	CriticalityLevel	Y	The higher the number the higher priority for the event. No SMT logic behind this element
	CoolingTemperationOffset	N	The offset is in tenths of deg C. To illustrate, if 20 was entered, it would be 2 deg C or 3.6 deg F. Most HAN Devices would raise the setpoint 4 deg F if in deg F mode Range 0-255
	HeatingTemperatureOffset	N	The offset is in tenths of deg C. To illustrate, if 30 was entered, it would be 3 deg C or 5.4 deg F. Most HAN Devices would lower the setpoint 5 deg F if in deg F mode. Range 0-255
	CoolingTemperationSetPoint	N	The temperature setpoint in hundredths of degrees Centigrade. To illustrate, if 3000 was entered, it would represent 30 deg C or 86 deg F. Normally the HAN Device will round off to the nearest degree F if displaying in deg F
	HeatingTemperatureSetPoint	N	The temperature setpoint in hundredths of degrees Centigrade. To illustrate, if 1500 was entered, it would represent 15 deg C or 59 deg F. Normally the HAN Device will round off to the nearest degree F if displaying in deg F
	AverageLoadAdjustPercent	N	Defines a maximum energy usage limit as a percentage of the client implementations specific average energy usage. Optional, usually not used
	DutyCycle	N	This is for load control switches and is the percent of time during the event that the device plugged in to the switch is active. The lower the number, the more energy you save. Range of 0 to 100 & 255 for NULL
	EventControl	Y	This is to randomize start time and end time and is normally zero

5.5.7 Price Message Example

The following example illustrates how to send a price message (11 cents) that starts immediately for a duration of 30 minutes.

```
<PriceMessageBlock>
  <ProviderID>123456789</ProviderID>
```

```
<RateLabel>Rate Label1</RateLabel>
<IssuerEventID>865888</IssuerEventID>
<CurrentTime>2000-01-01T00:00:00Z</CurrentTime>
<UOM>0</UOM>
<Currency>USD</Currency>
<PriceTier>1</PriceTier>
<PriceTrailingDigit>2</PriceTrailingDigit>
<RegisterTier>1</RegisterTier>
<StartTime>2000-01-01T00:00:00Z</StartTime>
<Duration>30</Duration>
<Price>11</Price>
<PriceRatio>255</PriceRatio>
<GenerationPrice>11000</GenerationPrice>
<GenerationRatio>95</GenerationRatio>
<AlternateCostDelivered>2222</AlternateCostDelivered>
<AlternateCostUnit>1</AlternateCostUnit>
<AlternateCostTrailingDigit>4</AlternateCostTrailingDigit>
</PriceMessageBlock>
```

5.5.8 Price Message Block

The following is a brief explanation of the elements of the Price Message block.

PriceMessageBlock		**Y**	
	ProviderID	Y	DUNS number of Commodity Provider- Requestor will provide.
	RateLabel	Y	ID for the price. Requestor will provide.
	IssuerEventID	Y	Requestor will provide. Mandatory in SEP, unique identifier controlled by REP for message.
	CurrentTime	Y	API will include currenttime field as optional for requestors and TDSPs. If the requestor does not send a value through, SMTxP will supply one. -As per SEP (r15)
	UOM	Y	Unit of Measure, 0 for KW & KWH
	Currency	Y	Requestor will provide. USD for US$.
	Price Tier	Y	Requestor will provide. As per SEP - 0 means no Tiers, values 1 thru 6 indicate a Price Tier, Tier 1 is the LEAST expensive, Tier 6 is the MOST expensive. Leave capability for values up to 15 to be provided.
	Price Trailing Digit	Y	Requestor will provide. As per SEP -number of digits to right of the decimal point in the price field. There is no multiplier or divisor in the Pricing message to influence the Price sent in the message..
	Register Tier	Y	As per SEP- Table D.31 in Zigbee spec. 0 means no tier related. Regster Tier values of 1 thru 6 allowed. 10/23 - compromise for RegisterTier - Include this in the requstor and TDSP APIs as optional. If the requestor does not send a value through, each TDSP must provide their own default value based on how their meters are configured.

PriceMessageBlock		Y	
	StartTime	Y	Examples: 2000-01-01T00:00:00Z this start time is used whenever you want the event to start immediately. 2012-02-23T14:15:00Z to start Feb 23, 2012 at 8:15 AM CST. The 2 zeros on the end represent seconds and rarely other than 00 used. The 14:15 is UTC or Greenwich Mean Time – CST +6hr). You have the option of using local time, leaving out the Z at the end. See the next line for an example which is commented out. 2012-02-23T17:00:00 example using local time to start Feb 23, 2012 at 5:00 PM CST It is recommended to use UTC time with the Z at the end
	Duration	Y	Duration of the event in minutes - from 1 minute to 1440 minutes (1 day)
	Price	Y	Requestor will provide. As per SEP - 32 bits unsigned ,the Price will make use of the Price Trailing Digit field to determine the decimal point location when the commodity is delivered to the premise.
	PriceRatio	N	Requestor will provide. As per SEP - 8 bit unsigned field, a 0xff indicates the field Is not used , but 0xff equates to 255, and the example shows 255 as possible. The value displayed will always have the low end digit (least significant) placed to the right of the decimal point. In the Zigbee example valid values displayed are .1 to 25.5 , the ratio of the price denoted in the price field to the "normal" price chosen by the commodity provider.
	GenerationPrice	N	Requestor will provide. As per SEP- 32 bit unsigned integer, also uses Price Trailing digit for decimal location. A value of 0xffffffff indicates the field is not used.
	GenerationRatio	N	Requestor will provide. As per SEP - 8 bit unsigned field, a 0xff indicates the field Is not used , but 0xff equates to 255, and the example shows 255 as possible. The value displayed will always have the low end digit (least significant) placed to the right of the decimal point. In the Zigbee example valid values displayed are .1 to 25.5 , the ratio of the price denoted in the generation price field to the "normal" price chosen by the commodity provider.
	AlternateCostDelivered	N	Requestor will provide. As per SEP-AlternateCostDelivered - integer(9), optional, to be provided by requestor. As per SEP - providing a mechanism for future use
	AlternateCostUnit	N	Requestor will provide. As per SEP -AlternateCostUnit - integer(3), optional, value 0 - 255. Value 0, 2-255 are reserved at this time. To be provided by requestor. If provided, 1 means "Kg of CO 2 per unit of measure". See Table D.33 in SEP 1.0(r15)
	AlternateCostTrailingDigit	N	Requestor will provide. AlternateCostTrailingDigit - integer(1). value 0 - 9. 0 means no decimal in AlternateCostDelivered, 9 means the whole value of AlternateCostDelivered is after decimal. To be provided by requestor. If this trailing digit is omitted but AlternateCostDelivered is provided, default to 0, i.e. no decimal. As per SEP - An 8 bit BitMap field used to determine where the decimal point is located in the Alternate Cost Field. The most significant nibble (high order 4 bits in the one byte field) indicates the number of digits to the right of the decimal point.

5.5.9 Utility Enrollment Group Example

The following example illustrates how to send an update utility enrollment group message to set the UEG of the In-Home Device 001B0000B0000000 to UEG = 10. The ESIID and Meter Serial Number should also be populated accordingly.

```
<DeviceUpdateUEGRequestList>
  <DeviceUpdateUEGRequest>
    <ESIID>10000000000000000000000</ESIID>
    <MeterSerialNumber>60000000</MeterSerialNumber>
    <DeviceMACAddr>001B0000B0000000</DeviceMACAddr>
    <UtilityEnrollmentGroup>10</UtilityEnrollmentGroup>
  </DeviceUpdateUEGRequest>
</DeviceUpdateUEGRequestList>
```

5.5.10 Utility Enrollment Group Block

The following is a brief explanation of the elements of the Utility Enrollment Group message.

DeviceUpdateUEGRequest			
	ESIID	Y	Energy Service Interface identifier
	MeterSerialNumber	Y	TDSP Meter manufacturer serial number
	DeviceMACAddr	Y	Device MAC Address
	UtilityEnrollmentGroup	Y	Utility Enrollment Group min value = 0, max value = 255

5.6 Process Flow Diagrams

5.6.1 In-Home Device Provisioning API Process Flow

010. Send Provisioning request API

020. SMTxP receives provisioning request

030. SMTxP assigns request ID

040. More than 1 Device in request

[N1] Yes: request fails

[N2] No: continue validation step 065

065. Validate Meter ID

070. Validate 5 slots

080. Validate Requestor

100. Validate MAC address and Install Code

110. Validate Device not yet provisioned to the ESIID

120. Accept provisioning request

130. Make status update available to the UI

140. Create provisioning request for the TDSP that owns the ESIID

170. Send provisioning request

180. Receive provisioning request

190. Send acknowledgement

200. Update provisioning status

210. Make status available to the UI

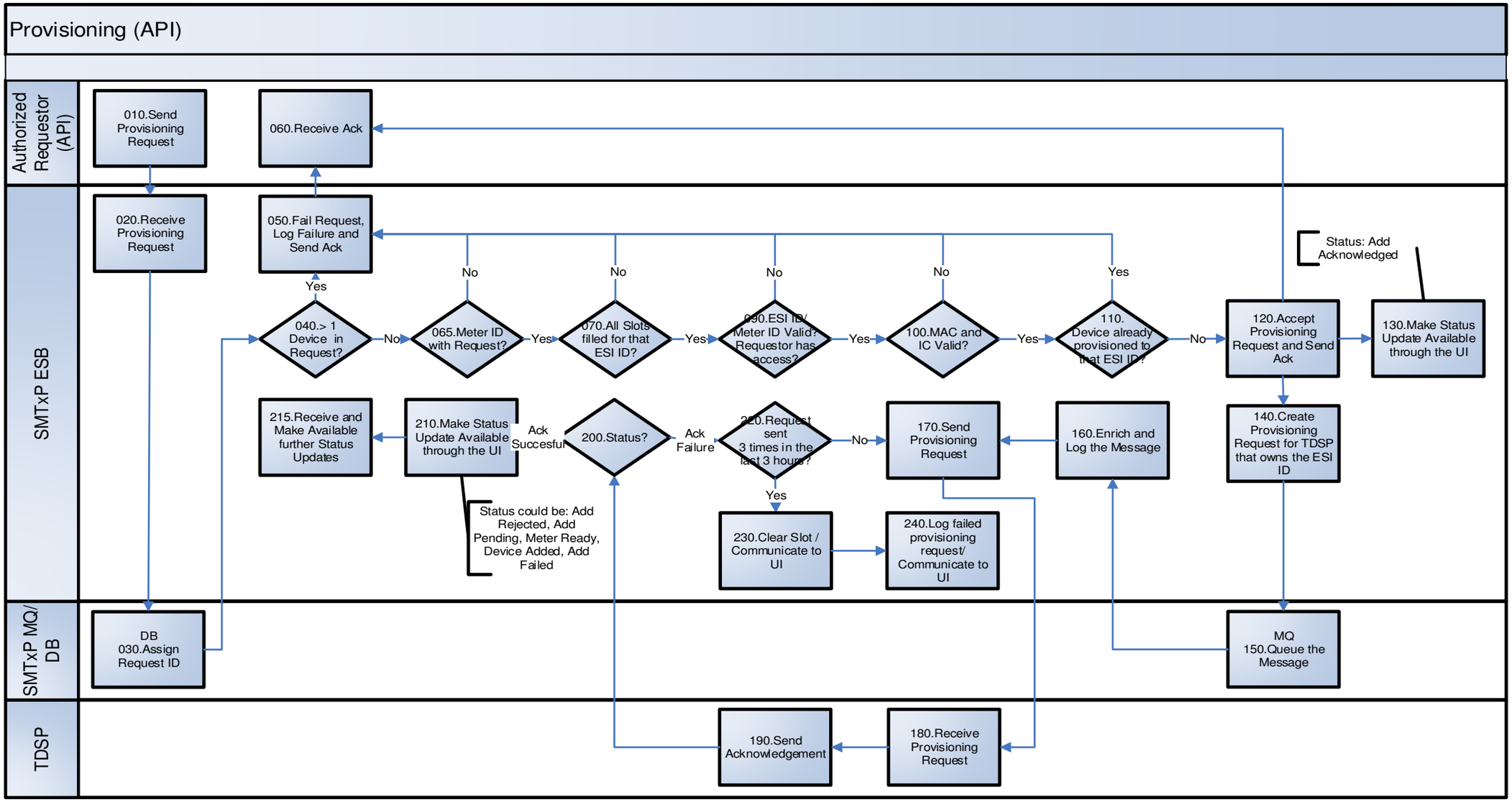


Figure 20: In-Home Device Provisioning API Process Flow

5.6.2 In-Home Device Deprovisioning API Process Flow

010. Send Deprovisioning request API

020. SMTxP receives deprovisioning request

030. SMTxP assigns request ID

040. More than 1 Device in request
    [N1] Yes: request fails
    [N2] No: continue validation step 065

065. Validate Meter ID

070. Validate ESIID

080. Validate Requestor

090. Accept request

100. Make status available to the UI

110. Create deprovisioning request for TDSP that owns the ESIID

120. SMTxP queues the message

140. Send deprovisioning request

150. Receive deprovisioning request

160. Send acknowledgement

170. Update deprovisioning status

180. Make status available to the UI

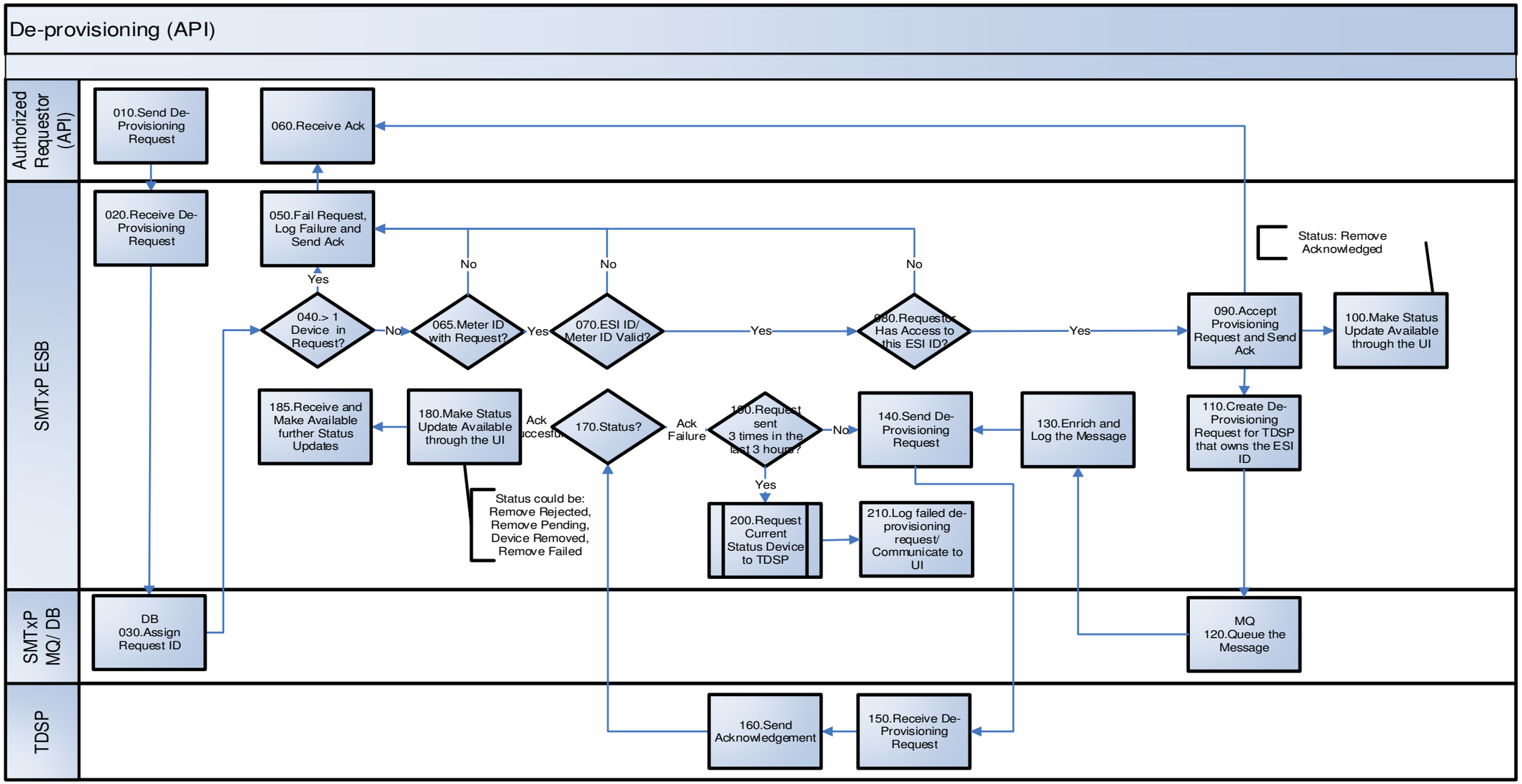


Figure 21: In-Home Device Deprovisioning API Process Flow

5.6.3 In-Home Device Messaging API Process Flow

010. Send messaging request API

020. SMTxP receives messaging request

030. Validate address block

[N1] Empty address block: request fails

[N2] DUNS only: go to step 160

[N3] DUNS and ESIID: go to step 070

[N2] ESIID only: go to step 070

070. Validate request has more than 10,000 ESIIDs

[N1] Yes: request fails

[N2] No: continue validation, go to step 065

065. Validate Meter ID

[N1] No valid meter id: request fails

[N2] Valid meter id: continue validation, go to step 120

120. Validate ESIID

[N1] No valid ESIID: request fails

[N2] Valid ESIID: continue validation, go to step 130

130. Validate Requestor

[N1] Not valid Requestor: request fails

[N2] Valid REP: continue validation, go to step 140

140. Validate mix of ESIIDs

[N1] Not valid mix: request fails

[N2] Valid mix: go to step 160

150. Accept messaging request partial success

160. Accept messaging request and send acknowledgement

170. Validate message format block according to message type

180. Message format valid

[N1] No: failed message

[N2] Yes: create messaging request for TDSP

200. Create messaging request for TDSP

210. SMTxP queues the message

220. Enhance and log the message

230. SMTxP sends messaging request

240. TDSP receives messaging request

250. TDSP sends acknowledgement

260. SMTxP receives and logs acknowledgement (270 If SMT receives FLR failure, SMT will retry to send the message)

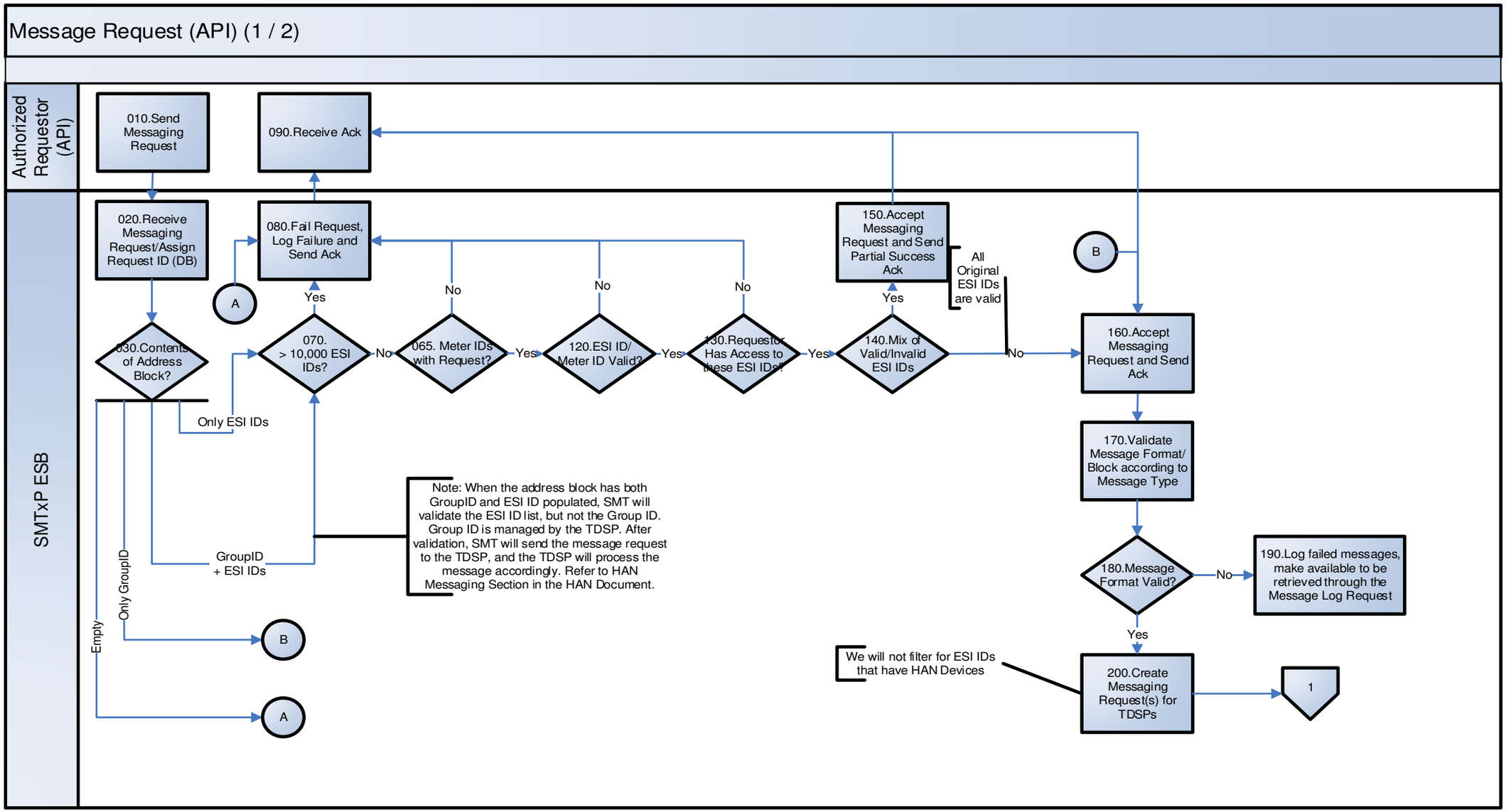

Message Request (API) (1 / 2)
Authorized Requestor (API)
SMTxP ESB
010.Send Messaging Request
090.Receive Ack
020.Receive Messaging Request/Assign Request ID (DB)
080.Fail Request, Log Failure and Send Ack
150.Accept Messaging Request and Send Partial Success Ack
All Original ESI IDs are valid
B
A
Yes
No
030.Contents of Address Block?
070. > 10,000 ESI IDs?
065. Meter IDs with Request?
120.ESI ID/ Meter ID Valid?
130.Requestor Has Access to these ESI IDs?
140.Mix of Valid/Invalid ESI IDs
160.Accept Messaging Request and Send Ack
Only ESI IDs
GroupID + ESI IDs
Only GroupID
Empty
Note: When the address block has both GroupID and ESI ID populated, SMT will validate the ESI ID list, but not the Group ID. Group ID is managed by the TDSP. After validation, SMT will send the message request to the TDSP, and the TDSP will process the message accordingly. Refer to HAN Messaging Section in the HAN Document.
170.Validate Message Format/ Block according to Message Type
180.Message Format Valid?
190.Log failed messages, make available to be retrieved through the Message Log Request
We will not filter for ESI IDs that have HAN Devices
200.Create Messaging Request(s) for TDSPs
1

Figure 22: In-Home Device Messaging API Process Flow (Part 1 of 2)

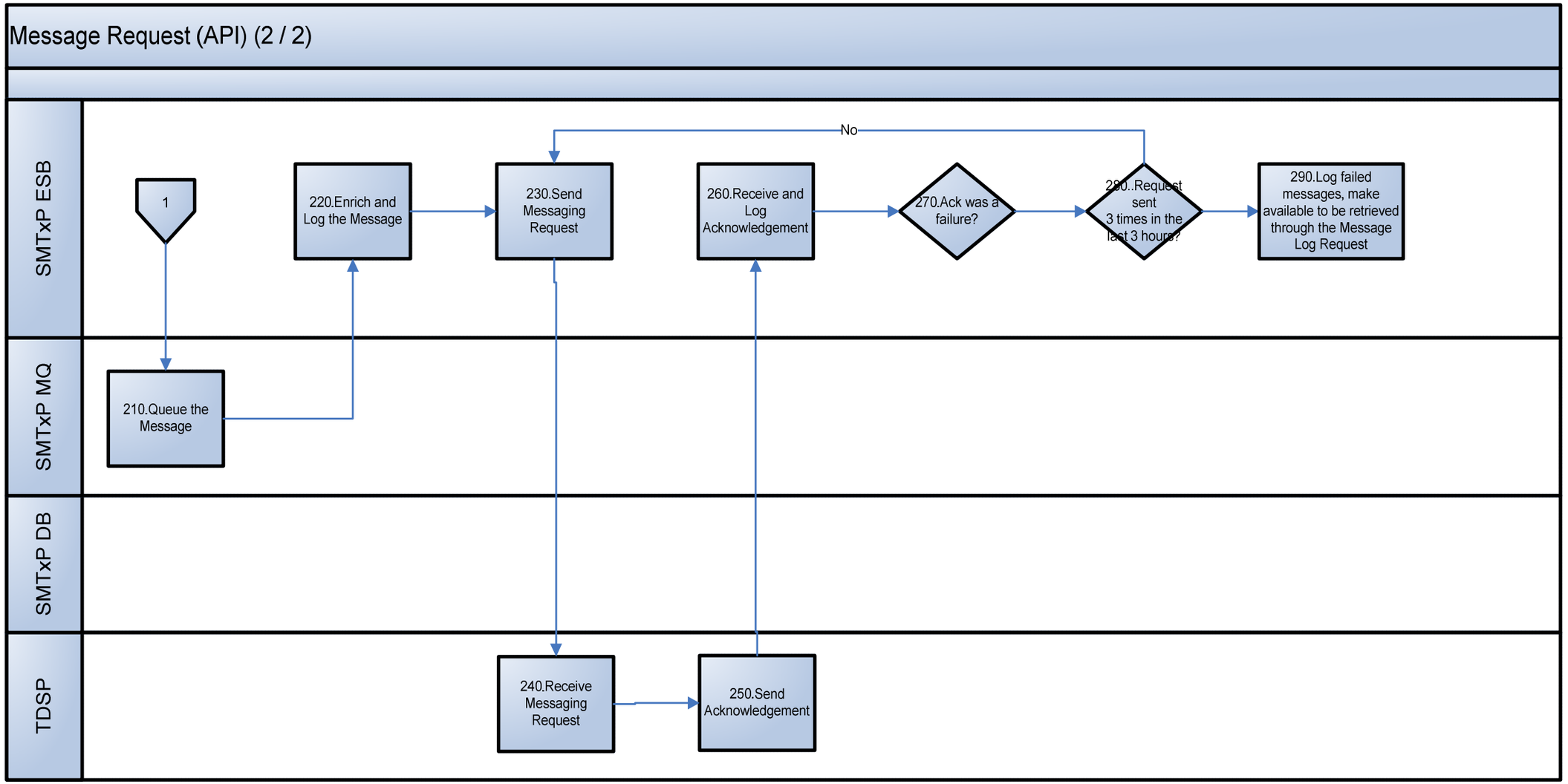


Figure 23: In-Home Device Messaging API Process Flow (Part 2 of 2)

6. In-Home Device API Starter Kit

6.1 Overview of the soapUI Starter Kit for In-Home Device Queries

This section describes soapUI Starter Kit that authorized users can use for invoking the Smart Meter Texas (SMT) In-Home Device Web Service interface.

6.1.1 Intended Audience

Users of this Starter Kit are assumed to have basic technical expertise in these areas:

- Downloading applications from the Internet
- Installation and setup of applications
- Creation and editing of XML documents
- Internet security including user ids, passwords, and the use of X.500 certificates
- Network communications including URLs, IP addresses and common network troubleshooting commands such as ping, telnet, FTP, etc.

6.1.2 About soapUI

soapUI is a free, open source desktop application available for download from http://www.soapUI.org for inspecting and invoking Web Services.

6.1.3 About this Starter Kit

This Starter Kit comes with the following:

Name	Description	File
soapUI project	Contains XML interface definitions that can be used by the soapUI application	SMT will provide the soapUI project XML. Project XML contains provisioning and messaging
SMT UAT/Staging SSL Certificate	SMT UAT/Staging SSL Certificate	 SMTxPStaging.cer
SMT In-Home Device Interface Security	Describes interface functions	See Section 7 SMT In-Home Device Interface Security

6.2 Prerequisites

This section presents the prerequisites for using the In-Home Device Starter Kit.

6.2.1 Environmental Setup

Prior to using this Starter Kit, Third-Party Service Providers (Third-Party) must provide the following Staging and/or Production information.

Staging

A REP or a Third-Party can submit this environmental information for access to the SMT Staging environment:

- SSL certification –SMT will accept a Certificate Authority (CA) or self-signed certificate. The entity needs to provide to SMT with their SSL certificate for Staging environment setup.
- Signing certificate–SMT will accept a CA or self-signed signer certificate. The entity will need to provide SMT with their signer certificate for Staging environment setup.
- DUNS – An SMT system account will be created by SMT and this account must be used when accessing the SMT Staging environment. One or more DUNS number must be associated with the SMT system account for REP. Only one DUNS number is allowed for Third-Party.
- Entity Name – This is the preferred Company name.

REP or Third-Party can submit this information via email to support@smartmetertexas.com.

Once SMT has setup the SMT System Account of the Staging environment for the entity, account information will be provided. SMT's SSL certificate is required in order to enable mutual authentication with the Staging environment. The SMT certificate is included as part of this Starter Kit.

Production

A REP or a Third-Party can submit this environmental information for access to the SMT Production environment.

- SSL certification –SMT will only accept a CA certificate. The entity needs to provide to SMT with their CA SSL certificate for Production environment setup.
- Signing certificate–SMT will accept a CA signer certificate. The entity will need to provide SMT with their CA signer certificate for Production environment setup.
- DUNS – An SMT system account will be created by SMT and this account must use when accessing the SMT Production environment. One or more DUNS number must be associated with the SMT system account for REP. Only one DUNS number is allowed for Third-Party.
- IP Address(es) – Access is restricted to the SMT Production Environment. IP Address is needed to enable access.
- Entity Name – This is the preferred Company name.

REP or Third-Party can submit this information via email to support@smartmetertexas.com.

SMT uses a CA certificate for SSL in Production. SMT's certificate will be downloaded automatically via soapUI.

Once SMT has setup the SMT system account of the Production environment for the entity, account information will be provided.

6.2.2 Key Store

An SSL KeyStore is required to invoke Web Services as part of the SMT starter kit.

The Keystore that is supported on SoapUI is JKS (Java Key Store). JKS is supported by[3]:

- iKeyMan
- Keytool and
- OpenSSL.

Staging

Self-signed or CA certificates may be used in Staging. When using self-signed certificates, follow these steps:

1. Create a JKS (Java Key Store).
2. Create Self signed SSL certificate.
3. Create Self signed signer certificate.
4. After the self signed SSL Certificate and Signer Certificates are generated, provide these two certificates to SMT.
5. Insert the self-signed certificates into the JKS if they are not put there during the creation process.

CA-issued certificates are can be used in Staging and Production so are preferred to self-signed certificates.
When using self-signed certificates, follow these steps:

1. Obtain certificates.
2. Create a JKS (Java Key Store).
3. Provide these two certificates to SMT.
4. Inserting the CA certificates into the JKS.
5. Insert the SMT Staging certificate into the JKS that is included with this Starter Kit.

Production

Only CA-issued certificate will be accepted in Production. Perform following steps:

1. Obtain certificates.
2. Create a JKS (Java Key Store).
3. Provide these two certificates to SMT.
4. Inserting the CA certificates into the JKS.

[3] iKeyMan is GUI tool for Key Management that comes as part of WAS(Websphere Application Server) and is available on <WAS_Home>/bin. One can launch iKeyMan on Dos prompt by running the command WAS_Home>/bin/iKeyMan. If WAS is not available, one has to download iKeyMan and associated jar files from Websphere Info center. If iKeyMan is used as stand alone component, the configuration steps need to be followed. Java Keytool comes as part of standard JDK.One can download JDK from http://www.java.com. OpenSSL is available on www.openssl.org.

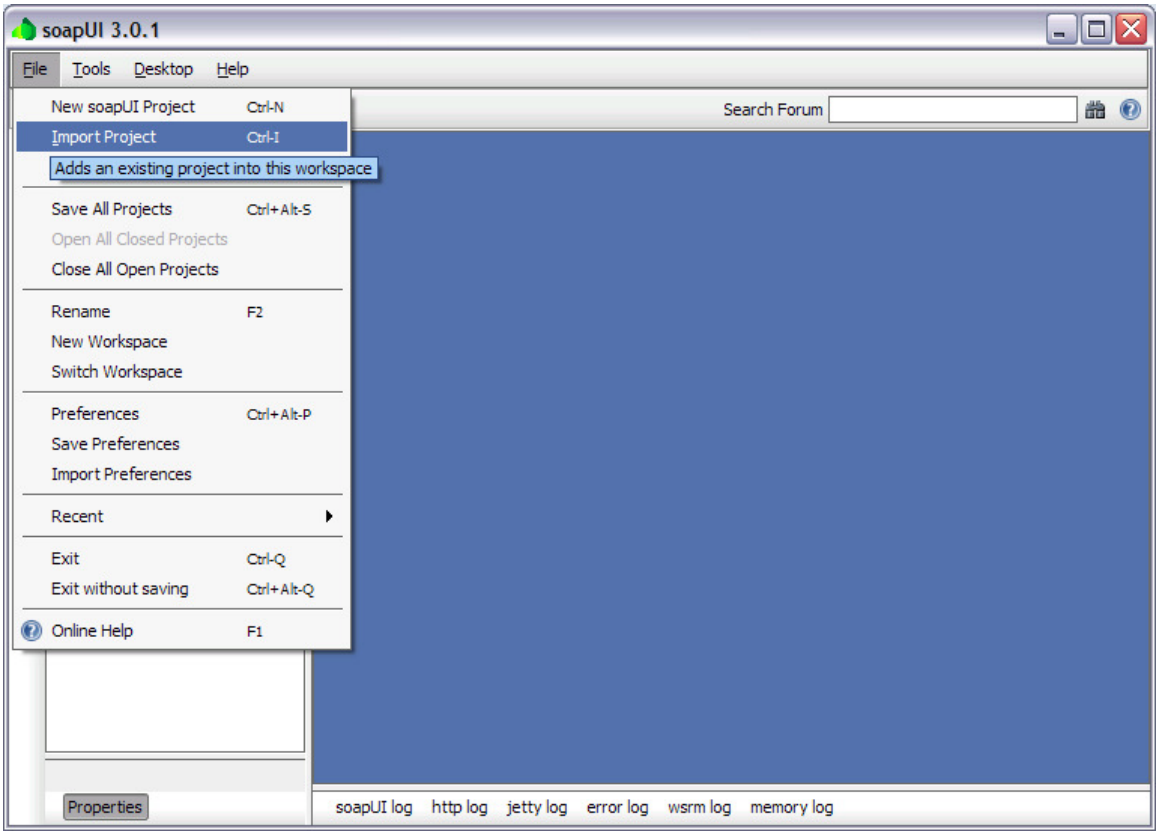
6.3 Steps for using the Starter Kit

This section covers the step by step instruction how to:

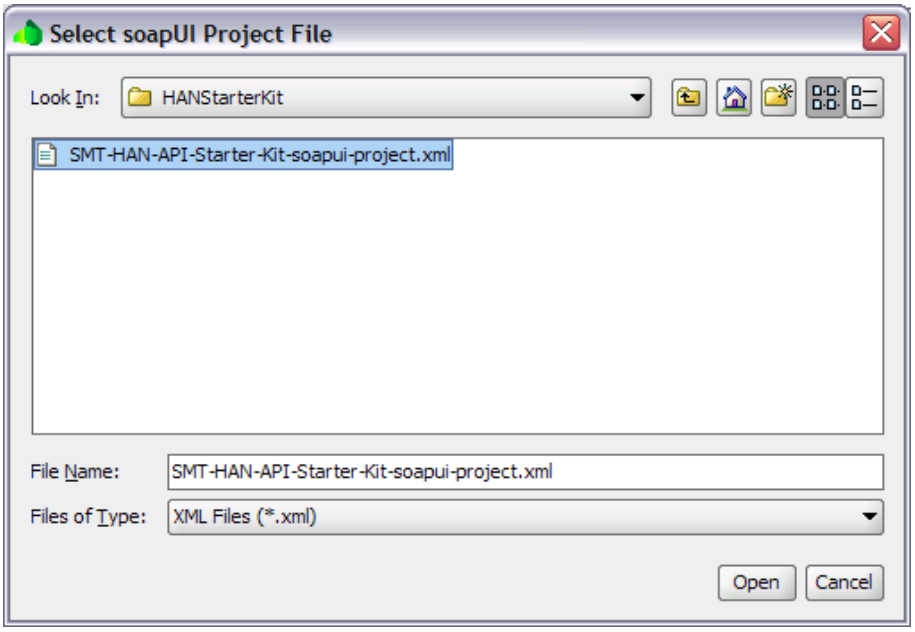
1. Set up the Starter Kit
2. Configure SSL
3. HTTP Header Configuration
4. Configure WS-Security
5. Invoke Web Services

6.3.1 Setting up the Starter Kit

Place the Starter Kit files in a target directory. Then, Launch soapUI and click on File -> Import Project as shown below.



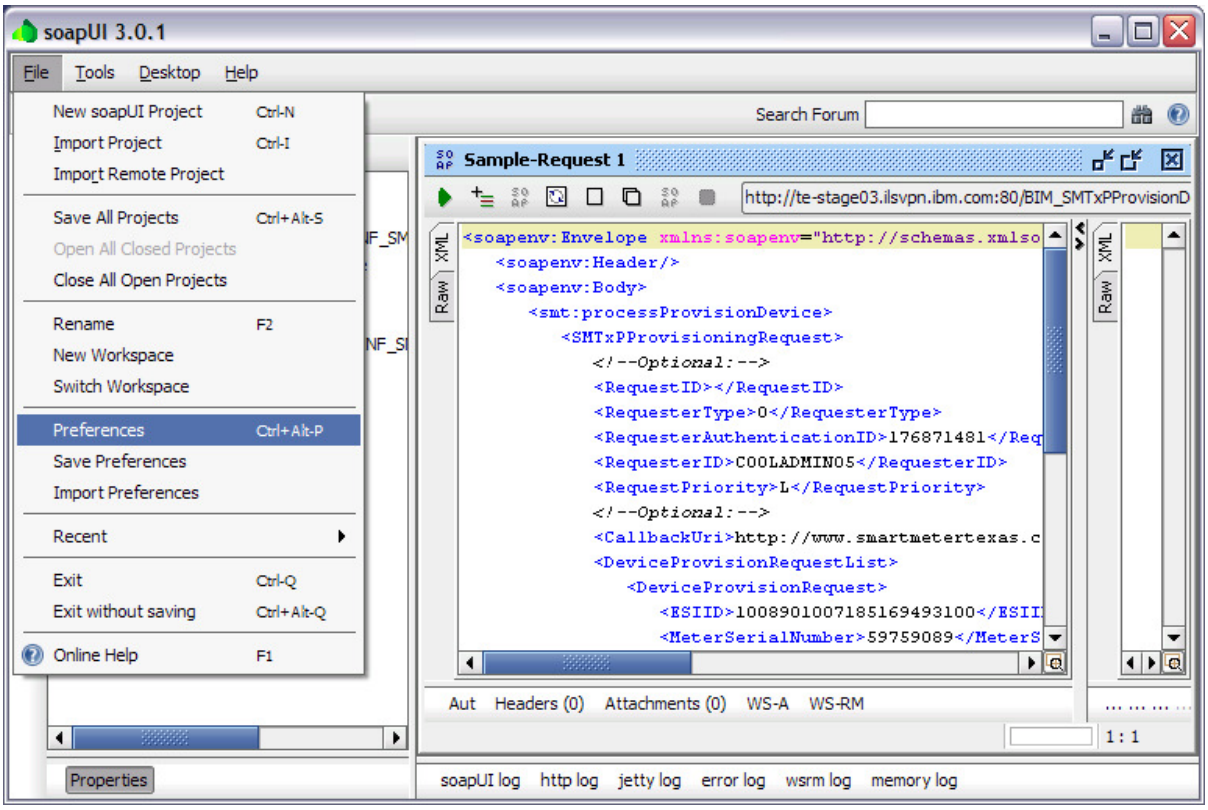
Navigate to directory and the Starter Kit project file and select it. Click Open. This is pictured below.



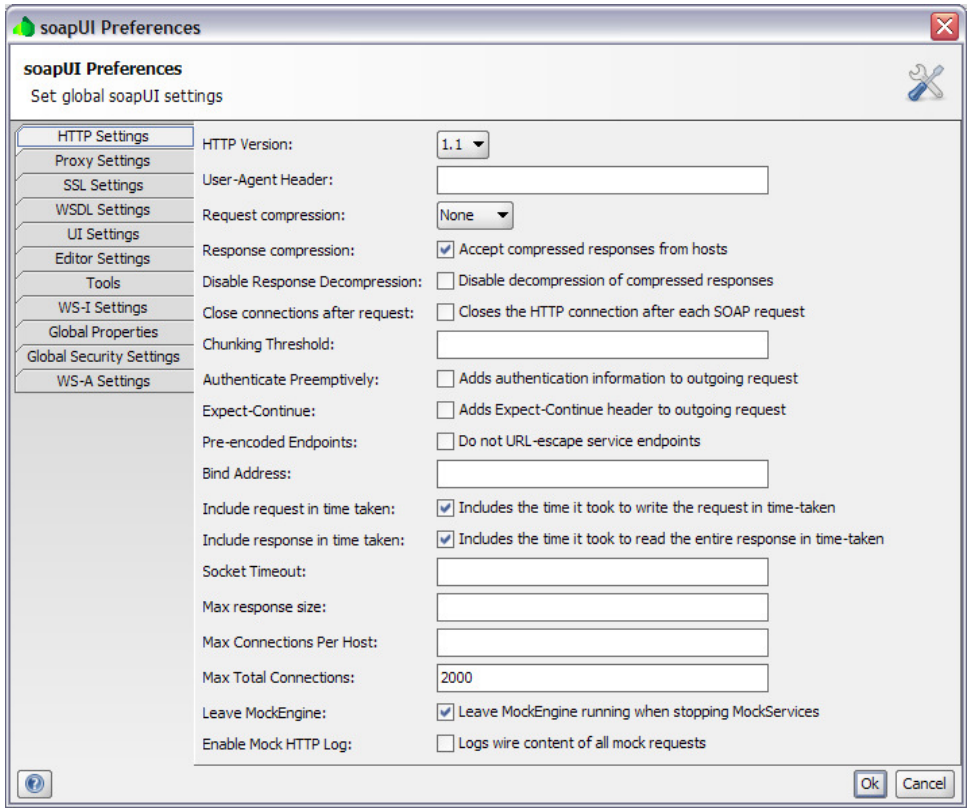
soapUI will load the Starter Kit project.

6.3.2 SSL Configuration

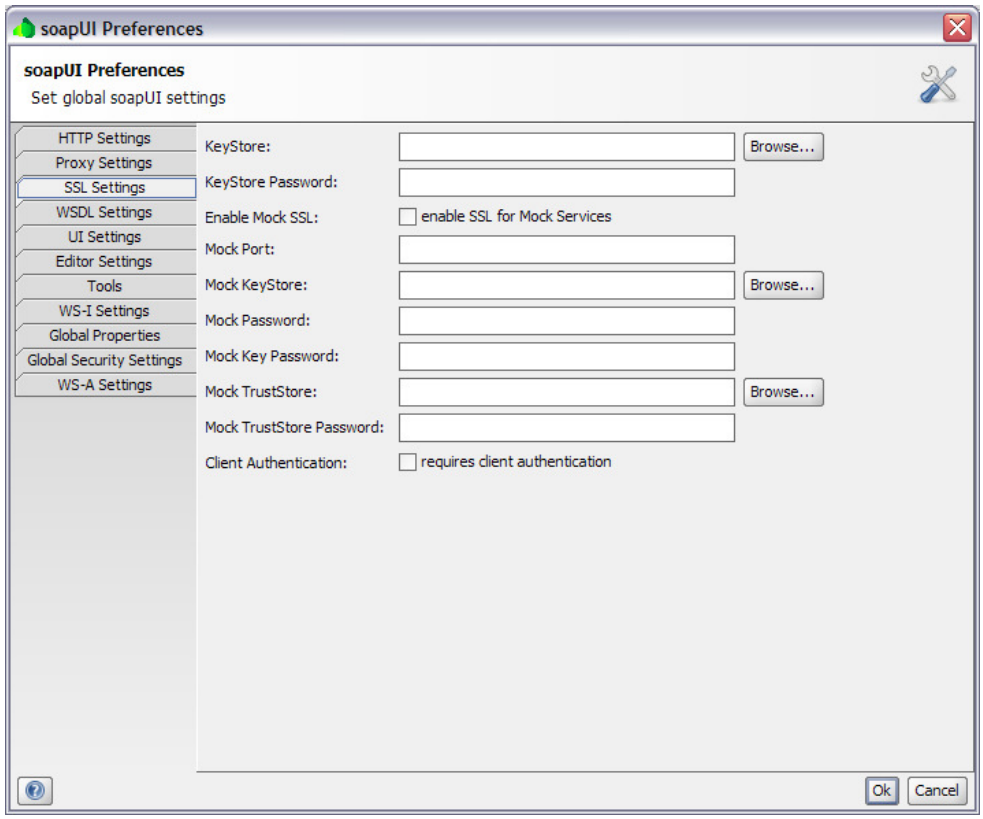
Launch SoapUI and click on File -> Preferences as shown below.



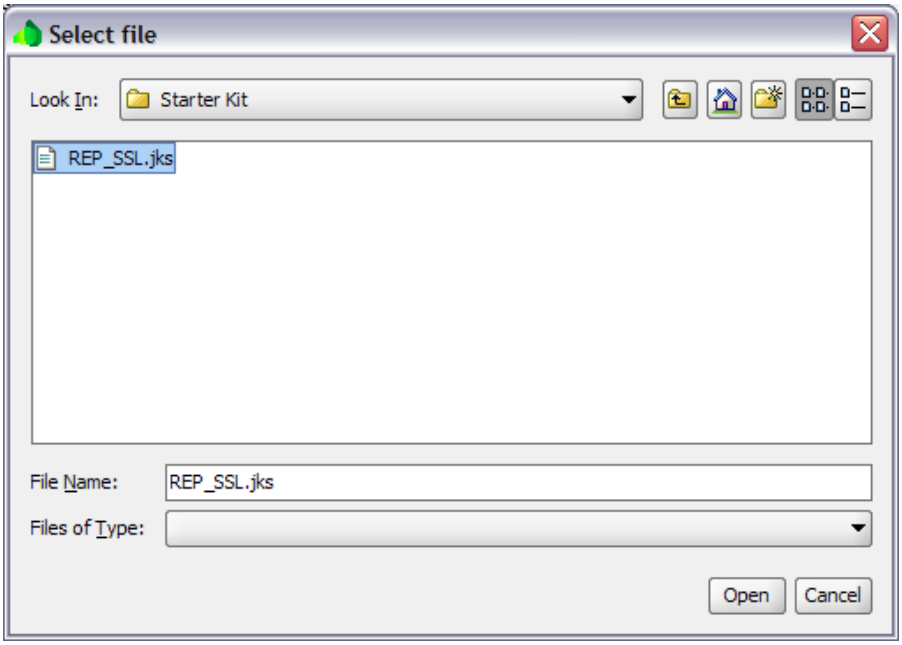
The soapUI Preferences will pop-up in a separate window.



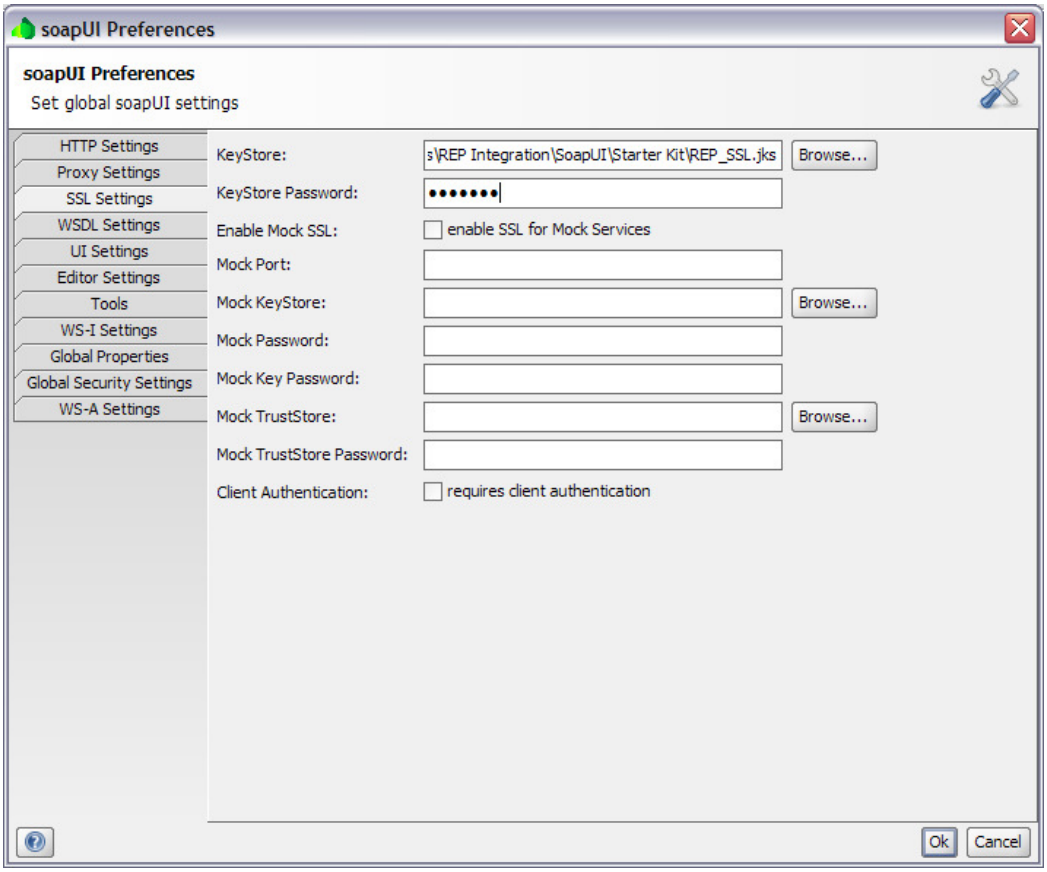
Select SSL Settings on the left navigation bar.



Click on browse button in Keystore field to select Keystore to use for SSL.



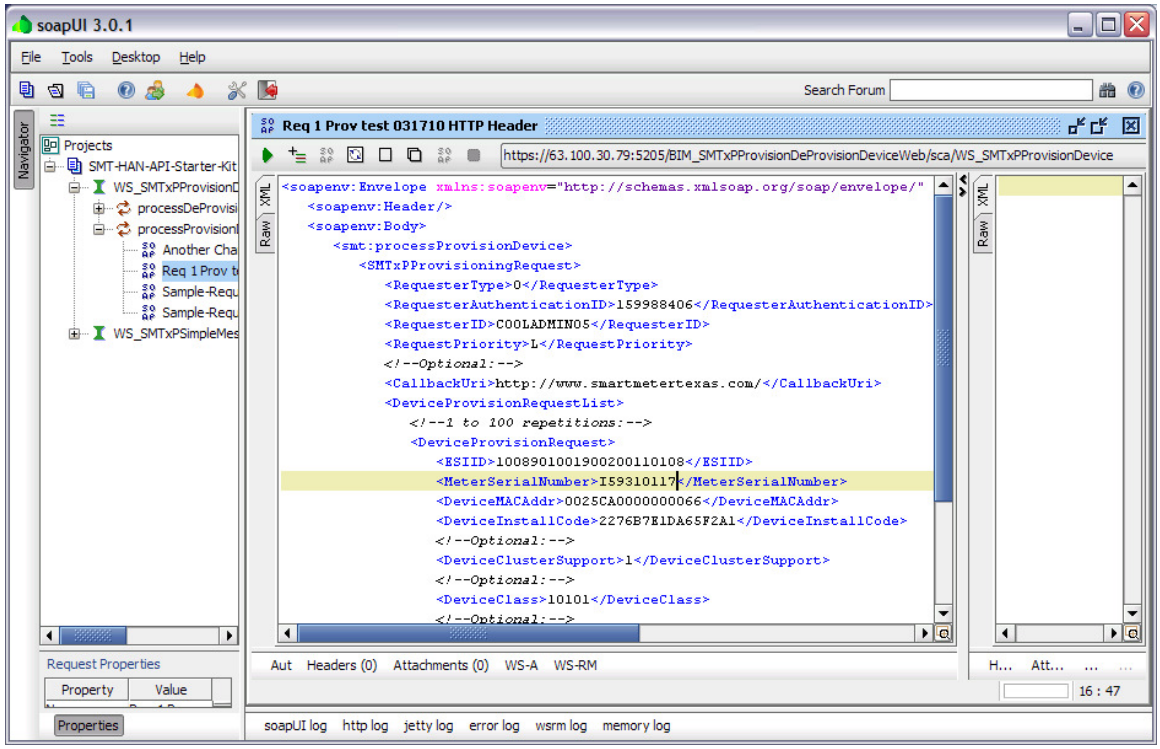
Input your Keystore password, for example, SMT1234, and click Ok.



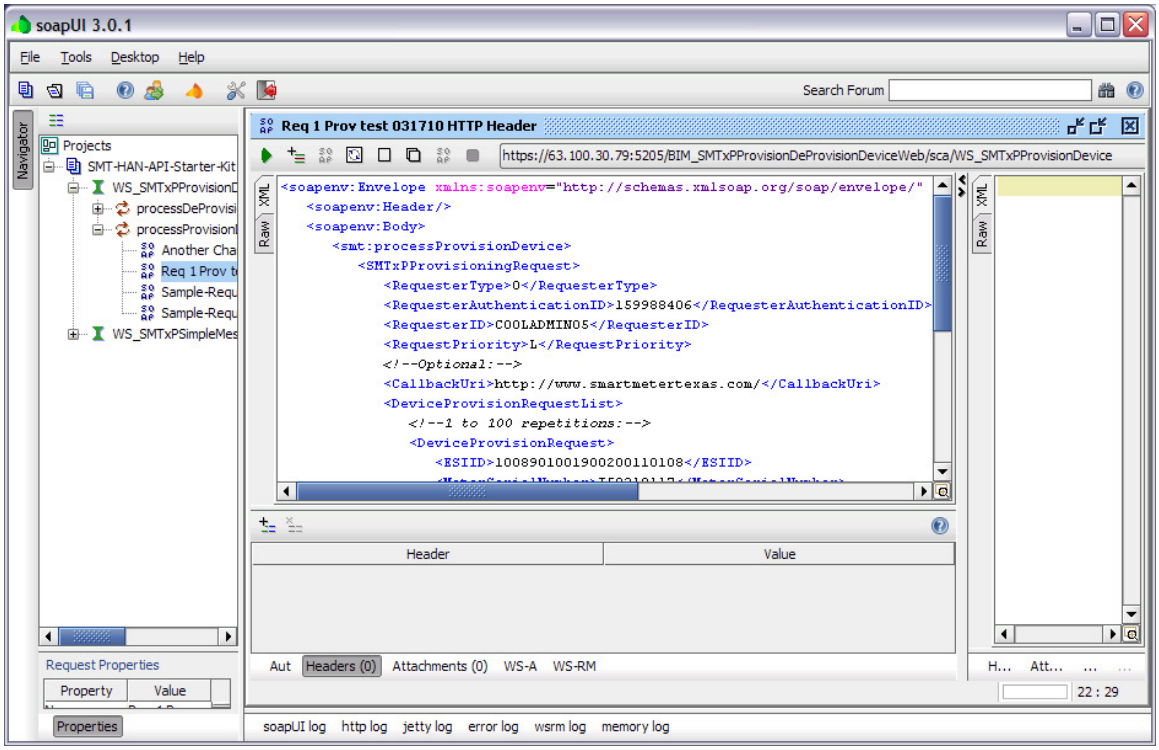
6.3.3 HTTP Header Configuration

An HTTP header with the name of ENTITY_NAME must be added to In-Home Device requests. The HTTP header needs to contain a value that is the entity name (e.g. Third-Party) that is submitting the request.

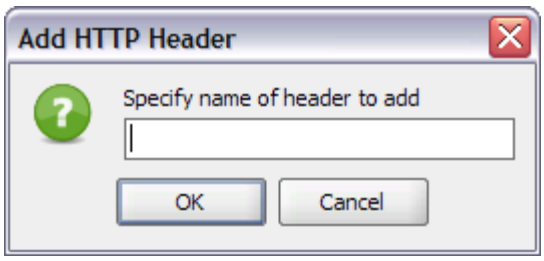
To add a HTTP header, locate the Headers field at the bottom middle of a request window as depicted below.



Click on the Headers field to open the Headers information box.

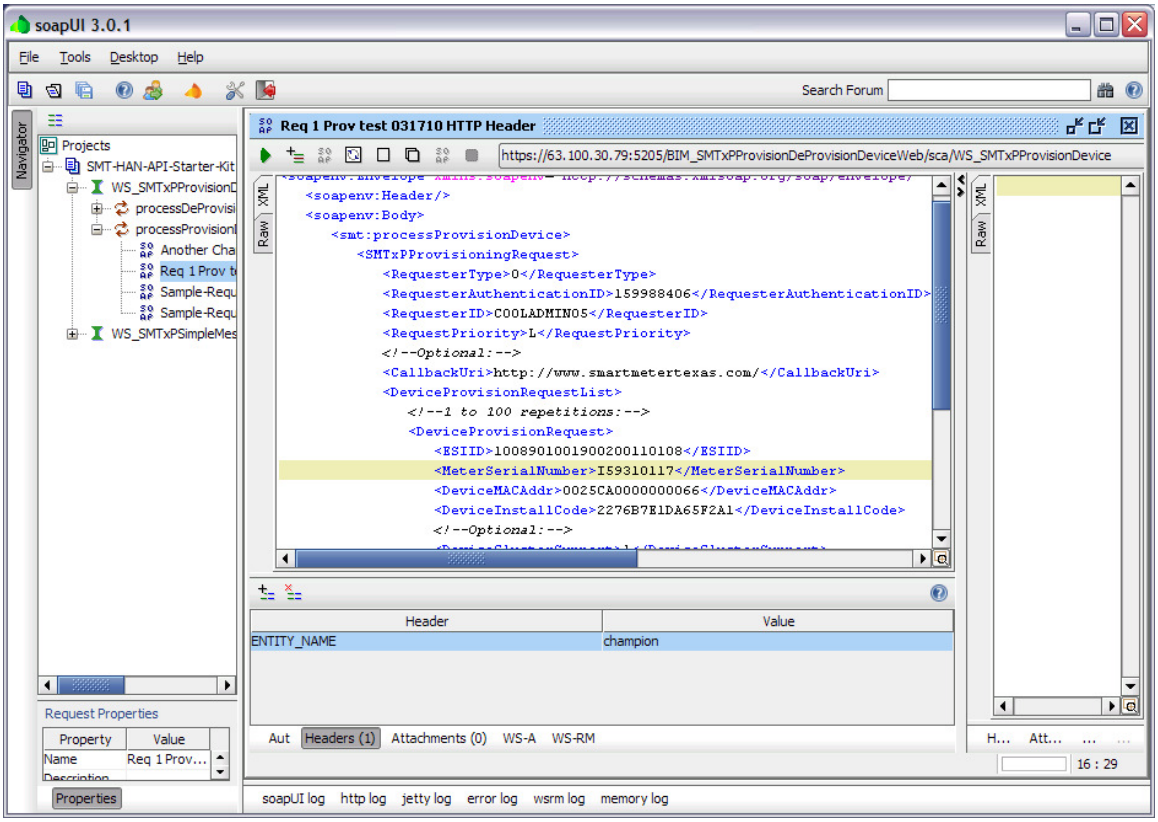


Clicking the + sign above the Headers information box to obtain a HTTP headers name input box as seen below.



Enter ENTITY_NAME and click OK.

An HTTP header with a name of ENTITY_NAME had been added to the request as seen below. In the value field, enter entity name or string that is recognized by SMT as the entity. The value should be the Entity Name provided as part of environment set up – see Section 6.2.1.

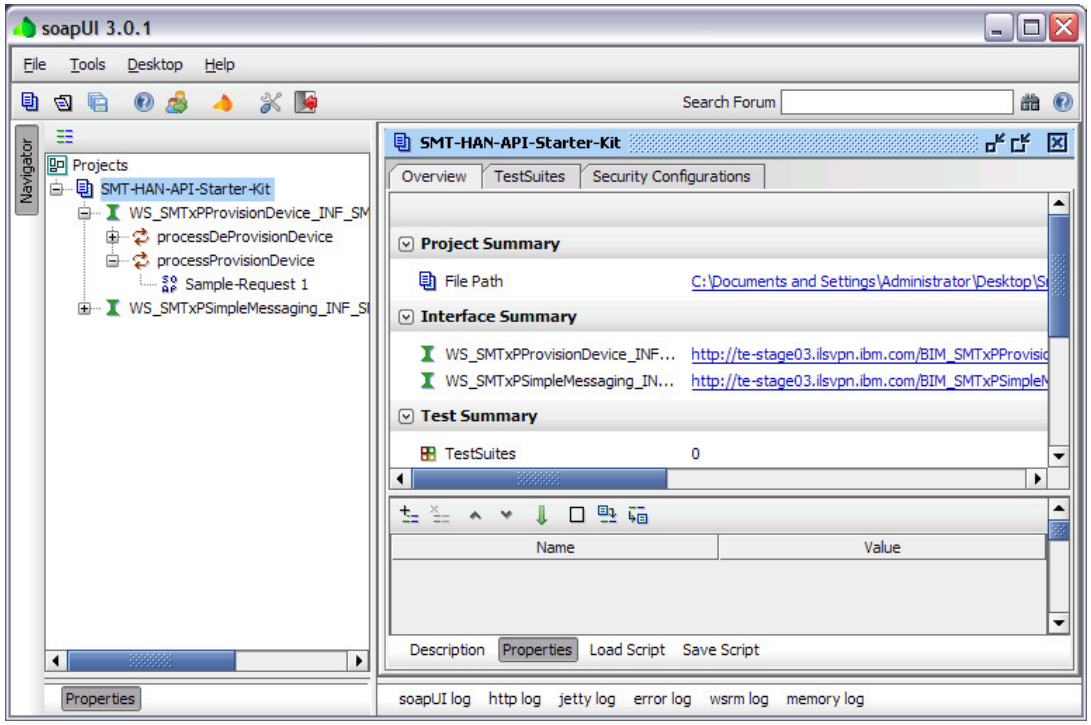


The above configuration allows SMT to determine source or origination of the request.

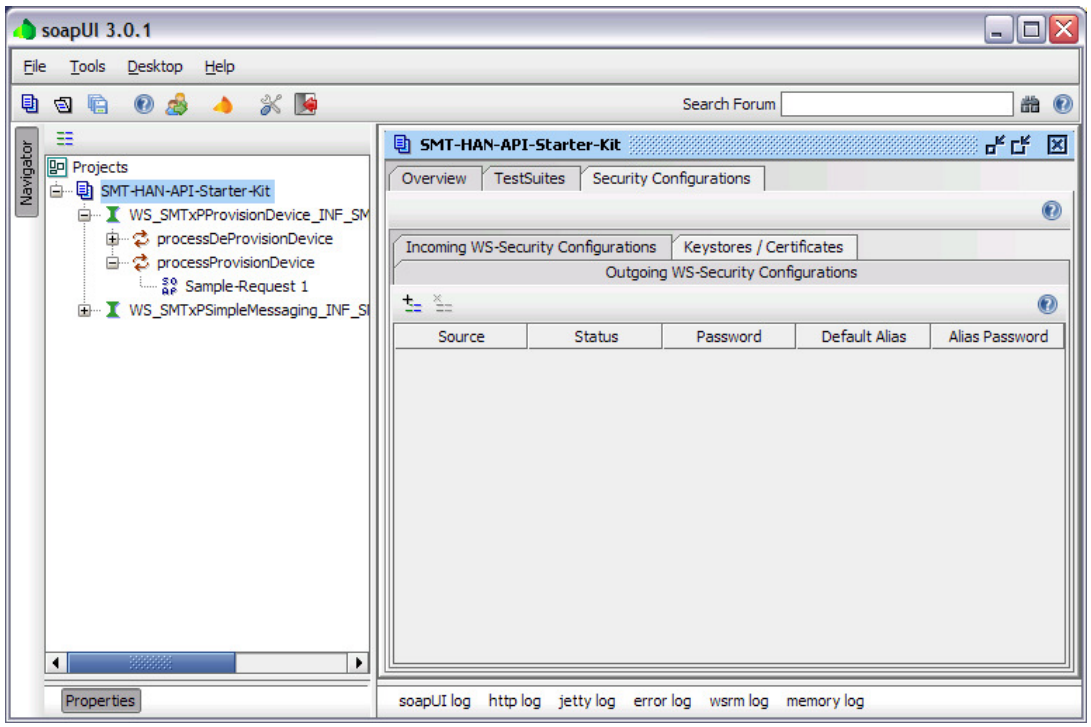
6.3.4 WS-Security Configuration

This chapter explains how to configure a WS-Security signature for outgoing Web Services call. The Time Stamp, UserNameToken and SOAP Body are signed. soapUI must be configured for Web Service calls.

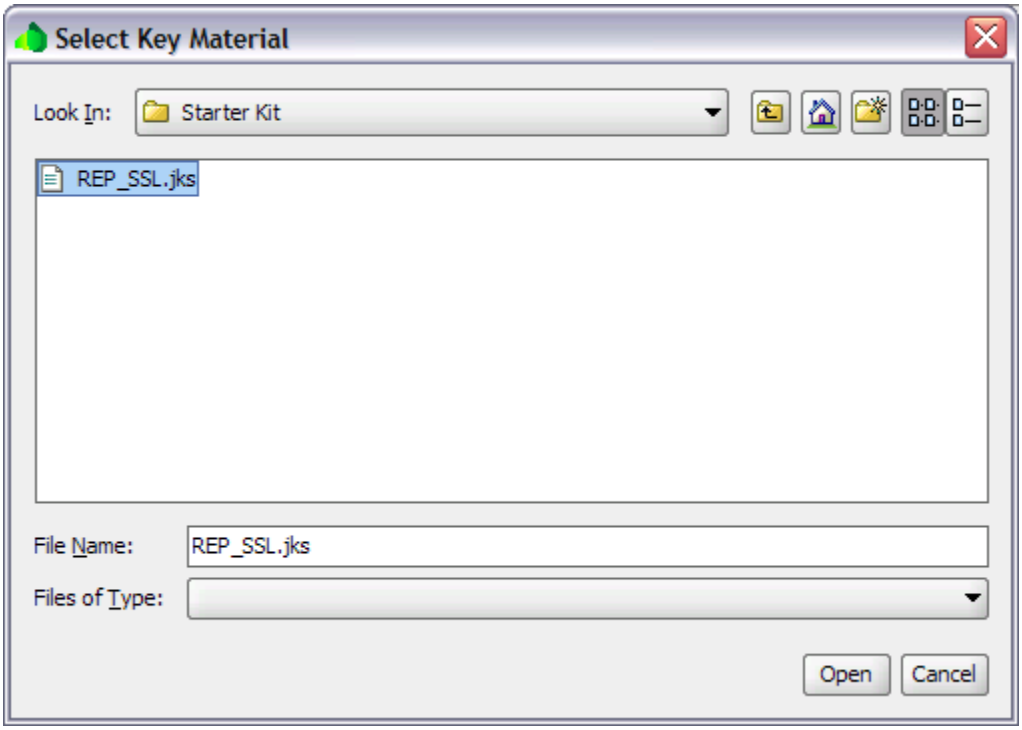
Select soapUI project and double click.



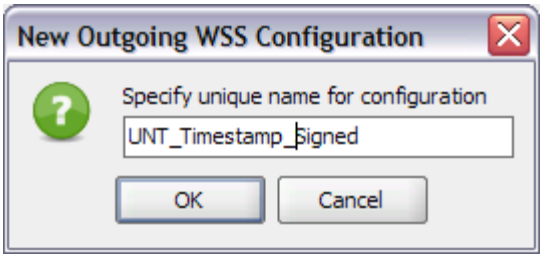
Select the Security Configurations tab and then the Keystore/Certificates tab as pictured below.



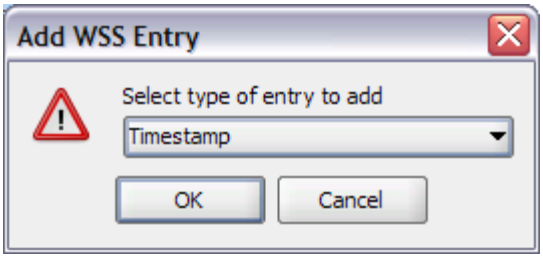
Click on + sign to specify Keystore/Certificate.



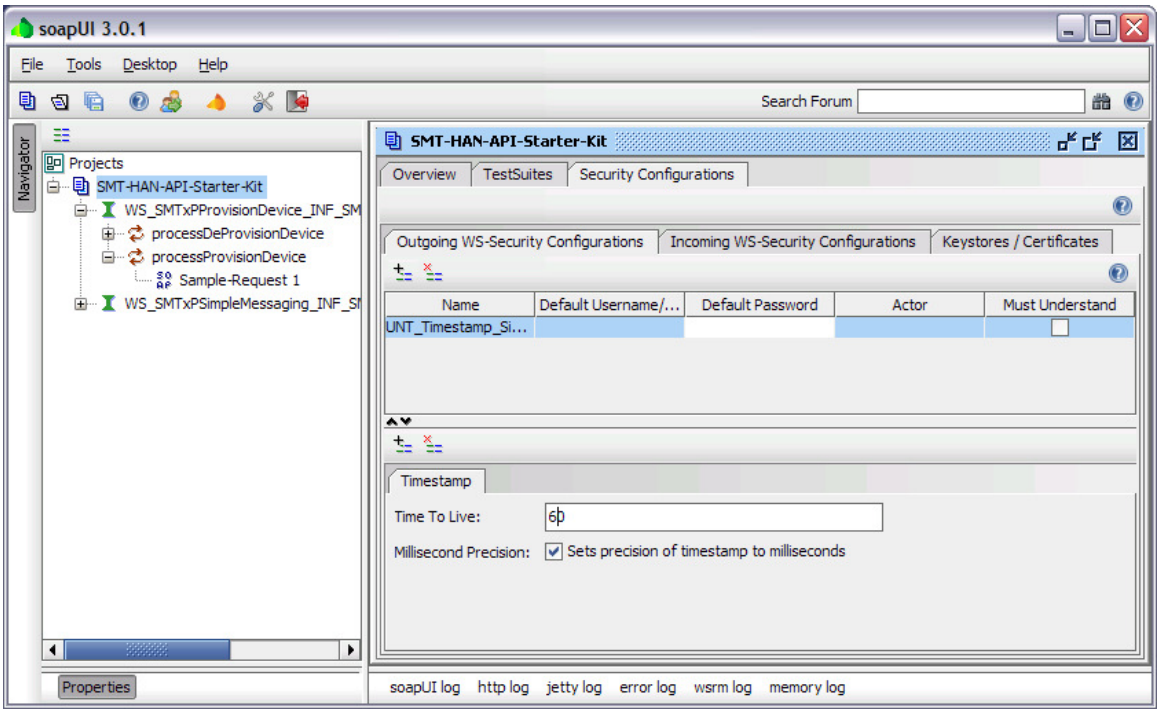
Now, click on Outgoing WS-Security Configuration tab. Then click on + sign and enter a unique configuration name. Below, UNT_Timestamp_Signed is used to represent: user name token, timestamp, and signed.



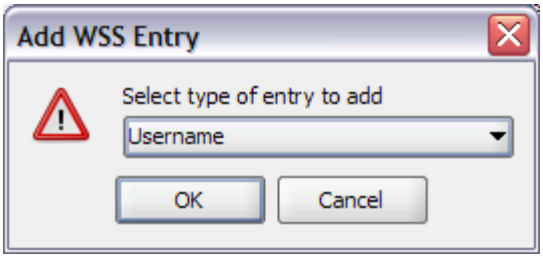
In the lower half panel. Click on + sign and select Timestamp as type of entry to add.



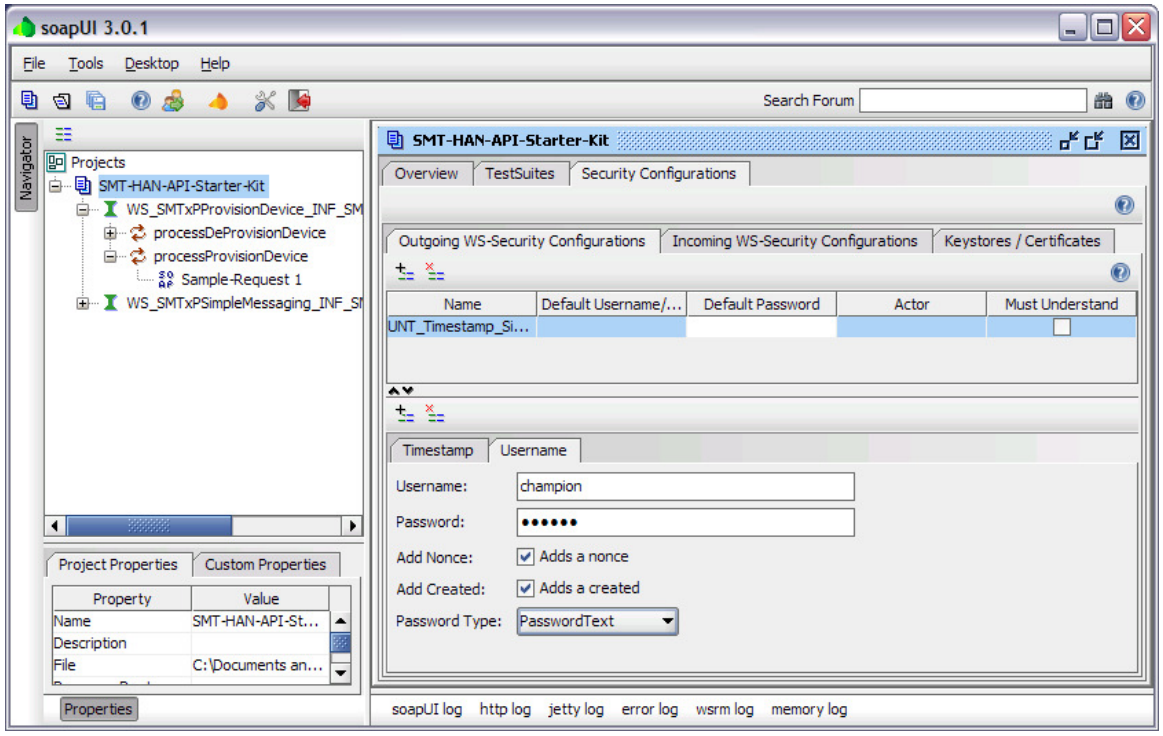
Enter Time to live value, for example, 60.



Select + again in lower half panel and select Username as type of entry to add.

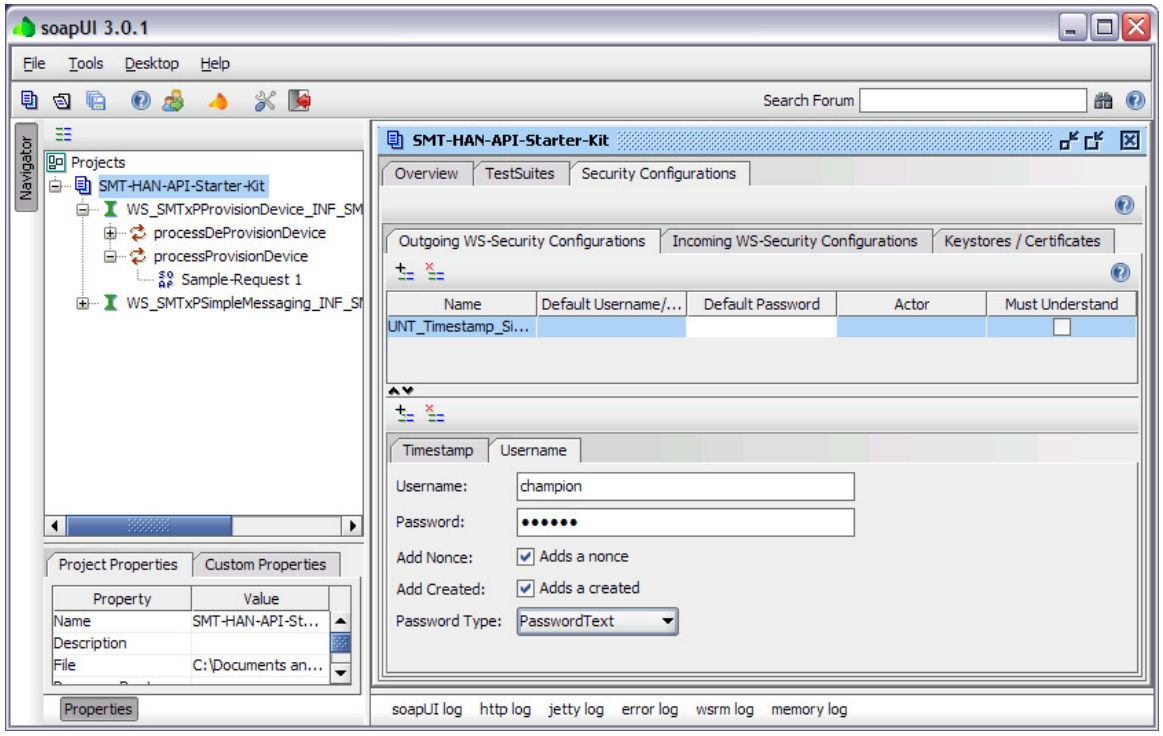


Specify Username, password and PasswordText as type of password to add. (Specifying password is mandatory).

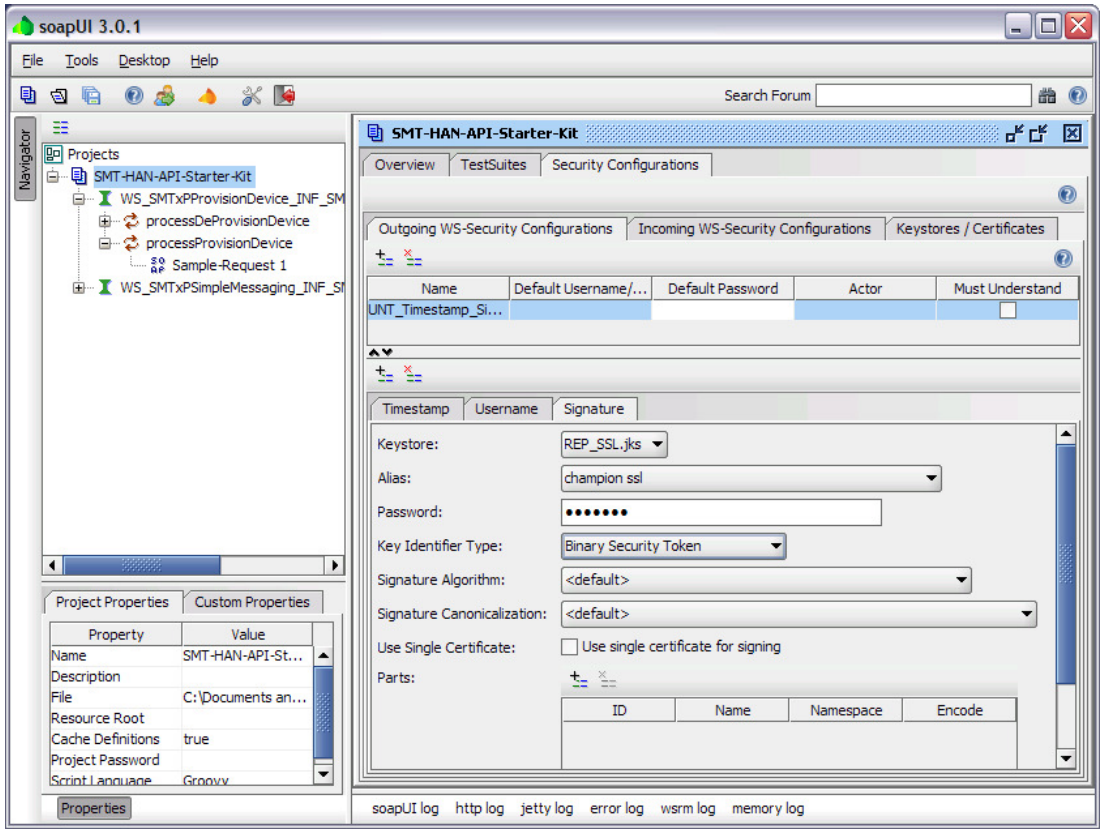


Now, select + sign at the lower half panel and specify Signature as type of entry to add.

Specify Keystore, Alias and Keystore Password.

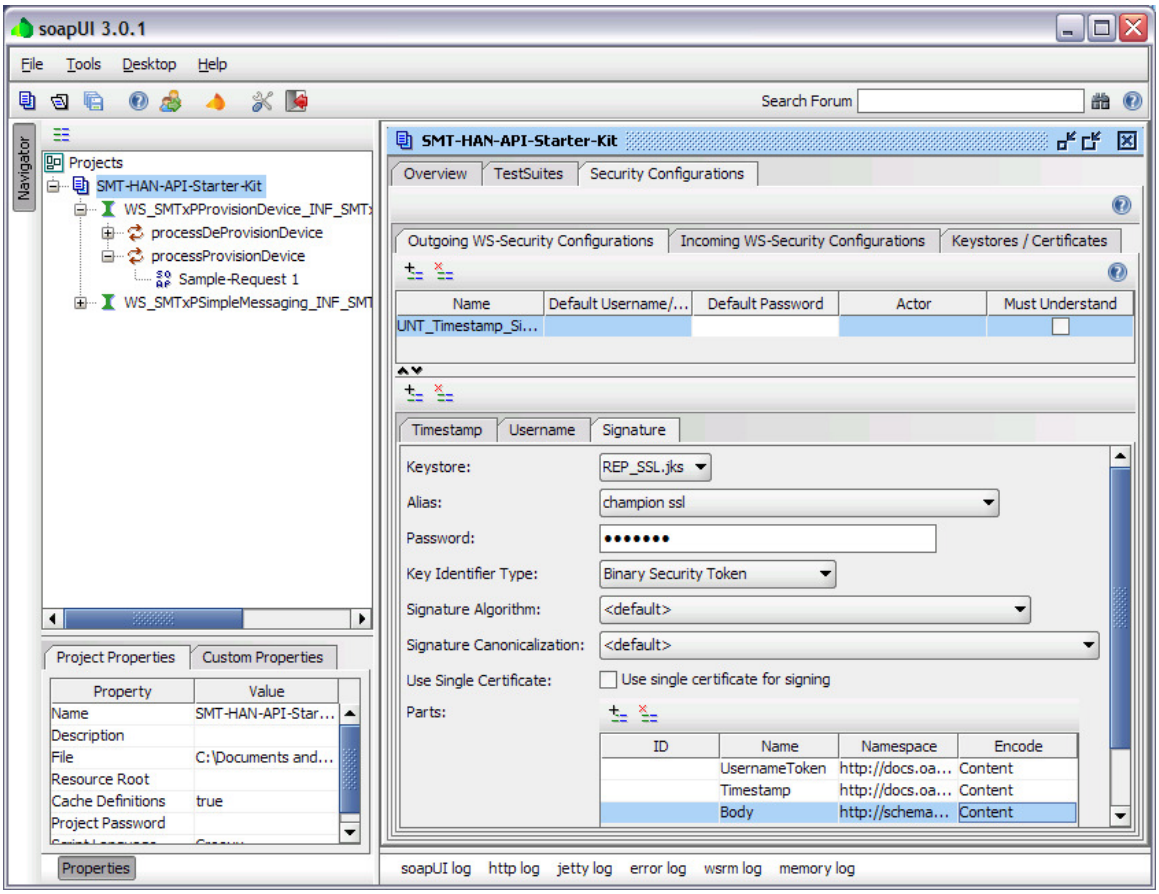


Then, select the correct Binary Security Token in Key Identifier Type field.



Now, enter the different parts of the signature. Click Parts + after the *Use Single Certificate* field to enter the information in the following table. (Click the + 3 times for each required entry: UsernameToken, Timestamp and Body).

Name	Namespace	Encoding
UsernameToken	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	Content
Timestamp	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	Content
Body	http://schemas.xmlsoap.org/soap/envelope/	Content



6.3.5 Invoking Web Service

This section describes how to invoke In-Home Device query Web Services.

6.3.5.1 URLs for invoking In-Home Device Queries

The In-Home Device Start Kit comes with Staging and Production URLs defined in the soapUI project. However, users must select the correct URL when sending a request to Staging or Production

The following subsections provide the URLs to be used for invoking In-Home Device query Web Services.

6.3.5.2 Staging URLs

- Provisioning / Deprovisioning
  https://testservices.smartmetertexas.net:5205/BIM_SMTxPProvisionDeProvisionDeviceWeb/sca/WS_SMTxPProvisionDevice
- Messaging
  - Load Event
    https://testservices.smartmetertexas.net:5206/BIM_SMTxPLoadControlEvent
  - Simple Messaging
    https://testservices.smartmetertexas.net:5206/BIM_SMTxPSimpleMessaging
  - Cancel Load Control Message
    https://testservices.smartmetertexas.net:5206/BIM_SMTxPCancelLCMessaging
  - Cancel Simple Message
    https://testservices.smartmetertexas.net:5206/BIM_SMTxPCancelSimpleMessaging
  - Cancel All Load Control Event
    https://testservices.smartmetertexas.net:5206/BIM_SMTxPCancelAllLCEMessaging
  - Price Signal
    https://testservices.smartmetertexas.net:5206/BIM_SMTxPPriceSignal
  - Utility Enrollment Group
    https://testservices.smartmetertexas.net:5212/BIM_SMTxPUpdateUEGDeviceWeb/sca/WS_SMTxPUpdateUEGDeviceExp

6.3.5.3 Production URLs

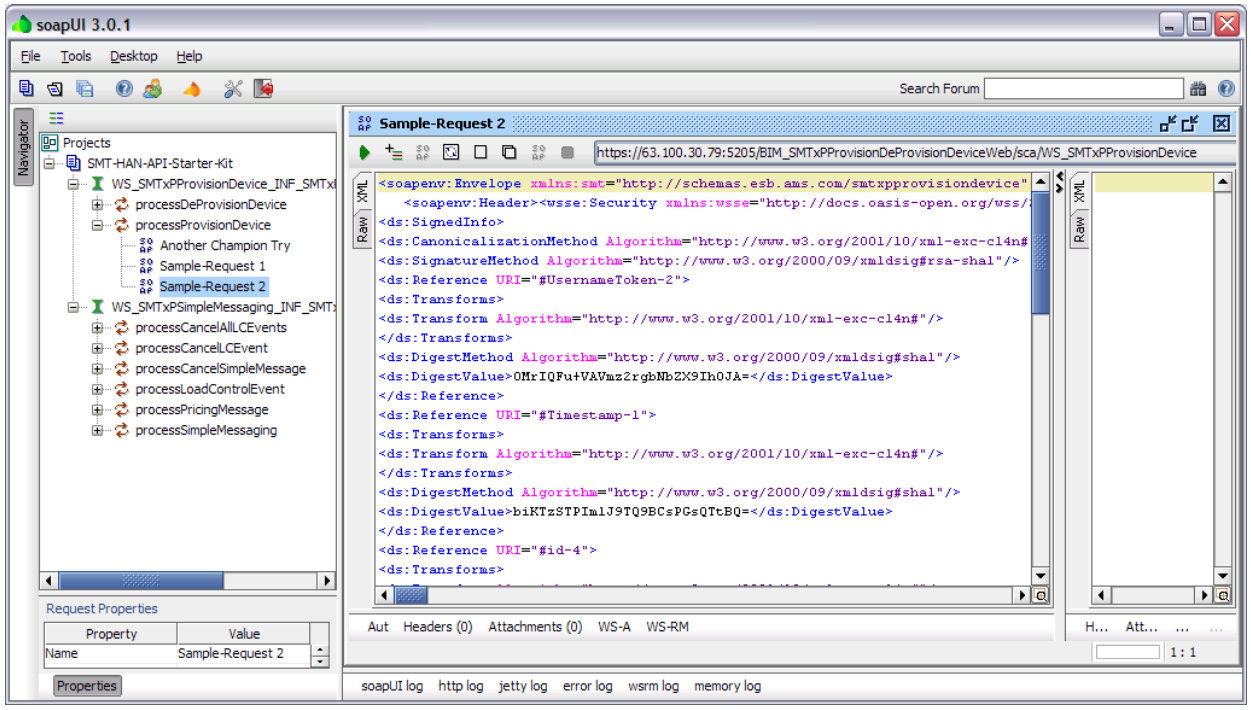
- Provisioning / Deprovisioning
  https://services.smartmetertexas.net:5205/BIM_SMTxPProvisionDeProvisionDeviceWeb/sca/WS_SMTxPProvisionDevice
- Smart Energy Profile Messaging
  - Load Event
    https://services.smartmetertexas.net:5206/BIM_SMTxPLoadControlEvent
  - Simple Messaging
    https://services.smartmetertexas.net:5206/BIM_SMTxPSimpleMessaging
  - Cancel Load Control Message
    https://services.smartmetertexas.net:5206/BIM_SMTxPCancelLCMessaging
  - Cancel Simple Message
    https://services.smartmetertexas.net:5206/BIM_SMTxPCancelSimpleMessaging
  - Cancel All Load Control Event
    https://services.smartmetertexas.net:5206/BIM_SMTxPCancelAllLCEMessaging
  - Price Signal
    https:// services.smartmetertexas.net:5206/BIM_SMTxPPriceSignal
  - Utility Enrollment Group

https://services.smartmetertexas.net:5212/BIM_SMTxPUpdateUEGDeviceWeb/sca/WS_SMTxPUpdateUEGDeviceExp

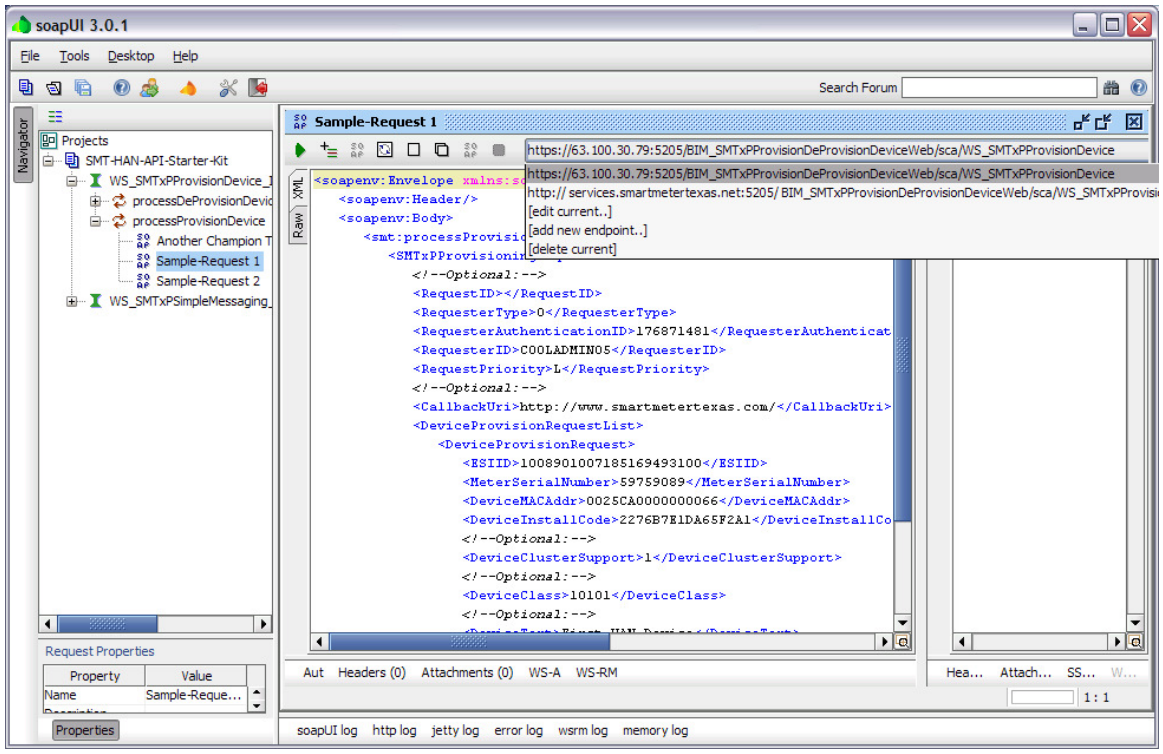
6.4 Selecting the appropriate URL when sending In-Home Device Requests

This section shows how to select the correct URL from within soapUI.

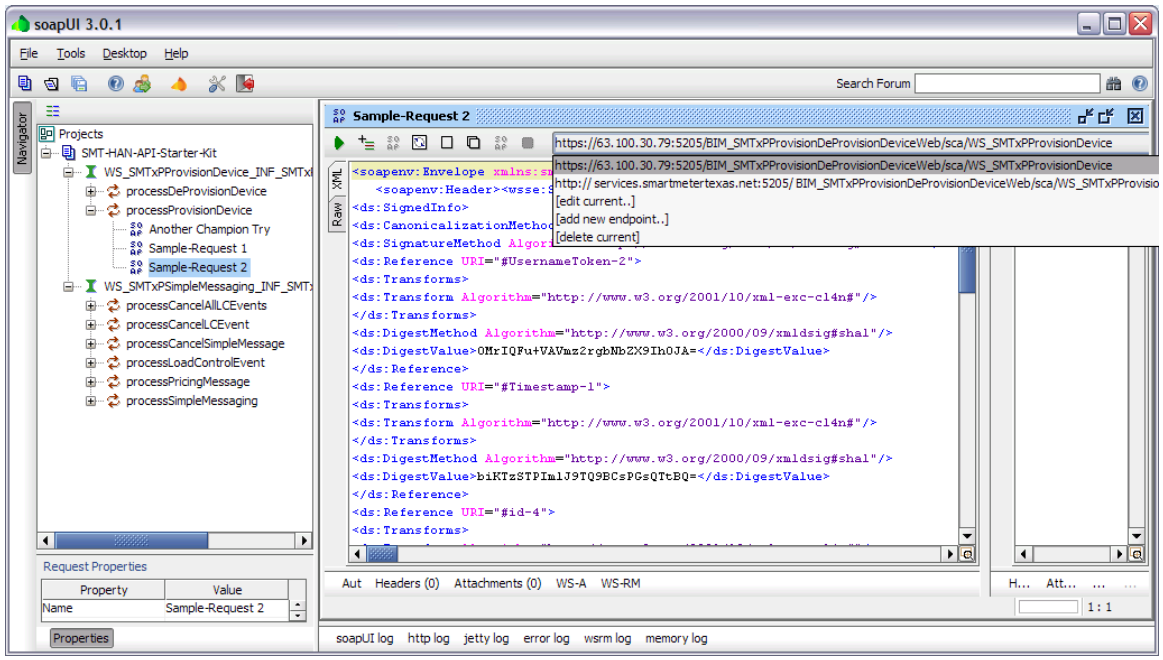
In the figure below, the Staging URL is displayed in the URL or endpoint drop-down box for Sample-Request2. This makes it the “current endpoint”. If the request were submitted without modification, it would be sent to the In-Home Device provisioning URL in the SMT staging environment.



To select the Production end-point for In-Home Device provisioning, click on the endpoint drop-down. soapUI will present several options. Choose the Production end-point.



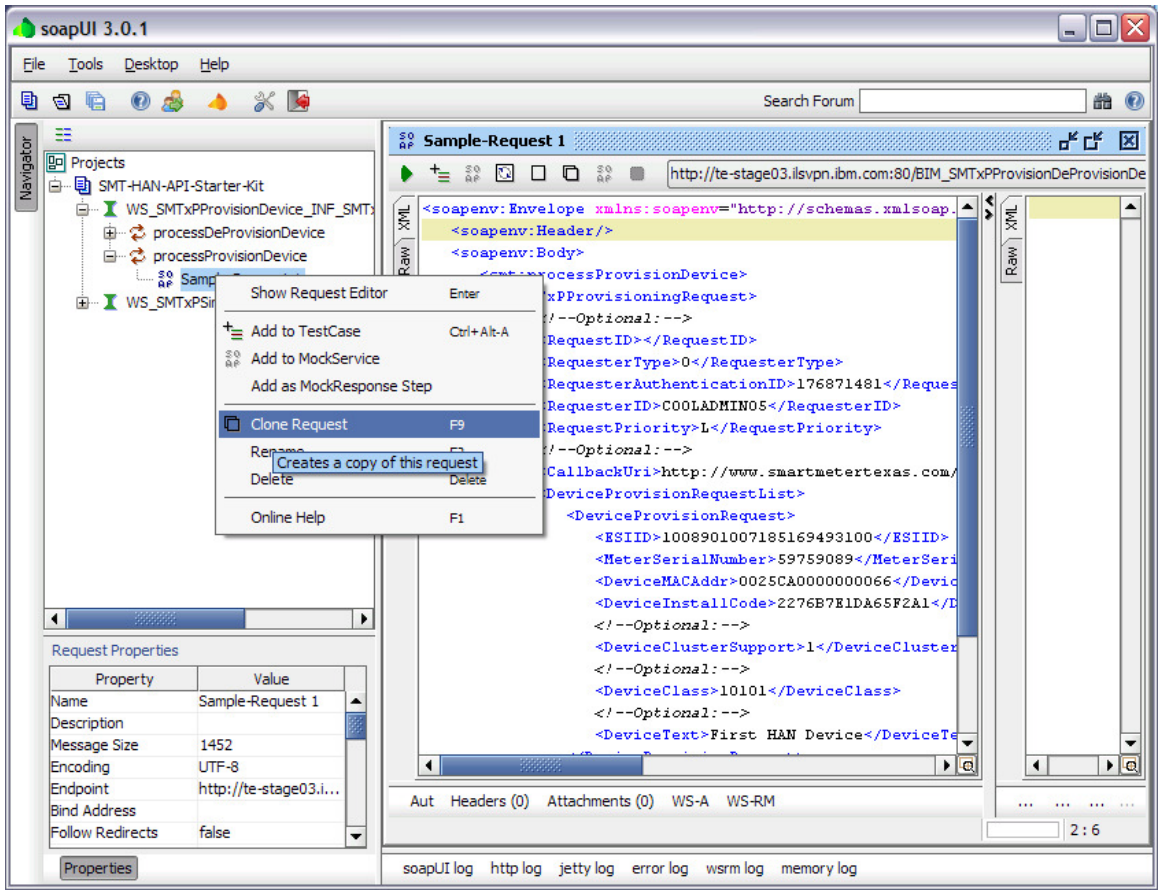
A total of 12 endpoints have been defined in the soapUI project for Smart Energy Profile 1.0 messaging. User should check the current endpoint before submitting requests to make sure the correct endpoint is selected. The correct endpoint must match the preferred environment and SEP message type.



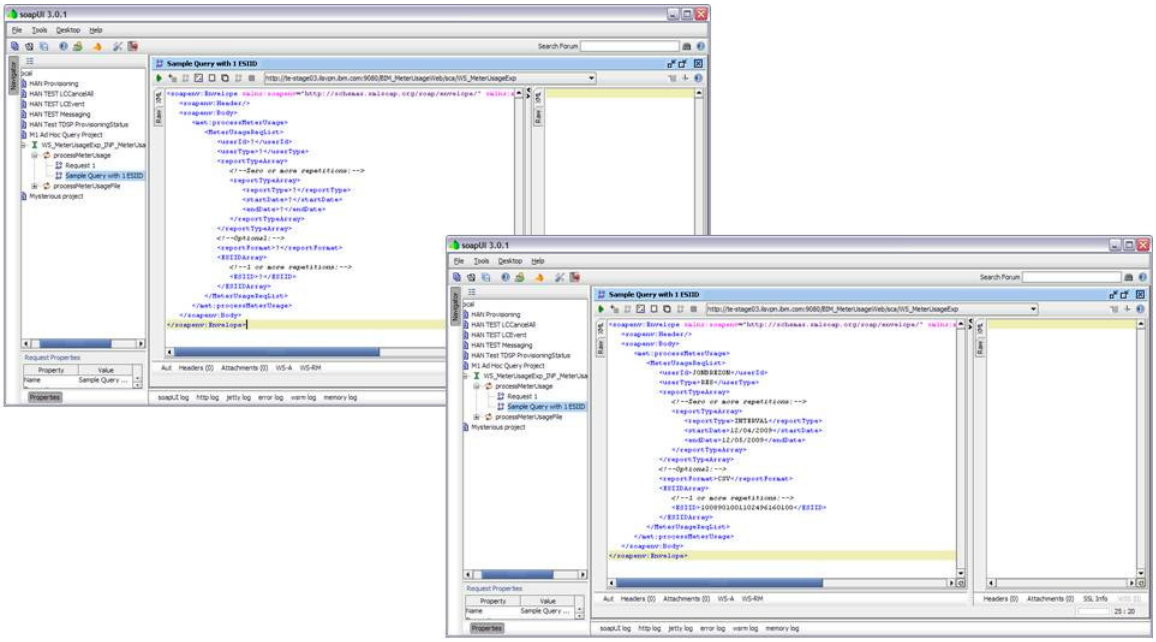
6.5 Applying a Web Services Signature to an Outgoing Request

The Starter Kit comes with empty request messages. These empty messages are named *Request 1*. It is recommended that these request messages be kept as starter messages.

To create an Ad-hoc Query request, it is recommended that a new request be created. Right click on the Request 1 object. Select the Clone Request option, and rename the request as depicted below.



Next, enter the appropriate API data in the request

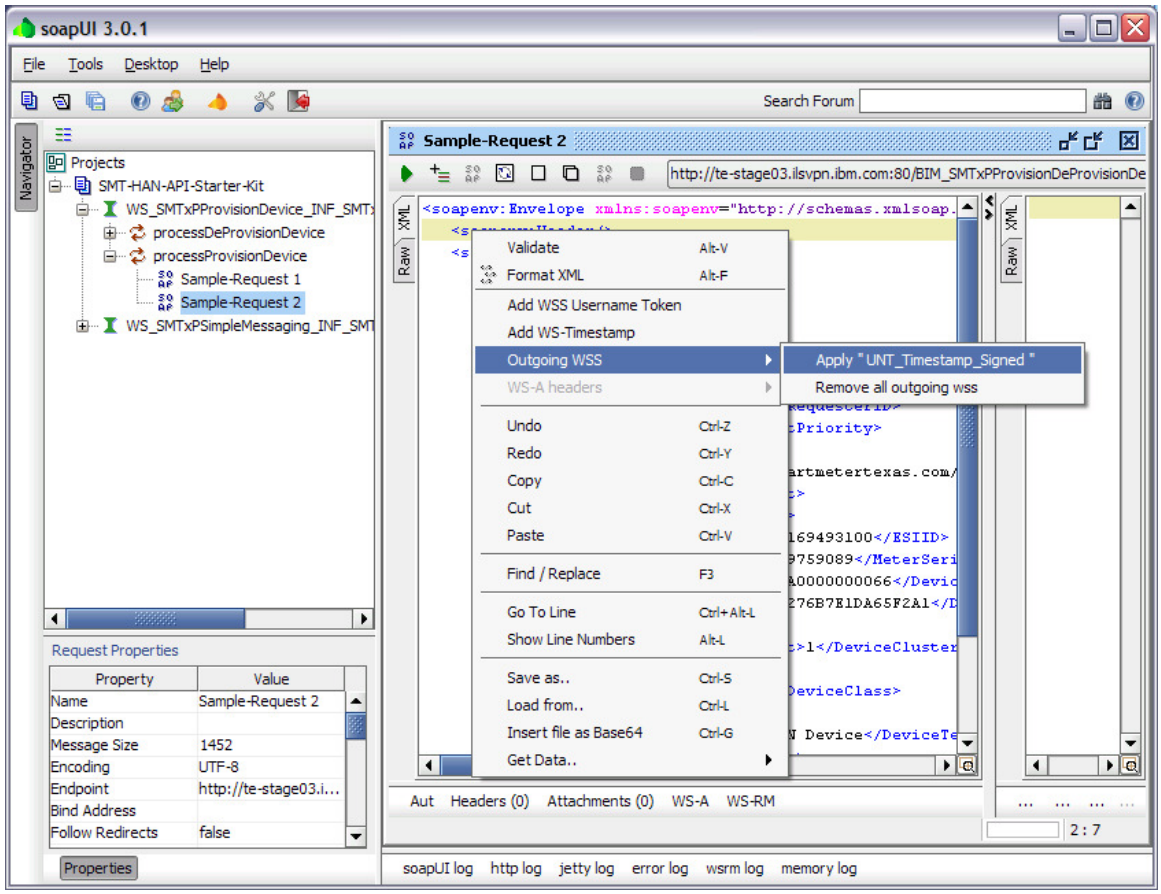


An example SOAP request appears below.

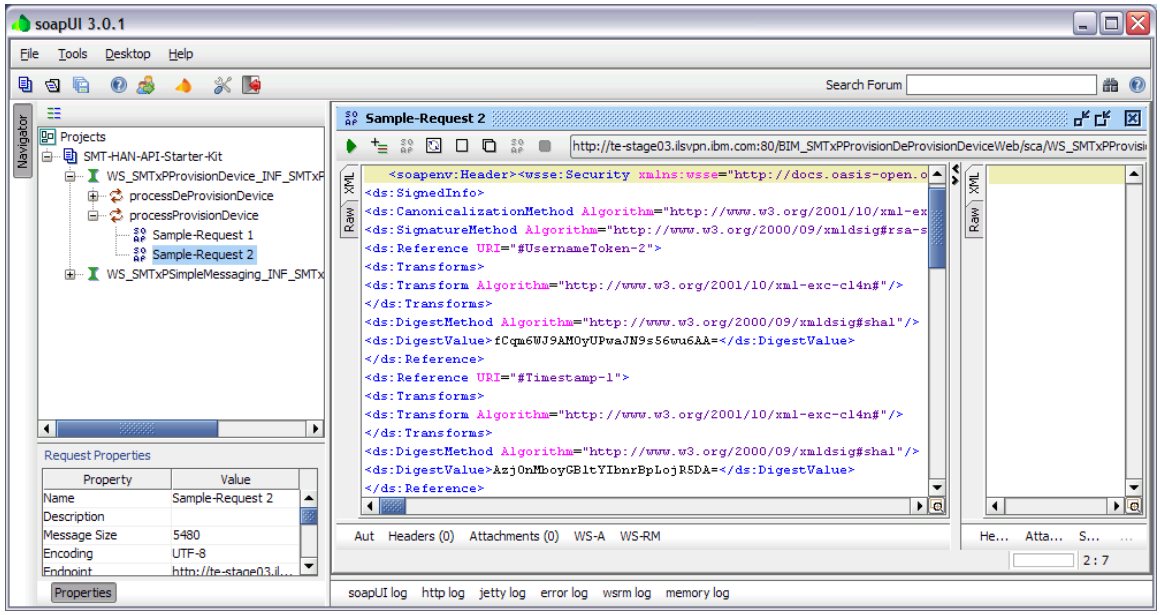
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpprovisiondevice">
  <soapenv:Header/>
  <soapenv:Body>
    <smt:processProvisionDevice>
      <SMTxPProvisioningRequest>
        <!--Optional:-->
        <RequestID></RequestID>
        <RequesterType>3</RequesterType>
        <RequesterAuthenticationID>176871481</RequesterAuthenticationID>
        <RequesterID>COOLADMIN05</RequesterID>
        <RequestPriority>L</RequestPriority>
        <!--Optional:-->
        <CallbackUri>http://www.smartmetertexas.com/</CallbackUri>
        <DeviceProvisionRequestList>
          <DeviceProvisionRequest>
            <ESIID>10089010071851694931 00</ESIID>
            <MeterSerialNumber>59759089</MeterSerialNumber>
            <DeviceMACAddr>0025CA0000000066</DeviceMACAddr>
            <DeviceInstallCode>2276B7E1DA65F2A1</DeviceInstallCode>
```

```
            <!--Optional:-->
            <DeviceClusterSupport>1</DeviceClusterSupport>
            <!--Optional:-->
            <DeviceClass>10101</DeviceClass>
            <!--Optional:-->
            <DeviceText>First HAN Device</DeviceText>
         </DeviceProvisionRequest>
      </DeviceProvisionRequestList>
   </SMTxPProvisioningRequest>
</smt:processProvisionDevice>
</soapenv:Body>
</soapenv:Envelope>
```

Finally, right click within the message, select Apply Outgoing WSS option, and then select Outgoing WS-Security Configuration.



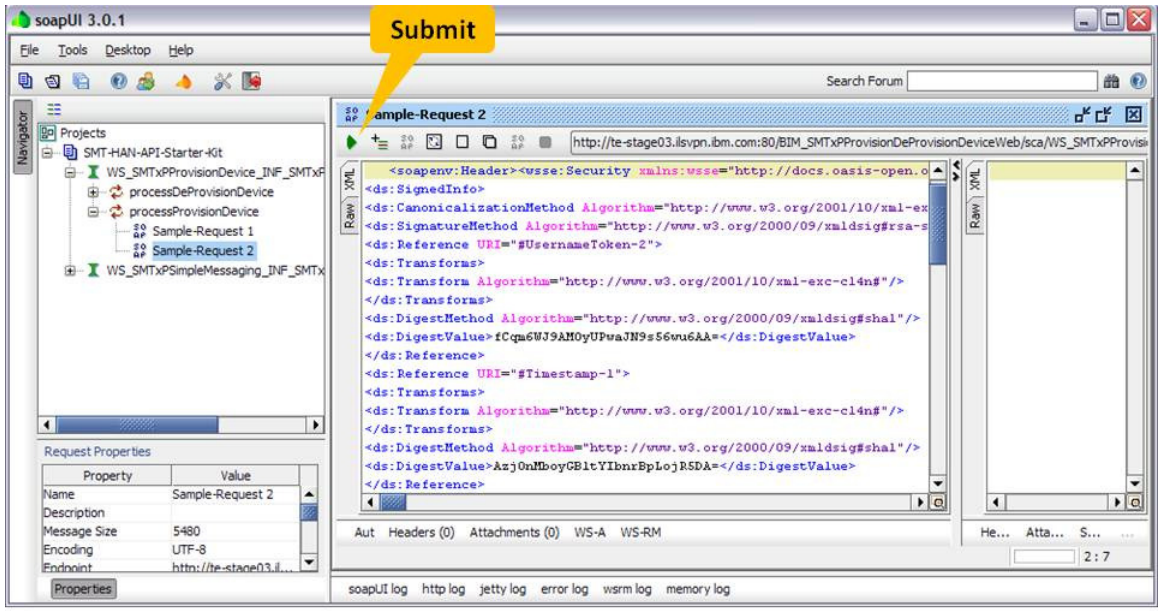
The last step signs the message as pictured below.



Do not reformat the message. If the message is modified, the signature should be removed and reapplied.

Make sure that the correct address is loaded into the URL bar at the top of the request.

After a Web Services Signature has been applied to the message and the URL is correct, submit message by pressing the Green arrow at the top of the message window.



6.6 Troubleshooting

In the event that Start Kit users are not able invoke a web service via SOAPUI client, these troubleshooting steps should be:

- Review the soapUI error log.
  Records in the soapUI error log should indicate a range of communication problems and can be used to determine the root-cause of a failure.

  Soap Fault Codes

2100	Invalid Message Signature failure
2200	SMT System Error
2300	Authentication Failure Invalid Credentials
2400	SMT Internal System Error
2500	SMT internal Fault
2600	SOAP Fault Message Rejected by SMT

- Check if you can ping the SMT Server, Example: "ping te-stage03.atlanta.ibm.com" from the machine where the SOAPUI client is running?
  - If ping succeeds, it means you are able to communicate to the server. Proceed to test telnet as described below.
  - If you cannot ping the SMT server, soapUI requests are not reaching the SMT server. Determine and fix the cause of the problem that is impeding end-to-end communications.
- Check if you can telnet the SMT Server, Example: "telnet te-stage03.atlanta.ibm.com 5205" from the machine where the SOAPUI client is running?
  If telnet succeeds, it means you are able to communicate to the server using port 5205.

  If you cannot ping the SMT server, soapUI requests are not reaching the SMT server. Determine and fix the cause of the problem that is impeding end-to-end communications.
- Check your public SSL key "Common Name" is same as the "hostname" of the server where SOAPUI client is running.
  You will need to generate and send a new certificate and submit it to SMT.
- For communications to the Production environment, validate that your public IP address matches with the value originally submitted to the SMT team during configuration.
  Starter Kit requests will only pass through the SMT firewall when they are submitted from defined IP addresses.
- If the submitted web service request failed with a SOAP Fault Exception, analyze the error code, description in the SOAP response and validate the input message.
  The actual SOAP Fault description in the response will contain a detailed message related to the specific input attributes. Check the input elements and retry the service with valid inputs
- Check to make sure the correct URL/endpoint has been selected

After you have tried all tests described above but still are not able to submit requests successfully, you may submit requests for help via email to support@smartmetertexas.com. Please collect and send as much diagnostic information as possible with your request, including:

- Information concerning the tests described above
- Information out of the soapUI error log
- The XML request that was submitted and any responses received.

6.7 In-Home Device Provisioning and Messaging WSDL Files

After an entity integrated with SMT In-Home Device API's using the API Starter Kit, the WSDL (Webservice description language) files for In-Home Device related services will be provided by SMT upon request. These files can be utilized to build client applications to consume the SMT services for In-Home Device. SMT will provide the WSDL files for the In-Home Device services listed below.

- In-Home Device Provisioning / Deprovisioning
- In-Home Device Utility Enrollment Group
- In-Home Device Messaging which includes:
    - Sending simple text message
    - Cancel simple text message
    - Sending price signal
    - Sending Load control event
    - Cancel a Load control event
    - Cancel all Load control events

Requestors are expected to raise a request with the SMT help desk (Call 1-888-616-5859) to request these WSDL files. SMT technical team would provide the WSDL files in a compressed (.zip) file. The WSDL files can also be imported to SOAP UI tool to create and setup the project to access the service.

7. SMT In-Home Device Interface Security

7.1 Introduction

This section describes Smart Meter Texas (SMT) interface security requirements for the In-Home Device API Starter Kit configuration set-up.

7.1.1 Prerequisite for Interfaces

This section lists interface security pre-requisites:

- All communication to SMT from requestors and TDSPs will be over 2-Way Secure Sockets Layer (SSL). For each TDSP, a VPN channel has to be established between SMT and TDSP systems. In the case of TDSPs, SSL will be employed over a virtual private network (VPN).
- For API requests from TDSPs, SMT requires that a user credential be passed in a SAML token that is part of SOAP header. The specific of SAML token is described in a later section.
- For API requests from an organization, SMT requires that a user credential be passed in a UserName Token that is part of SOAP header. SMT does not require password to be passed as part of UsernameToken. The specifics of UsernameToken are described in a later section.
- SMT will only accept CA issued certificates (SSL and Signer Cert) in its production environment. Selfsigned certificates (SSL or Code Signed) will not be accepted.
- SMT will accept self-signed certificates for testing purposes only. Although the self-signed certificates will be accepted for testing, CA certificates are preferred.
- It is assumed that partners will use Class 3 certificates.
- The system account for TDSPs and the organization should exist in the SMT user repository and be known to TDSP and the organization in advance. The system account is case sensitive.
- SMT will only accept signed requests as per WS-Sec 1.1 specification for all the incoming requests. The SMT signature processing module does explicit checks for the signature of UserNameToken, Simple Object Access Protocol (SOAP) Body and Time stamp. Although the SOAP request may be signed, the request will be reject if these elements are not signed.
- Signature Confirmation is not implemented.

7.2 SMT WS-Security Implementation features

This section describes the implementation of WS-Security by SMT.

- SMT is going to have a Certificate Management System in place. Hence it will use certificates in its certificate store for signature verification purposes. If a certificate is passed as part of the SOAP envelope, the SML signature processing module ignores it.
- SMT does certificate chain validation before using certificates for Signature validation.
- A SOAP Fault is thrown with an appropriate Fault Code in the event of error.
- The rule processing stops at the action which results into error.
- SMT receives entity information from HTTP header variable named ENTITY_NAME. The value of the header variable should be the name of the organization or a string that uniquely identifies the organization.

7.3 Trust relationship establishment

Entities are required to establish a trust relationship with the TDSPs and the organizations requesting access to the SMT APIs. Entity creation is an out-of-band process.

7.3.1 Trust relationships in Production

These entities are required by SMT:

- Signer Certificate – There should be only one CA-issued Signer Certificate that should be given to SMT.
- Value of HTTP header variable ENTITY_NAME.
- SSL Intermediate CA certificate.

This entity is provided by SMT to an organization that requests access to the SMT APIs:

- SystemAccount – There will be one SystemAccount that will be created for each organization. The System Account is used to validate the user against the SMT account database. The System Account for corresponding to the organization will be provided.

7.3.2 Trust relationships in Test

These entities are required by SMT:

- Signer Certificate - Self Signed Certificate or CA certificate. The number of this certificate is 1.
- Value of HTTP header variable ENTITY_NAME.

- SSL Certificate – SSL Certificate should be provided to SMT if an organization is using a self-signed certificate.

- Intermediate CA Certificate – This may be required if a CA certificate is going to be used.

Entity provided by SMT to the organiation that requests access to SMT APIs:

- SystemAccount – There will be one SystemAccount that will be created for each organization. The SystemAccount is used to validate the user against the SMT account database. The SystemAccount corresponding to the organization will be provided.

7.4 Validation Parameters and Steps

7.4.1 Example SOAP Envelope with UserName Token

```
<soapenv:Envelope xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/
 xmlns:smt="http://schemas.esb.ams.com/smtxpmessaging">
 <soapenv:Header>
  <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd">
    <wsse:UsernameToken>
     <wsse:Username>CNP</wsse:Username>
    </wsse:UsernameToken>
  </wsse:Security>
 </soapenv:Header>
 <soapenv:Body>
  <smt:processPricingMessage>
   <SMTxPPriceSignalRequest>
    <RequesterType>3</RequesterType>
     <RequesterAuthenticationID>123456789</RequesterAuthenticationID>
     <RequesterID>ADMIN2</RequesterID>
     <RequestPriority>L</RequestPriority>
     <AddressBlock>
      <AddressList>
       <!--0 to 10000 repetitions:-->
       <Address>
        <ESIID>1234567890123456789012</ESIID>
        <MeterSerialNumber>60333050</MeterSerialNumber>
        <DeviceMACAddr>PRC-MACADDR1</DeviceMACAddr>
       </Address>
      </AddressList>
     </AddressBlock>
     <PriceMessageBlock>
      <ProviderID>123456789</ProviderID>
      <RateLabel>Rate Label1</RateLabel>
```

```
        <IssuerEventID>7001</IssuerEventID>
        <CurrentTime>2009-12-14T16:30:00</CurrentTime>
        <UOM>1</UOM>
        <Currency>USD</Currency>
        <PriceTier>1</PriceTier>
        <PriceTrailingDigit>3</PriceTrailingDigit>
        <RegisterTier>1</RegisterTier>
        <StartTime>2009-12-18T16:30:00</StartTime>
        <Duration>55</Duration>
        <Price>12777</Price>
        <PriceRatio>105</PriceRatio>
        <GenerationPrice>12111</GenerationPrice>
        <GenerationRatio>95</GenerationRatio>
        <AlternateCostDelivered>1111</AlternateCostDelivered>
        <AlternateCostUnit>1</AlternateCostUnit>
        <AlternateCostTrailingDigit>2</AlternateCostTrailingDigit>
      </PriceMessageBlock>
    </SMTxPPriceSignalRequest>
  </smt:processPricingMessage>
 </soapenv:Body>
</soapenv:Envelope>
```

- SMT accepts a UserNameToken from the requestor with the UserName element. A password is not required.
- The Username element within UserNameToken should be the System Account assigned to the calling organization. The System Account is set up after the organization's first admin is registered.
- The RequesterType element should be 3 for Third-Parties.
- The RequesterAuthenticationId should be the DUNS number of the organization.

7.4.2 Example Signed SOAP Envelope

```
<soapenv:Envelope
xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/xmlns:smt="http://schemas.esb.ams.com/smtx
pmessaging">
 <soapenv:Header>
  <wsse:Security soapenv:mustUnderstand="1"
   xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
   <wsu:Timestamp wsu:Id="Timestamp-6f087de8-475a-4a73-a156-7550dfdb227a"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <wsu:Created>2010-01-19T21:33:16Z</wsu:Created>
    <wsu:Expires>2010-01-19T21:38:16Z</wsu:Expires>
   </wsu:Timestamp>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
```

```
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#Id-a73451ca-350b-4ab0-8fb8-4c8a845676fe">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>IIADgpAo5apSEJbNFeq84eyK4p4=</DigestValue>
</Reference>
<Reference URI="#Id-7bae2f18-a07b-4602-bc3d-237765fd72d0">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>Dw97YWmyoFZ1zEHdfu6yR9dY7Zs=</DigestValue>
</Reference>
<Reference URI="#Timestamp-6f087de8-475a-4a73-a156-7550dfdb227a">
<Transforms>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>oI1HC0SNO3lZldrEaOSxGUFzFn4=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>gJbQeqjQYVwcLjTRj30y1u8xEhnCIbPeNUL1Ky83rl6f+ZVjmuBBnAyJ3SHLsD
xi/DXfcKCbsPagSGAxcxch0/HPP+yT6bdIMiLWd/lkGSipBETfWWkeWfAKBLoIQCorbE+j2FxNPKV
R/mU1nrg2iVV9cLM8Bwy2Mu90U969r3c=</SignatureValue>
<KeyInfo>
<wsse:SecurityTokenReference>
<dsig:X509Data xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" >
<dsig:X509IssuerSerial>
<dsig:X509IssuerName>CN=www.REP.com, OU=Retail, O=REP Energy, L=Dallas,
ST=TX, C=US</dsig:X509IssuerName>
<dsig:X509SerialNumber>1262968678</dsig:X509SerialNumber>
</dsig:X509IssuerSerial>
</dsig:X509Data>
</wsse:SecurityTokenReference>
</KeyInfo>
</Signature>
<wsse:UsernameToken wsu:Id="Id-a73451ca-350b-4ab0-8fb8-4c8a845676fe"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<wsse:Username>SYSTEMACCOUNT</wsse:Username>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="Id-7bae2f18-a07b-4602-bc3d-237765fd72d0"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<smt:processSimpleMessaging>
```

```
<SMTxPSimpleMessageRequest>
 <RequesterType>3</RequesterType>
 <RequesterAuthenticationID>123456789</RequesterAuthenticationID>
 <RequesterID>FIRSTADMIN16JAN</RequesterID>
 <RequestPriority>M</RequestPriority>
 <CallbackUri />
 <AddressBlock>
  <GroupID>799530915</GroupID>
 </AddressBlock>
 <SimpleMessageBlock>
  <MessageID>40004</MessageID>
  <StartTime>2010-01-19T16:39:00</StartTime>
  <DurationTime>5</DurationTime>
  <Message>Simple Message on 2010-01-19</Message>
  <MCTransmission>0</MCTransmission>
  <MCPriority>0</MCPriority>
  <MCConfirmation>0</MCConfirmation>
 </SimpleMessageBlock>
</SMTxPSimpleMessageRequest>
</smt:processSimpleMessaging>
</soapenv:Body>
</soapenv:Envelope>
```

- SMT accepts signed message from its partner. In the event that it receives an unsigned message or message with invalid signature, the request will be rejected and SOAP Fault will be sent.

- For signed messages, SMT mandates that the SOAP Body, UsernameToken and TimeStamp elements be explicitly signed as in the example above. If anyone of the elements is not signed, the request will be rejected and SOAP Fault will be sent.

- The Token reference type is IssuerSerial. SMT will not extract a certificate from the SOAP Header for Signature validation. It uses certificates from its certificate store for Signature Validation. Therefore, it is imperative that certificates are exchanged prior to commencement of transaction.

7.4.3 Validation Parameters

Following table describes validation parameters, source and purpose:

Parameter	Source	Purpose
Subject Name	SSL Client Certificate	To know the originator of request
UserName	Child element of UserNameToken element of SOAP Header	To validate against System Account
RequesterType	Child element of SOAP Body	To get a LDAP branch where System Account will be validated.
RequesterAuthenticationID	Child element of SOAP Body	To validate the DUNS number that is presented in this element.
Signer Certificate	Out-of-Band	To validate the signature
Intermediate SSL Certificate	Out-of-Band	SSL handshake
Self Signed SSL Certificate	Out-of-Band	SSL Handshake(Staging Only)

7.4.4 Validation Steps

Following are the authentication and validation sequence that happens on the SMT perimeter:

- SMT does 2-way SSL hand-shake with the requestor's endpoint.
- SMT gets the requestor's name or string identifying the requestor by reading the HTTP Header variable.
- SMT performs Schema Validation.
- SMT validates the signature of the incoming request.
- SMT validates the system account of the requestor using the HTTP header variable ENTITY_NAME, UserName from UserNameToken, and RequesterType elements.
- SMT validates the DUNS number of the requestor using the HTTP header variable ENTITY_NAME, RequesterType and RequsterAuthenticationID elements

If all the steps are successful, the request is sent to SMT internal systems. In the event of failure at any step, the fault message is sent with an appropriate fault code.

7.4.5 Certificate Authorities List

SMT will accept certificates (SSL and Signer) issued by following Certificate Authorities:

- American Express
- ANX
- Belacom-E-Trust
- C-and-W-HKT-SecureNet-CA
- Certipose
- Certisign
- Certplus
- Deutshe
- Entrust
- Equifax
- EUnet
- FESTE
- First-Data
- GlobalSign
- GTE-CyberTrust
- Microsoft
- NetLock
- RSA
- Saunalahaden
- SecureNet
- SecureSign
- SwissKey
- TC-TrustCenter
- Thawte
- UTN-DATACORP
- Valicert
- Verisign
- ViaCode

8. In-Home Device API Authentication and Authorization

8.1 Introduction

8.1.1 Purpose

This section discusses how the API authentication and authorization will be handled when direct web service request is made by the requestor to Smart Meter Texas Portal (SMTxP) Enterprise Service Bus.

Clients who communicate with SMT using the In-Home Device web service interface must support mutual authentication over SSL. DataPower and Tivoli components will authenticate users. Authorization is enforced by the SMT integration environment.

Two kinds of tokens will be used for authentication: Username or SAML tokens. The majority of the In-Home Device web service consumers are expected to use a Username token. In either case, token data is used to map the sender to a system account. When a Username token is sent, the User Name element identifies the system account. If a SAML token is passed, the NameId element identifies the system account. DataPower validates the originator by verifying the WS-Security signature using the signer certificate from the SMT certificate store. If the digital signature is valid and the user can be authenticated, the web service request is passed to the ESB. Otherwise, a SOAP fault is issued.

8.1.2 Scope

This section addresses the security requirement and schema validation of the SOAP requests passing through DataPower to Enterprise Service Bus

The interface supports:

- Provisioning an In-Home Device
- Deprovisioning an In-Home Device
- Simple Messaging
- Load Control Events
- Pricing Signal
- Provisioning Status
- Messaging Status

8.1.3 Intended Audience

This is intended for the

- Security Team and ESB Team for developing common understanding.
- Development team for construction of the interfaces
- TDSP & other IT teams for public Interface specifications & APIs.
- Testing team to understand interface level test scenarios and test cases.
- Infrastructure & Maintenance team for interface SLAs, build, deployment and operational procedures
- It may also be useful for review from the technical system architect as it contains technical implementation details

.

8.2 Technical Service Design

This section outlines In-Home Device Security requirement & overview.

8.2.1 High Level System View

The following diagram & listed steps provides a high level overview of the system.

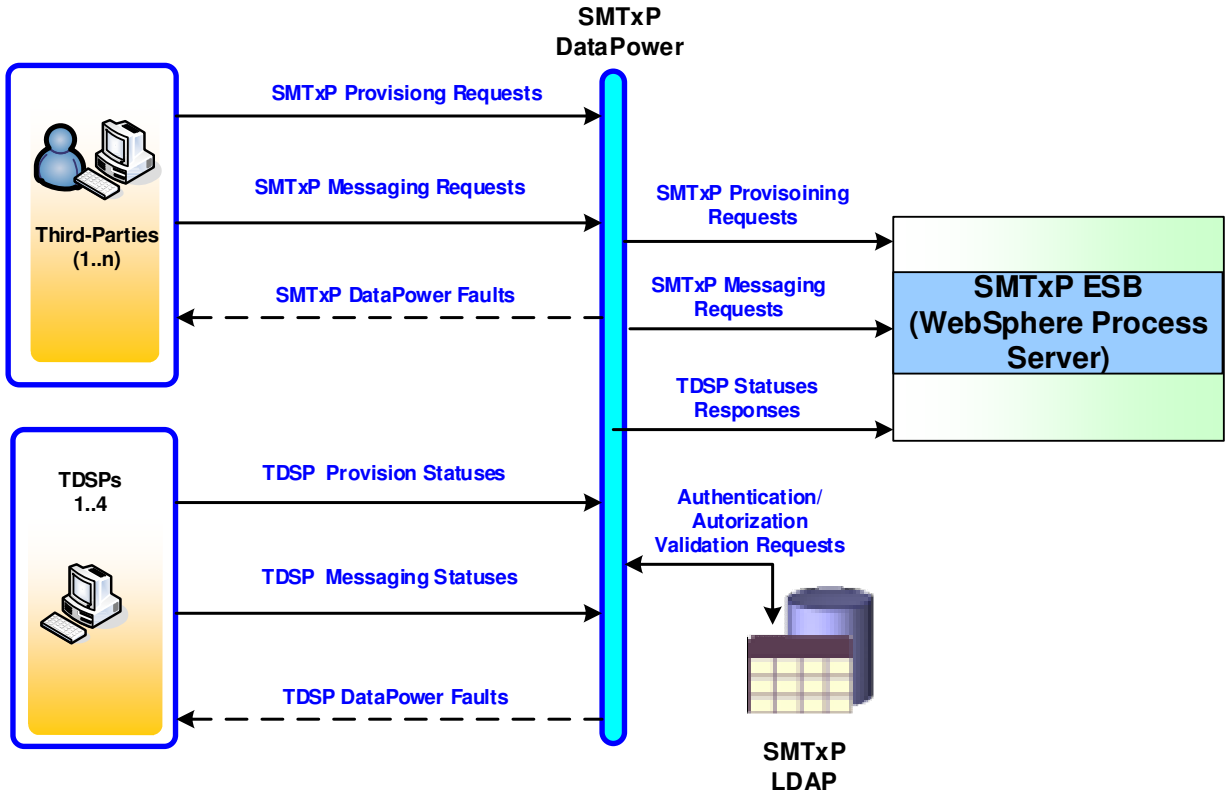


Figure 24: In-Home Device DataPower & ESB - Integration Overview

The diagram above provides a high level overview of the In-Home Device requirement for DataPower. It only shows inbound SOAP messages. NO VALIDATION will be done for outbound SOAP messages by DataPower.

1. **Third-Party Service Providers (Third-Party):** The Smart Meter Texas Portal (SMTxP) web users are Third-Parties & TDSPs who access portal through http channel or web services channels. The http channel has graphical user interface, through which they can provision & deprovision HAN Device. Third-Party users can also interact with SMTxP through secured web service channels, by posting SOAP messages to SMTxP ESB.
2. **Transmission & Distribution Service Provider (TDSPs):** TDSPs are responsible for propagating various requests to their head end systems and ultimately to the HAN Device. SMTxP ESB, makes various web service calls to TDSPs interface and TDSPs reports backs the status of requests asynchronously to SMTxP.
3. **Datapower:** For processing XML messages as well as any-to-any legacy message transformation.

4. **Enterprise Service Bus (ESB)** – SMTxP ESB is integration environment to facilitate exchange, transformation, routing of requests between front end portal and the requestor's API to backend TDSPs interfaces.

5. **SMTxP Repository**: – This is repository of interval, register and monthly billed usage data of various consumers belonging to four TDSPs operate in Texas region. It also maintains current and historical views of meter attributes, premise and REP of Record information. For In-Home Device requirement, it maintains, device provisioning information, status of devices, messaging requests & messaging logs.

8.2.2 Sequence Diagram

The following sequence diagram shows interactions between the requestor, TDSP, DataPower and SMTxP ESB.

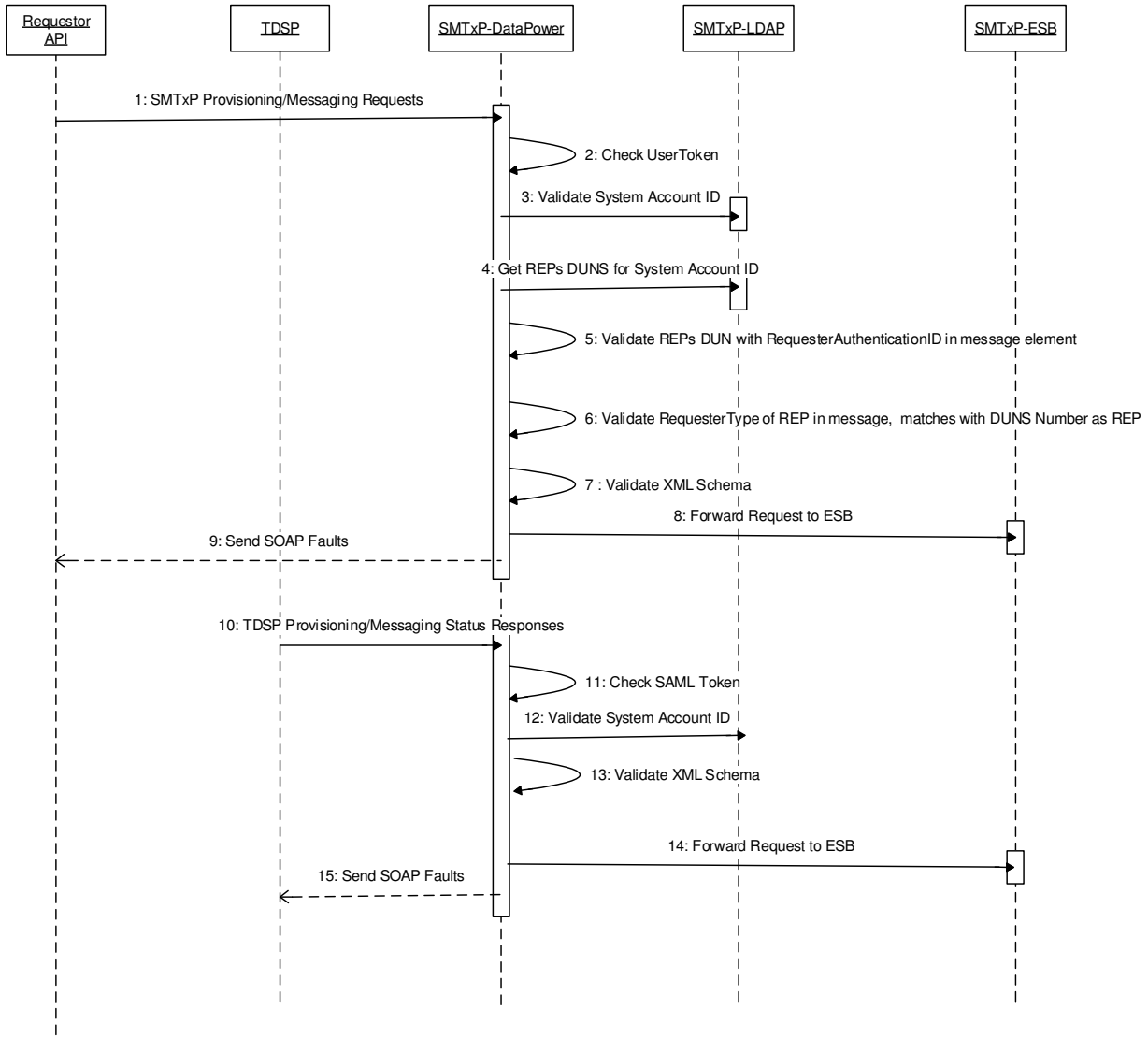


Figure 25: Sequence Diagram – Requestor-API, DataPower, ESB interaction

1. SMTxP Provision/Messaging Request: A provisioning/messaging request is received from the requestor through web service API.
2. Check User Token: DataPower authenticates User-Token (SSL keys) mechanism
3. Validate System Account ID : DataPower extracts System Account ID from the request and validates it against the SMTxP LDAP
4. Get requestor's DUNS Number: Based on System Account ID, DataPower retrieves DUNS Number from the LDAP
5. Validate DUNS Number: Compare DUNS Number retrieved from LDAP to DUNS Number from SOAP message request element <RequesterAuthenticationID>. If matched, go to next step, else generate SOAP Fault with error message

   "User Authentication failed"
6. Validate Requester Type: Compare <RequesterType> element value from SOAP message request to the requester type determined from DUNS Number. For example, if the DUNS Number belongs to a registered Third-Party, then the requester type is "THRD", if the DUNS Number belongs to a TDSP, then requester type should be "TDSP"

   "User Authentication failed"
7. Validate XML Schema: Data Power to perform following XML schema validation.

   - Check mandatory fields and if does not exists, generate SOAP fault with message "Required element <element name> does not exists in the request"

     for example -

```
<xsd:element minOccurs="1" maxOccurs="1" name="RequestID"
             type="xsd:string">
</xsd:element>
```

   - Validate fields lengths, if not within the specified range generate SOAP fault with message "Incorrect length for element <element name>"

     For example, minLength is 9 and maxLength is 16, if not in range generate fault-

```
<xsd:element minOccurs="1" maxOccurs="1" name="TDSPDUNSNumber">
      <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                  <xsd:maxLength value="16"></xsd:maxLength>
                  <xsd:minLength value="9"></xsd:minLength>
            </xsd:restriction>
      </xsd:simpleType>
</xsd:element>
```

   - Validate predefine enumeration values, if not one of them, generate SOAP fault with message "Invalid value for element <element name>"

     For example, the predefined values for StatusCode here are CON, PEN, STR, OPT, FLR

```
<xsd:element minOccurs="1" maxOccurs="1" name="StatusCode">
```

```
      <xsd:simpleType>
            <xsd:restriction base="xsd:string">
            <xsd:maxLength value="3"></xsd:maxLength>
                  <xsd:enumeration value="CON"></xsd:enumeration>
                  <xsd:enumeration value="PEN"></xsd:enumeration>
                  <xsd:enumeration value="STR"></xsd:enumeration>
                  <xsd:enumeration value="OPT"></xsd:enumeration>
                  <xsd:enumeration value="FLR"></xsd:enumeration>
            </xsd:restriction>
      </xsd:simpleType>
      </xsd:element>
```

- Validate xsd types, If incorrect generate SOAP fault with message “Invalid type of Element <element name>”

  For example, xsd:int type

```
<xsd:element minOccurs="1" maxOccurs="1" name="MCConfirmation">
      <xsd:simpleType>
      <xsd:restriction base="xsd:int">
            <xsd:enumeration value="0"></xsd:enumeration>
            <xsd:enumeration value="1"></xsd:enumeration>
      </xsd:restriction>
      </xsd:simpleType>
</xsd:element>
```

  xsd:string type

```
<xsd:element minOccurs="1" maxOccurs="1" name="Message">
      <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                  <xsd:maxLength value="80"></xsd:maxLength>
            </xsd:restriction>
      </xsd:simpleType>
</xsd:element>
```

  xsd:dateTime type

```
<xsd:element minOccurs="1" maxOccurs="1" name="StartTime"
                  type="xsd:dateTime">
</xsd:element>
```

- Validate max number of element in List, If incorrect generate SOAP fault with message “Element <element name> exceeds maximum limit”

For example, the max limit is10000,

```
<xsd:complexType name="BO_TDSPAddressList">
      <xsd:sequence>
            <xsd:element maxOccurs="10000" minOccurs="0"
```

```
                    name="Address" type="bons0:BO_TDSPAddress">
                </xsd:element>
            </xsd:sequence>
        </xsd:complexType>
```

8. Forward Request to TDSP: If not faults are generated, forward the valid requests to SMTxP ESB.
9. Send SOAP Faults to Requestor-API: If any faults generated, DataPower to send faults to the requestor's systems.

Similar validations apply for the interactions for SOAP messages flowing from TDSP to SMTxP.

8.3 Error Messages

The following Schema and Authentication error messages for In-Home Devices will be generated by Data Power:

Error Code : 2100 - Invalid Message Signature failure
Error Code : 2200 - SMT System Error
Error Code : 2300 - Authentication Failure Invalid Credentials
Error Code : 2400 - SMT Internal System Error
Error Code : 2500 - SMT internal Fault
Error Code : 2600 - SOAP Fault Message Rejected by SMT

9. In-Home Device Testing

9.1 Overview

NOTE: Verify that TDSPs have processes in place to support In-Home Device Testing with authorized requestors and In-Home Device vendors.

TDSPs provide a standardized method of testing and verifying In-Home Device functionality to ensure that In-Home Devices function as designed within the specifications detailed in the Smart Energy Profile 1.0 when operated on TDSPs advanced metering system (AMS) network. Authorized requestors and In-Home Device vendors should contact the TDSPs to initiate requests to perform In-Home Device testing.

Please initiate requests using the following contact information:

TDSP	TDSP In-Home Device Contact Information
AEP	HANSupport@aep.com
CenterPoint	han.support@centerpointenergy.com
Oncor	hansupport@oncor.com
TNMP	HANSupport@tnmp.com

9.2 In-Home Device Technical Requirements

The following are the technical requirements necessary for In-Home Device testing:

- 64-bit IEEE MAC address and installation code
- SEP 1.0 certification
  Note: If your device is not SEP 1.0 certified, contact ZigBee at http://www.zigbee.org or 1-925-275-6607.
- Production certificate
  Note: If your device does not have production certificates, contact Certicom at http://www.certicom.com/index.php/regzigbee to register for production certificates.

Each In-Home Device must have a unique MAC address and installation code assigned to it. These hexadecimal codes are used during key establishment and confirmation to set up the communication link between the In-Home Device and the AMS smart meter.

ZigBee Smart Energy is the world's leading standard for interoperable products that monitor, control, inform, and automate the delivery and use of energy. All ZigBee Smart Energy products are ZigBee certified to perform according to the SE 1.0 specification regardless of manufacturer. The ZigBee standard was custom-designed by industry experts to meet the specific market needs of businesses and consumers. All In-Home Devices submitted for validation testing should be Zigbee SE 1.0 certified.

Each In-Home Device MAC Address must have it's Certicom Elliptic Curve Cryptography (ECC) certificate. The ZigBee Smart Energy Public Key Infrastructure (PKI) uses Elliptic Curve Qu Vanstone (ECQV) implicit certificates. Each certificate binds a device MAC address and manufacturing identifier to an ECC key pair, allowing the device to authenticate itself to the network using its unique private key.

9.3 In-Home Device Test Cases

TDSPs perform a set of In-Home Device tests to validate compliance with ZigBee Smart Energy Profile 1.0. Due to the differences in their respective meters and Advanced Metering Infrastructure systems, the number and exact tests performed will vary by TDSP. The test cases include provisioning, deprovisioning, and messaging (simple text, load control and pricing). The TDSPs record the testing results and provide feedbacks to the authorized requestors and In-Home Device vendors that requested the tests.

If a list of test cases is needed, please request from the TDSPs via the following contact information:

TDSP	TDSP In-Home Device Contact Information
AEP	HANSupport@aep.com
CenterPoint	han.support@centerpointenergy.com
Oncor	hansupport@oncor.com
TNMP	HANSupport@tnmp.com

See below for a sample of the test cases.

ZIGBEE HAN TEST CASE	DEVICE TYPE	DESCRIPTION	DESIRED OUTCOME
PROVISIONING	ALL	Add a device to the AMS ESI	Device successfully joined to target ESI
DEPROVISIONING TEXT MESSAGE	ALL IHD PCT	Remove device from the AMS ESI Send a text message	Device disassociated from ESI Device displays the correct message
CANCEL TEXT MESSAGE	IHD PCT	Message cancelled	Message removed from the device
CANCEL FUTURE TEXT MESSAGE	IHD PCT	Message cancelled	Message removed from the device
PRICE MESSAGE	IHD PCT	Send a price signal	Price signal displayed on the device
TIME SYNCRONIZATION	ALL	HAN Device receives current time	Time is synchronized Time is displayed and supports DST
SEND LOAD CONTROL MESSAGE -	PCT	Temperature setpoint change for	Device adjusts setpoint at the

ZIGBEE HAN TEST CASE	DEVICE TYPE	DESCRIPTION	DESIRED OUTCOME
COOLING TEMPERATURE SETPOINT		COOLING for a prescribed period	requested time for requested duration
SEND LOAD CONTROL MESSAGE - HEATING TEMPERATURE SETPOINT	PCT	Temperature setpoint change for HEATING for a prescribed period	Device adjusts setpoint at the requested time for requested duration
SEND LOAD CONTROL MESSAGE - COOLING TEMPERATURE OFFSET	PCT SOME LCS	Temperature offset change for COOLING for a prescribed period	Device adjusts setpoint at the requested time for requested duration
SEND LOAD CONTROL MESSAGE - HEATING TEMPERATURE OFFSET	PCT SOME LCS	Temperature offset change for HEATING for a prescribed period	Device adjusts setpoint at the requested time for requested duration
CANCEL LOAD FOR A FUTURE EVENT	PCT LCS	Cancel a specific future Load Control event	Device cancels the event
CANCEL LOAD FOR AN IN - PROGRESS EVENT	PCT LCS	Cancel a specific in progress Load Control event	Device cancels the event
CANCEL ALL LOAD CONTROL EVENTS	PCT LCS	Cancel all load control events	Device cancels all events
SEND LOAD CONTROL FOR FUTURE EVENT FOR LC SWITCH	LOAD CONTROL SWITCH (LCS)	Activate the switch for the specified time period	Device activates switch for the requested period
DEVICE OPT OUT	PCT LCS	Device sends an opt-out signal to the ESI	ESI receives opt-out message Setpoint or switch is not altered

10. Texas In-Home Device Test Report

10.1 Overview

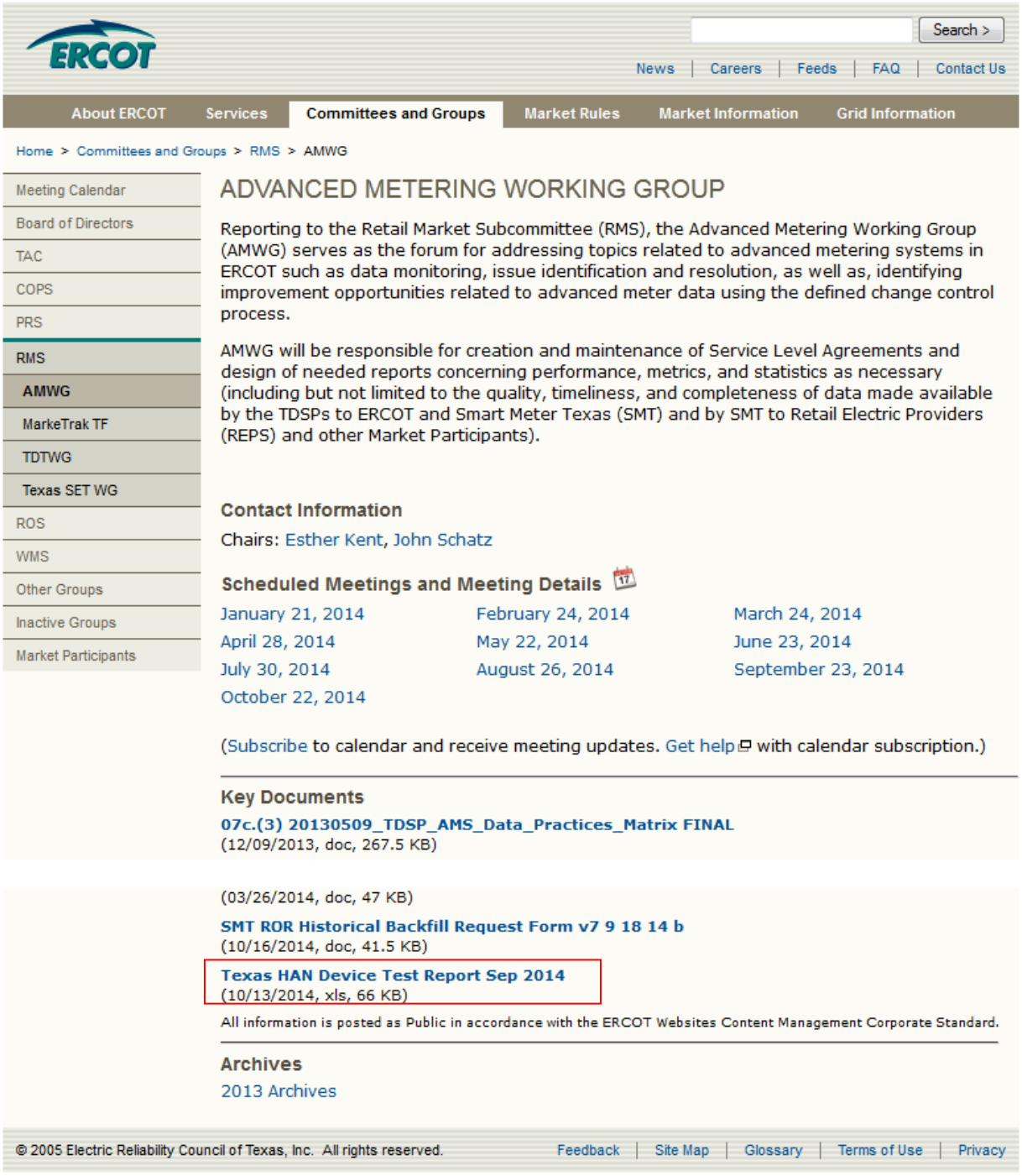
The TDSPs create a report monthly that reflects In-Home Devices that have successfully passed their interoperability testing. The Texas HAN Device Test Report is filed with each TDSP's monthly Advanced Metering Status compliance report. This report contains the manufacturer, product name, version, device type, device firmware, meter configuration, and date device was tested.

This report replaces previous reports known as In_Home Device Scorecard, In-Home Device Interoperability List, and In-Home Device Interoperability Evaluation Scorecard.

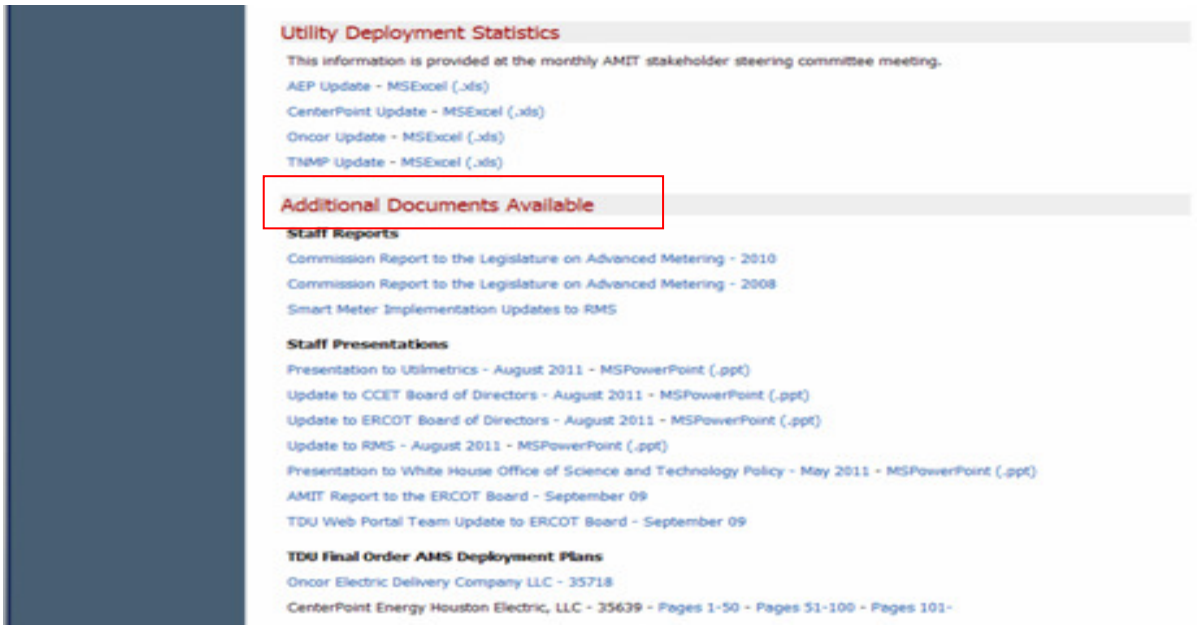
Report Name: Texas In-Home Device Test Report
Location of the report: PUCT Project 34610 Page: *http://www.puc.state.tx.us/industry/projects/electric/34610/34610.aspx*
Frequency: Monthly, every 15th of the month, included in TDSP filing of AMS compliance Report. The consolidated report is uploaded to the PUCT website within a week after TDSP filing.
Audience: The report is primarily geared towards market participants, but is also available to the public.
The report is cumulative and is current as of the last day of the previous month Because the report is cumulative, it is not expected to change much every month. The Remarks field (free-form text) will be used to indicate new entries or devices that have been removed. If there are no updates the report will still be included in the filing, with a note that no updates have been made. Refer to the report template.

The Texas In-Home Device Test Report can be found in the following Page:

www.ercot.com/committees/board/tac/rms/amwg/



Clicking the Texas In-Home Device Test Report link will launch the PDF version of the report, while clicking MSExcel will launch the Excel version of the report.



NOTE: The most current version and all previous versions of the "Historical Texas In-Home Device Test Report" can be found in the Additional Documents Available section.

10.2 Report Template

The report template of the Texas In-Home Device Test Report consists of two worksheets:

- Introduction - includes a brief description of the report, acronyms used in Device Types, Docket Numbers used by the TDSP's in filing the AMS compliance report, and the PUCT Interchange link.
- In-Home Devices – contains the list of the In-Home Device that were tested by the TDSPs

The following columns are available:

Texas HAN Device Test Report	
Column Name	**Description**
TDSP	Transmission and Distribution Service Provider that performed the test
In-Home Manufacturer	Manufacturer of the In-Home Device
Product	Manufacturer product name
Device Type	Device Type – • GW: Gateway • PCT: Programmable Communicating Thermostat • IHD: In Home Device

Texas HAN Device Test Report	
Column Name	**Description**
	• LCS: Load Control • SMA: Smart Appliance • RXT: Range Extender
In-Home Device Firmware	Firmware version of the In-Home Device
Meter Configuration	Configuration of the meter, varies by TDSP
Date Device Tested	Date when the In-Home Device was tested by the TDSP
Remarks	Free form text field

Sample Report Template

The following is a sample report template:

Texas HAN Device Test Report
As of 2012-04-30

TDSP	HAN Manufacturer	Product	Device Type	HAN Device Firmware	Meter Configuration	Date Device Tested	Remarks
CNP	Comverge	Power Portal	IHD	1.16	SR3.0.221	2009-08-30	
CNP	Comverge	Power Portal	IHD	1.17	SR3.0.221	2010-02-03	
CNP	Comverge	Power Portal	IHD	1.18	SR3.0.221	2009-07-15	
CNP	Control4	EC100	IHD	2.0705.1.109518	SR4.0.221	2012-01-05	
CNP	Control4	EC100	IHD	2.0705.1.109518	SR5.0.221	2012-03-03	
CNP	Control4	EC100	IHD	2.0705.1.109518	SR6.0.221	2012-03-03	
CNP	Energate	Energate LCS	LCS	1.2.59	SR3.0.221	2012-03-03	
CNP	Energate	Pioneer Series	PCT	1.8.8	SR3.0.221	2011-08-05	
CNP	General Electric	Energy Display	IHD	V.1.2.7-110624	SR3.0.221	2011-05-07	
CNP	General Electric	Nucleus	GW	1.2.27-110902	SR3.0.221	2012-04-30	*New
CNP	Tendril	Insight	IHD	1.12.1	SR3.0.221	2011-10-10	
CNP	Tendril	Setpoint TST-7	PCT	1.10.0d20804	SR3.0.221	2012-04-12	
CNP	Tendril	Volt	LCS	1.10.2d6295	SR3.0.221	2012-04-30	*New
Oncor	Comverge	Power Portal	IHD	1.16	5.65, 1.6.9	2009-08-30	
Oncor	Comverge	Power Portal	IHD	1.17	5.65, 1.6.9	2010-02-03	
Oncor	Comverge	Power Portal	IHD	1.18	5.65, 1.6.9	2009-07-15	
Oncor	Control4	EC100	IHD	2.0705.1.109518	5.65, 1.6.9	2012-01-05	
Oncor	Control4	EC100	IHD	2.0705.1.109518	5.65, 1.6.9	2012-03-03	
Oncor	Control4	EC100	IHD	2.0705.1.109518	5.65, 1.6.9	2012-03-03	
Oncor	Energate	Energate LCS	LCS	1.2.59	5.65, 1.6.9	2012-03-03	
Oncor	Energate	Pioneer Series	PCT	1.8.8	5.65, 1.6.9	2011-08-05	
Oncor	General Electric	Energy Display	IHD	V.1.2.7-110624	5.65, 1.6.9	2011-05-07	
Oncor	General Electric	Nucleus	GW	1.2.27-110902	5.65, 1.6.9	2012-04-30	*New
Oncor	Tendril	Insight	IHD	1.12.1	5.65, 1.6.9	2011-10-10	
Oncor	Tendril	Setpoint TST-7	PCT	1.10.0d20804	5.65, 1.6.9	2012-04-12	
Oncor	Tendril	Volt	LCS	1.10.2d6295	5.65, 1.6.9	2012-04-30	*New
AEP	Comverge	Power Portal	IHD	1.16	5.65, 1.6.9	2009-08-30	
AEP	Comverge	Power Portal	IHD	1.17	5.65, 1.6.9	2010-02-03	
AEP	Comverge	Power Portal	IHD	1.18	5.65, 1.6.9	2009-07-15	
AEP	**Control4**	**EC100**	**IHD**	**2.0705.1.109518**	**5.65, 1.6.9**	**2012-01-05**	***Remove**
AEP	Control4	EC100	IHD	2.0705.1.109518	5.65, 1.6.9	2012-03-03	
AEP	Control4	EC100	IHD	2.0705.1.109518	5.65, 1.6.9	2012-03-03	
AEP	Energate	Energate LCS	LCS	1.2.59	5.65, 1.6.9	2012-03-03	
TNMP	Energate	Pioneer Series	PCT	1.8.8	5.65, 1.6.9	2011-08-05	
TNMP	General Electric	Energy Display	IHD	V.1.2.7-110624	5.65, 1.6.9	2011-05-07	
TNMP	General Electric	Nucleus	GW	1.2.27-110902	5.65, 1.6.9	2012-04-30	*New
TNMP	Tendril	Insight	IHD	1.12.1	5.65, 1.6.9	2011-10-10	
TNMP	Tendril	Setpoint TST-7	PCT	1.10.0d20804	5.65, 1.6.9	2012-04-12	
TNMP	Tendril	Volt	LCS	1.10.2d6295	5.65, 1.6.9	2012-04-30	*New

11. In-Home Device Reprovisioning During Meter Exchange

11.1 Overview

During the meter exchange process, the old smart meter is replaced by new smart meter. The new meter is physically installed in the premise. In addition, the TDSPs reprovision the In-Home Devices i.e. send the In-Home Device network keys to the new meter to provision the In-Home Devices that were previously paired/connected to the old meter.

The processes and procedures that the TDSPs perform during the meter exchange process are TDSP-specific, and these internal processes can affect the processing time on when the In-Home Devices are displayed in the new meter in the Smart Meter Texas portal.

In general, the following are the steps that Smart Meter Texas and the TDSPs undertake during meter exchange to automatically reprovision the In-Home Devices to the new meter.

Step	Description
1	TDSP sends meter exchange transactions with old meter id, new meter id and ESIID
2	SMT removes the In-Home Devices from the old meter
3	SMT removes the old meter from the ESIID
4	SMT adds the new meter to the ESIID
5	SMT adds the In-Home Devices to the new meter. (This is accomplished via the TDSP In-Home synchronization and other TDSP-SMT processes)
6	SMT displays the In-Home Devices in the UI

The In-Home Device reprovisioning process is a function of the TDSP meter exchange. The TDSPs remove the old meter, and add the new meter to the ESIID. If In-Home Devices were previously paired/connected to the old meter, the TDSPs will provision these In-Home Devices to the new meter i.e. the In-Home Device networking keys will be deposited to the new meter. TDSPs provide this In-Home Device information to SMT in order to display and synch up the In-Home Devices in the portal. This is accomplished using several TDSP-SMT processes that include the TDSP MeterHANSynch service, which is an internal process between the TDSPs and SMT to display the In-Home Devices in the new meter. The SMT website will display the ESIID with the new meter id. The In-Home Device screen of the new meter will display the In-Home Devices accordingly. An email will be sent to inform the customer if the customer is registered to SMT that their Smart Meter has been replaced if they have In-Home Device(s) provisioned with the Smart Meter.

11.2 Process Flow Diagram

Here are the detail process steps for In-Home Device Meter Exchange (In-Home Device Reprovisioning) process.

005. TDSP performs meter exchange process

090. TDSP performs reprovisioning of In-Home Devices from old meter to new meter

010. TDSP sends meter exchange information to SMT

020. SMT receives meter exchange information

030. SMT requests information on In-Home Devices associated with ESIID

040. TDSP receives request from SMT

050. TDSP sends In-Home Device information update to SMT

060. SMT receives In-Home Device information

070. SMT updates the In-Home Device provisioning status and make available to the In-Home Device screen in the SMT website

080. SMT updates the In-Home Device provisioning tables

100. If meter has provisioned In-Home Device

110. If customer is registered at SMT and has provided an email address in profile

120. SMT sends an email to inform the customer of the meter exchange

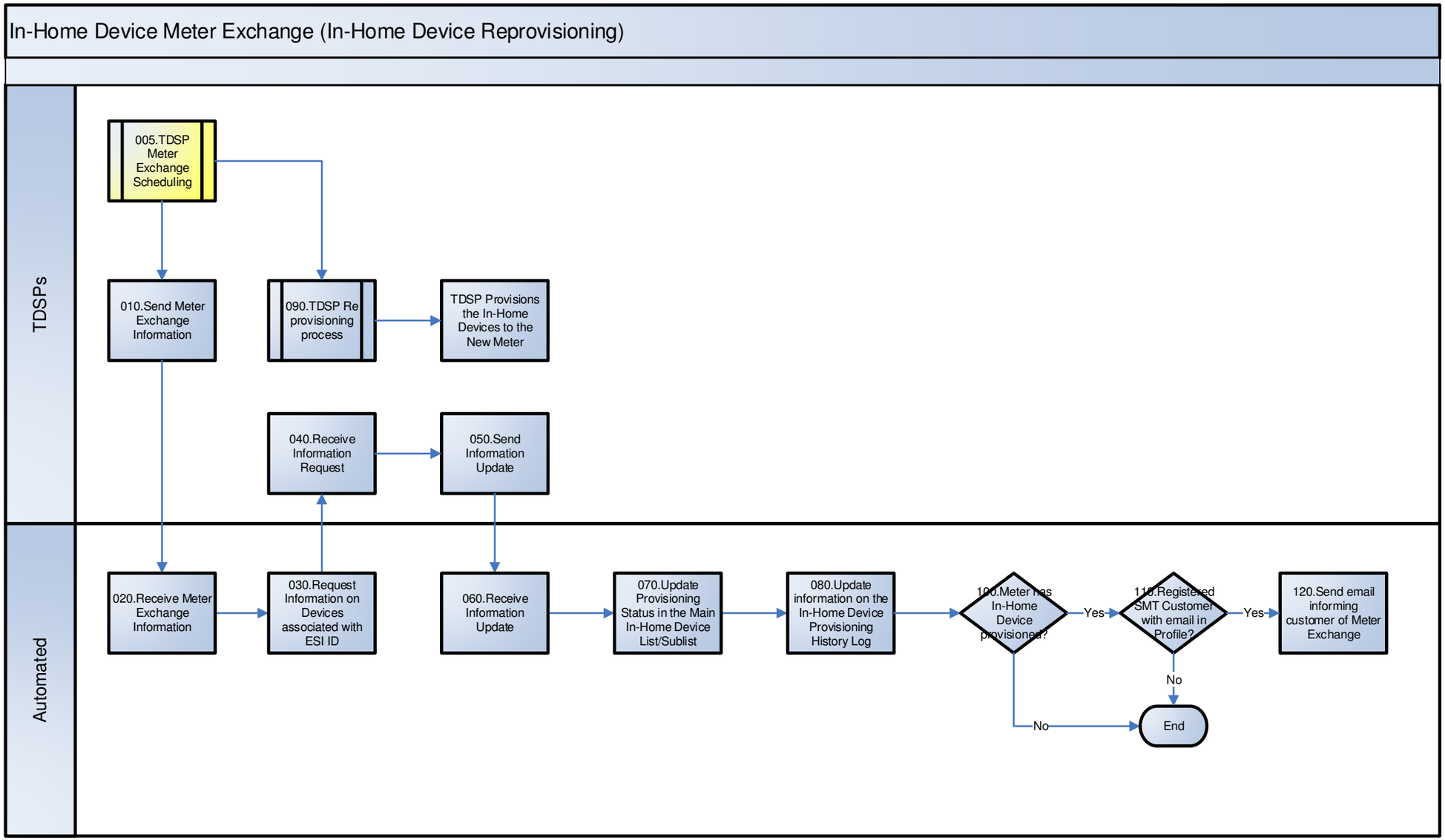


Figure 26: In-Home Device Meter Exchange (In-Home Device Reprovisioning) Process

12. Appendices

12.1 Smart Energy Profile 1.0

The SMT In-Home Device API's are based on Smart Energy Profile 1.0.

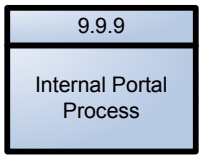
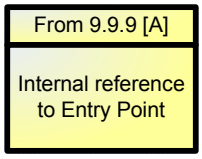
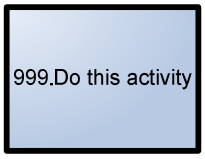
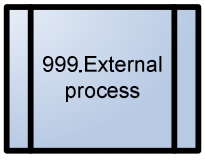
075356r15ZB_SE_PT
G-SE_Profile_Specific

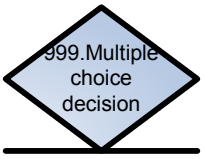
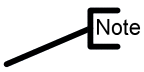
12.2 Process Flows

The process diagrams are drawn in Visio 2003 using a Cross Functional Flowchart method, i.e., Actors in horizontal swim lanes.

The flows contain activity boxes as well as associated UI Wireframes. Therefore, the flows represent both the process steps and the UI transition.

The following contains a legend that describes the various shapes that are used in the Process flows.

Shape	Name	Description
	Process	This shape represents a process within the Portal environment for which a process diagram exists. The process number will be in the top bar, the process name in the box.
	Process Entry Point Link	When this shape has 'From' in the title box, it represents the process that you came from – the initiating process that brought you to this point. The linking process number along with a letter reference is shown in the title box. If you were to open the linking process, you would find the corresponding linked process which includes the same letter reference. Since these typically represent an Entry Point into a process, these shapes are most often yellow.
	Activity	This shape represents a single activity or step within a process diagram. The text will be a description of the activity.
	External Process	This shape represents a process that is external to Portal but which requires an information exchange. An example would be receiving authorization paperwork which would trigger a Portal process.

Shape	Name	Description
	State	This shape is used in State diagrams rather than Process flows. The box contains text that describes a specific State being explored, e.g., a State diagram for a status field might contain states of Pending, Active, etc.
	Decision	This shape represents a decision box. The text will be a question that requires a Yes or No answer. Connectors coming out of the box will delineate which path to take based on the response to the question.
	Multiple Choice Decision	This shape represents a multiple choice decision. Multiple Connectors come from the bar attached to the box and each will represent a possible answer to the question. This shape is used most often to designate a path to a link when multiple actions can be taken from a UI screen. In this situation, each Connector will contain the text shown on the screen link (e.g., *Register Now*) or a button or keyboard key (e.g., *Enter*).
	Wait	This shape represents a break in the process for the affected actor. It is used to designate a waiting period before continuing with additional activities required to finalize the process.
	UI Wireframe / Screen	This shape represents a UI Wireframe or Screen. The box contains a label that represents the UI identifier. This shape will be next to a process or activity box and implies that the process or activity is occurring while this UI screen is presented to the user. The succession of these screen boxes on a Process flow represents the screen transition associated with the process.
	On-page Reference	The on-page reference represents a break in the process flow that is continued elsewhere on the same page. The shape will contain a label, typically an upper-case letter. The same shape with the same letter will be found on the same page and represents where the flow should continue.
	Off-page Reference	The off-page reference is similar to the on-page reference with the exception that the associated connection point will be found on another page within the same process. The shape will contain a label as well as a hyperlink to/from its associated reference point. The label typically contains the process number and unique upper-case letter.
	Annotation	This shape is used to enter a note on the diagram that is informational but not an activity to be performed. The text of the note is contained within the bracket. The extended line, or connector, for the shape is attached to the related diagram item to which the note applies.

12.3 In-Home Device Project Assumptions

HAN Assumptions
The communication and securing of an In-Home Device (i.e. devices provisioned with the ESI) in the activity of sending and receiving messages through the AMS are in scope for this project.
Only In-Home Devices that are provisioned with the ESI will be able to access data directly from ESI.
The ESI will be the clear service boundary between the AMS and the Provisioned In-Home Device(s).
AMS will provide a safe, secure and reliable conduit for the delivery of information to and from the ESI.
The common web portal will have the ability to maintain an updated list of provisioned (i.e., connected) In-Home Devices or the pending provisioning requests
The ESI and the In-Home Device will exchange provisioning information to establish a Home Area Network.
There will always be two way communication across the AMS infrastructure.
There is an expectation that authorized requestors of the APIs and Customers will require availability approaching 24 x 7 x 365 access to the AMS. Note: There will be uncontrollable down times affecting the availability of the AMS which is unavoidable. It may be cost prohibitive to have 99.9999% availability. Additionally there will be predetermined agreed upon maintenance windows or down times when full access to the ESI may be restricted or not available. These may change over time.
The AMS will supply accurate time keeping and time synchronization, so that data moving off the AMS will be accurately time stamped.
Non-provisioned In-Home Devices are out of scope for this project and there will not be any TDSP AMS communication link directly with these devices, although we acknowledge that they will exist at our customer sites.
The TDSPs will update firmware in the ESI and provide advanced communication of the updates to the authorized users per the PUC Rule 25.130. The TDSPs will notify the market of their schedule for testing and upgrading firmware.
The Texas In-Home Device applications, functionality, and processes will conform, to applicable national standards for Smart Energy and In-Home Device applications as those standards develop.
Only In-Home Devices that adhere to nationally recognized non-proprietary standards such as ZigBee, Home Plug, or the equivalent will be the only devices that can be provisioned to the ESI.
We will be able to communicate unique messages to a unique Provisioned In-Home Device.
The project solution will minimize “dead / stranded devices” (i.e., a device that has no functionality to future owners / authorized users).
Customers will be able to deprovision any In-Home Device associated with their premise
There will be a minimum set of Smart Energy clusters and attributes, for Texas, supported by the TDSPs ESIs which also support the minimum requirements of the PUCT Rule. In-Home Devices will be able to see this information at the ESI. · Demand Response / Load Control · Pricing · Text messages · Direct real time access to customer usage data · 15 minute usage (interval data)

12.4 Glossary of Terms

Term	Description
3rd party	Any party that has registered on the TDSP portal, other than the customer's current REP of Record or ERCOT or the Retail Customer A registered user of the portal that, when granted permission by a customer via an LOA, can access that customer's historical usage data. 3rd Parties typically are aggregators, consultants, or competing REPs that are seeking information in order to provide aggregation services or to propose pricing for alternative suppliers to the customer. All REPs are, by default, also 3rd Parties when they are not the customer's ROR.
ACL	Access Control List
ADA/508	Section 508 of the Americans with Disabilities Act – an act to establish a clear and comprehensive prohibition of discrimination on the basis of disability.
Add In-Home Device / Adding	See Provisioning
Admin	Someone who can assign different users access rights/permissions: add and delete users; change role of users.
Aggregator	PUC registered aggregator pursuant to 25.111.
Alert	A notification that an event has taken place (e.g. general, system, meter, etc.)
AMS	Advanced Metering Solutions A system including advanced meters and the associated hardware, software and communications systems including meter information networks that collect time differentiated energy usage and performs the functions and has the features specified in this section / rule.
AMS WAN	Wide Area Network – this is the network between the TDSPs, REPs and ERCOT.
API	Application Programming Interface that allows one program to talk to another
Authenticated user	Users who have exchanged credentials with the portal. Authenticated users have full access to information associated with their portal role.
Broadcast Addressing	a network address that allows
Business Participant	These are the project participants that define the NEEDS or (What's) for the organization or groups they represent. Business Participants include: Consumers TDSPs REPs PUC Staff Power Marketers Solution Providers / Manufacturers / Vendors ERCOT
CAPTCHA	Completely automated public turing task to tell humans and computers apart.
CIM/CDM	Common Information Model/ Common Data Model
Connect In-Home Device / Connecting	See Pairing
CSV	Comma Separated Values – a common file format in which the data is presented as a list of fields that are separated by commas. CSV files are typically opened with an application or spreadsheet software, such as MS-Excel.
Customer	The actual end use retail consumer or the Customer authorized agent acting on behalf of the actual end use Retail Customer.
Customer Service	Service for retail customers

Term	Description
Deprovisioning	Process of removing the In-Home network keys (MAC Address and Install Code) from the Meter. This means that the In-Home Device communication with the AMS network is terminated.
Deregistering	Process of terminating the In-Home Device's enrollment in a Third-Party program.
Device Added	See Paired
DUNS	Number assigned to a business organization by Dunn and Bradstreet. REPs may have multiple DUNS Number associated with their SMT account. Third-Parties can establish only one DUNS Number in SMT.
EDM	Electronic Delivery Mechanism. EDM is a standard defined by NAESB. Version 1.6 is used for exchange of usage data by Texas market participants.
Energy Data Agreement	An agreement between a Customer and a Third-Party in which the Customer allows a Third-Party to have access to his historical usage data.
Entity	A profile containing a collection of company information about the Entity (TDSP, REP, Regulatory, Third-Party, Non-Residential Customer).
Entity Administrator	An employee or representative of an Entity that is assigned the role and responsibility to manage (grant and revoke) permissions to the Entity's users, including additional Entity Administrators.
Entity User	An individual that has permission to see or retrieve data from the portal that is associated with an Entity.
ERCOT	Electric Reliability Council of Texas that operates the electric grid and manages the deregulated market for 75 percent of the state
ESB	Enterprise Server Bus
ESI	Energy Services Interface - This is a service boundary that provides security and, often, coordination functions that enable secure interactions between the Home Area Network and the AMS. It facilitates two way communications. Note that ESI has nothing to do with "ESIID" or "ESI ID". Energy Services Interface. Provides security and, often, coordination functions that enable secure interactions between relevant In-Home Devices and the TDSP (Utility) and REP. Permits applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and integration with building management systems. Also provides auditing/logging functions that record transactions to and from In-Home Devices. This may also be referred to, in national standards, as ESP (Energy Services Portal)
ESI ID	Electric Service Identifier, a unique identifier for the point of electric delivery to a consumer.
ESIID	Electric Service Identifier, a unique identifier for the point of delivery
FAQ	Frequently asked questions.
FTPS	File Transfer over SSL protocol
HAN	Home Area Network - – this is the network between the advanced meter and the home device as mentioned in the AMS rules
HTTP	Hyper Text Transfer Protocol
Human Web Interface	Presentation layer of the portal accessed by human beings.
IEC	The International Electrotechnical Commission is the international standards and conformity assessment body for all fields of electrotechnology.

Term	Description
Individual accounts	The collective of Residential Customer and Supplemental User roles. An Individual account may have one, both, or neither of the 2 roles. An Individual account takes on the Residential Customer role upon attaching ESIIDs to his account. An Individual account takes on the Supplemental User role when another Residential Customer grants him access to the Residential Customer's ESIIDs.
Interface-T	Machine to machine interface (e.g. API, etc.) between the data warehouse and authorized users.
Interface-Z	Transport of the TDSP data to the common data warehouse.
Join In-Home Device / Joining	See Pairing
Link In-Home Device / Linking	See Pairing
LDAP	Lightweight Directory Access Protocol.
LTPA	Lightweight Third-Party Authentication
M2M	Machine-to-machine. A system-level interface to be implemented using web services.
MARS	Market Advanced Readings and Settlements.
Master Data	Includes data related to a premise, meter attribute, the Rep of Record, and user settings
MDMS	Meter Data Management System.
Message	Any information communicated between the In-Home Device and an authorized entity (for example, a Third-Party Service Provider).
Meter Group	A collection of meters within some pre-defined or assigned boundary, such as reading cycle or zip code. (This could be a select group of meters.)
Meter Ready	The In-Home Device network keys have been transmitted to the Meter. The Meter is ready to establish communication with the In-Home Device.
MLS	Multiple Language Support.
MOM	Message Oriented Middleware
Multicast addressing	a network technology for the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the multiple destinations split. (e.g. – a conference call)
NAESB	North American Energy Standards Board. NAESB is an industry forum for the development and promotion of standards for wholesale and retail natural gas and electricity.
Near Real Time	As frequently as each attribute of the meter can be provided, in accordance with the delivery mechanism.
Non-residential Customer	A Non-residential Customer is a type of Customer that can have multiple users and a user administrator.
OPC	Office of Public Utility Council
Operating day	The day energy is consumed. This is also known as "Day 0" when discussing the processing of energy usage.

Term	Description
Organizational Entity	An entity that could have multiple users that have access to portal data and are responsible for the security there of. A centralized location that allows for a hierarchical structure or that you can associate one or more user ids or ESIIDs to. A virtual relationship between related Admins and user ids. This is not a physical role, identity and does not have permissions
Paired	The In-Home Device and the Meter have successfully exchanged data transformation and validation of test vectors using Certificate based key exchange (CBKE) based on Elliptical Curve Cryptography (ECC). The In-Home Device is ready to display usage or receive messages.
Pairing	Per SEP 1.0 r15-"The following details the key establishment exchange data transformation and validation of test vectors for a pair of Smart Energy devices using Certificate based key exchange (CBKE) based on Elliptical Curve Cryptography (ECC). " -For example, when a Tendril IHD completes pairing, the device is PAIRED to the Meter, and will be capable of displaying the Meter Cluster data on the device.
Ping	An on demand request to determine the network status of a meter or In-Home Device (i.e. is a device active on the network)
Point In Time Selectivity	There is an insert time stamp and an update / delete time stamp, so you know the birth and death of the record. You will know if a record exists or not based on the time stamp. Similar to Push Down Stack
Point to Point	Generally refers to a connection restricted to two endpoints. The endpoints are truly defined. (e.g. – A telephone call)
Poll	An on demand request for data from a meter or In-Home Device
Private Home Page	The Private Home Page is the non-promoted public home page for the Common AMS portal. This page will be utilized by the administrators and users of REPs, Third-Parties, TDSP and Regulatory.
Provisioning	Process of transmitting the In-Home Device network keys (MAC Address and Install Code) to the Meter. Provisioned means the In-Home Device Status is "Meter Ready". The meter is ready to establish communication with the In-Home Device.
Public Home Page	The Public Home Page is the promoted public home page for the Common AMS portal. This page will be utilized by Residential Customers, Supplemental Users, Non-Residential Administrators and Users, and 3rd Party Administrators and Users.
PUCT	Public Utilities Commission of Texas.
Push Down Stack	Once you write a piece of data to an interval, you write the date you wrote it. If you change it, you don't overwrite the data, you add another layer entry (row) for the data with the new date. The oldest version of the data is on the bottom of the stack. Similar to Point in time selectivity
Range extender	an unsecured device whose function is to extend the broadcast range between two secured devices. Range extenders provide no logic functionality and are not invested with connectivity details. Range extenders provide neutral signal amplification between an ESI and In-Home Device(s) and will not occupy a HAN Device allocation slot provided by a utility ESI. A range extender provides an open communication support.
Range repeater	a secured broadcast range extending device that participates in developing a secured trust link between an ESI and an In-Home Device. A range repeater will occupy an In-Home Device slot provided by a utility ESI. A range repeater provides a closed communication link between target In-Home Devices.
Reading	The register value on a meter at a point in time

Term	Description
Registration	Process of enrolling an In-Home Device in a program in the REP or Third-Party CSS. Provisioning is a pre-condition of registering a In-Home Device
Rejoin	Process of provisioning a previously provisioned In-Home Device to a replaced ESI at the same premise
Release	A new subset of additional functionality and / or improvements to existing functionality on the portal. A release is planned for and comes at a specific time.
Remove In-Home Device / Removing	See Deprovisioning
REP	Retail Electric Provider who is PUC certified pursuant to 25.107.
Reprovision	See Rejoin
Retail Market Functionality	These are the business processes and system processes around move ins and move outs, switches and other market activities.
ROR	REP of record, which is the REP which is currently in the TDSP records as serving the premise.
RPM	Rational Portfolio Manager, an internal IBM tool being used as a document repository.
RPO	Recovery Point Objective
RTO	Recovery Time Objective.
Security Question and Answer	This is a predetermined list of user specific questions a user can select from and provide an answer to in order to have the user id or a temporary password emailed to you.
SEP	Smart Energy Profile
Service Boundary	This is where the REP of Records connect to the TDSP operated AMS (for example,. web portal, TDSP In-Home Interface).
SFTP	Secure File Transfer Protocol
SMT	Smart Meter Texas
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOI	Service Oriented Integration
SSL	Secure Socket Layer is a set of cryptographic protocols that provide security and data integrity for communications over networks such as the Internet
SSO	Single Sign-on
Supplemental User	A friend or family member of the residential user who has been granted access by the residential account holder. The intent is for this user to be an individual and not a business.
System Integrator	An entity, other than the TDSP, that is the developer and hosting agent for the portal and services.
TAI	Trust Association Interceptor
TAM	Tivoli Access Manager
TDI	Tivoli Directory Integrator
TDSP	Transmission and Distribution Service Provider
TDSP In-Home Device Interface (THI)	This is a service boundary that provides security and, often, coordination functions that enable secure interactions between the Home Area Network and the AMS. It facilitates two way communications.

Term	Description
Technical / Solution Participant	These are the project participants that define the Solutions or agree that the Solutions that are documented are appropriate to address the Business Needs defined for the project.
THI	TDSP In-Home Device Interface - This is a service boundary that provides security and, often, coordination functions that enable secure interactions between the Home Area Network and the AMS. It facilitates two way communications.
TIM	Tivoli Identity Manager.
UEG	Update Utility Enrollment Group
Unauthenticated user	Users who have mot exchanged credentials with the portal. An unauthenticated user is able to access the Home page and education content.
Usage data	Calculated number of KWH, KVA, KW, KVAR, KVARH, PF consumed for a given period of time as applicable to the ESIID/meter
Use Case Verbs	· Enter: Keying information into a User Interface field · Select: Selecting an option (link) on a User Interface page · Logon: Initiate a web portal session · Logoff: End a web portal session · Import: Upload information from a file into a web portal field · Export: Download information from the web portal · Submit: Initiating actions to update the portal (e.g., validate, record, post information, etc.) · Navigate: Accessing the web site and or a specific web portal page
VPN	Virtual Private Network.
Web portal	May be referred to as portal or web portal
WSDL	Web Service Description Language - XML-based language for describing Web services
XML	Extensible Markup Language
ZigBee	Specification of a suite of high level communication protocols using small low-power radios