soapUI Starter Kit for Smart Meter Texas Portal In-Home Device Interfaces

Prepared for

Texas Competitive Electric Market

AMIT Working Group

November 20, 2014

Table of Contents

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

This document describes a soapUI Starter Kit that Third-Party Service Providers can use for invoking the Smart Meter Texas (SMT) In-Home Device Web Service interfaces.

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.

1.2 About soapUI

soapUI is a free, open source desktop application available for download via the WWW (visit http://www.soapUI.org) for inspecting and invoking Web Services.

1.3 About this Starter Kit

This Starter Kit comes with the following:

- SMT In-Home Device interface document – describes interface functions
- soapUI project – contains XML interface definitions that can be used by the soapUI application

Prerequisites and steps for using the Starter Kit are described below.

1.4 Prerequisites

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

1.4.1 Environmental Setup

Prior to using this Starter Kit, you must provide the following Production information.

Production

Third-Parties can submit this environmental information to request access to the SMT Production environment.

- SSL certification –SMT will only accept a CA certificate. You need to provide to SMT with their CA SSL certificate for Production environment setup.
- Signing certificate–SMT will accept a CA signer certificate. You need to provide SMT with their CA signer certificate for Production environment setup.

- DUNS – An SMT system account will be created for each Retail Electric Providers (REPs) and Third-Party Service Providers. You must use this account created for your Company when accessing the SMT Production environment. If you are a Retail Electric Provider (REP) you may have one or more DUNS number associated with the SMT system account. If you are an independent Third-party Service Provider, you can only have one DUNS number associated with your SMT system account.
- IP Address(es) – Access is restricted to the SMT Production Environment. IP Address is needed to enable access.
- Entity Name – This is the preferred name of your Company.

You 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 your SMT system account for Production, account information will forwarded to the SMT administrator of your organization.

1.4.2 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[1]:

- iKeyMan
- Keytool and
- OpenSSL.

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.

[1] 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.

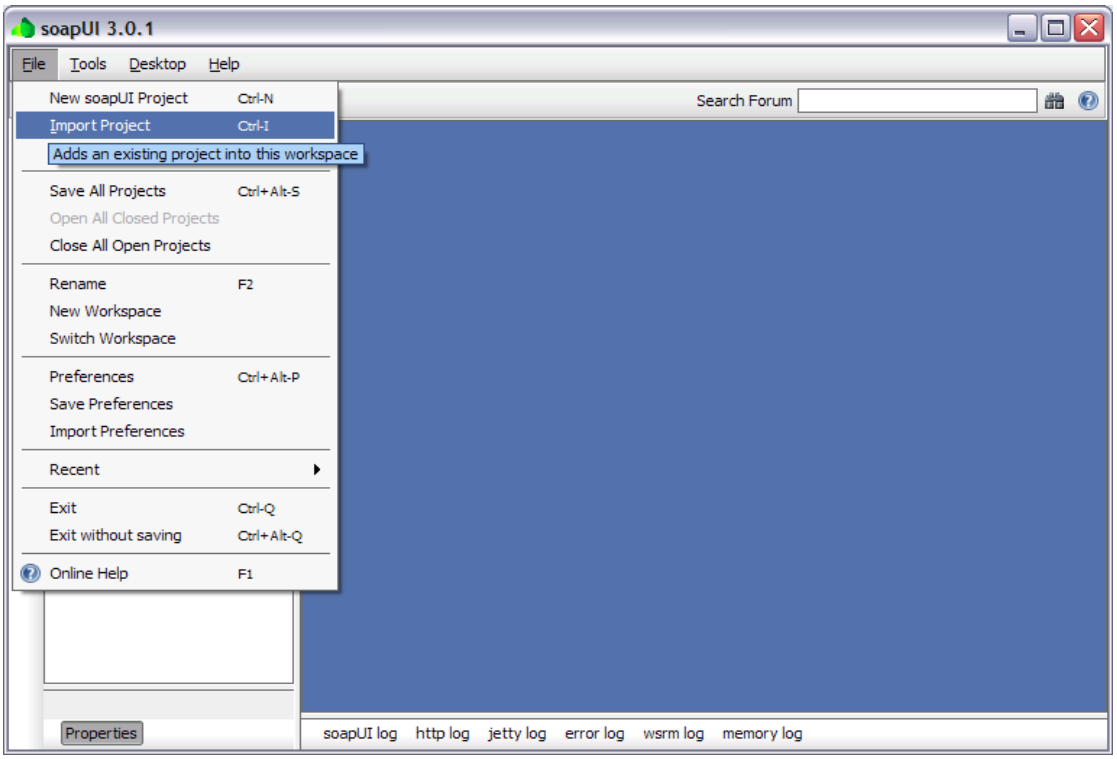
1.5 Overview of Steps for using the Starter Kit

The next sections of this document describes how to:

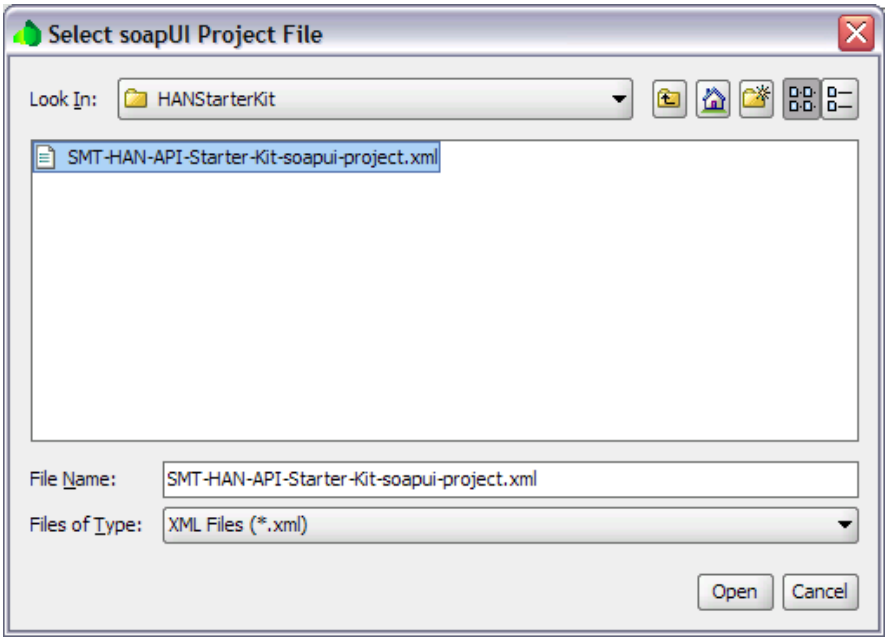
1. Set up the Starter Kit
2. Configure SSL
3. Configure WS-Security
4. Invoke Web Services

2 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.



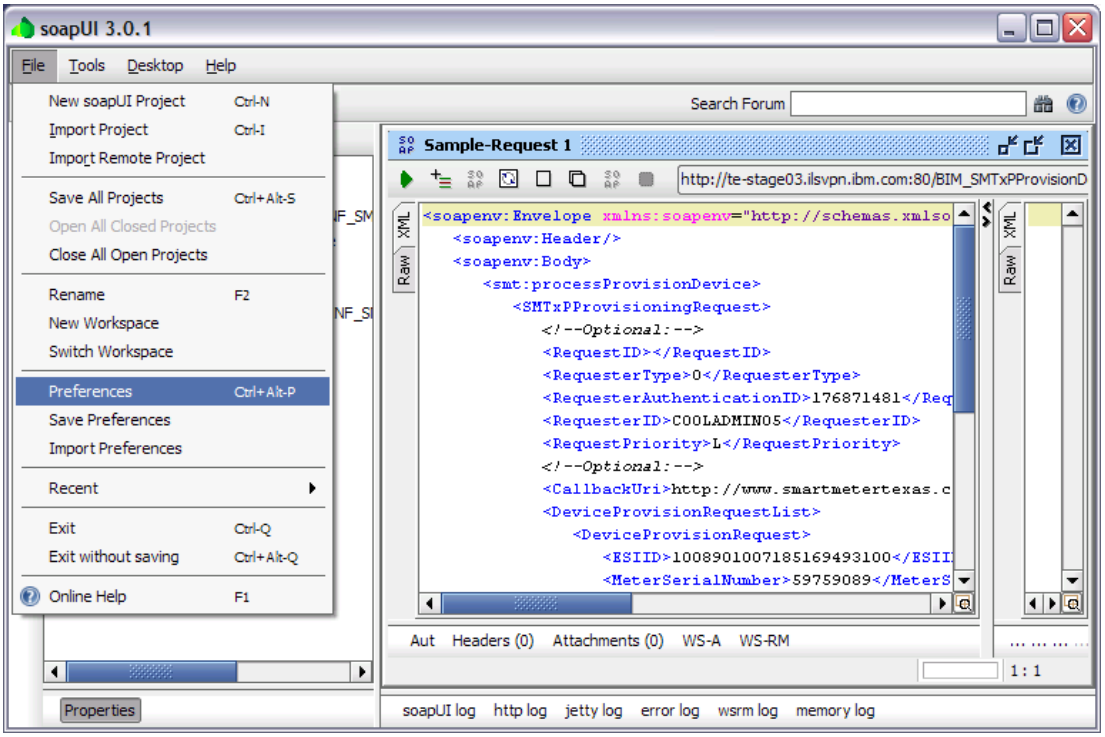
Navigate to directory and the Starter Kit project file and select it. Click Open. This is pictured below.



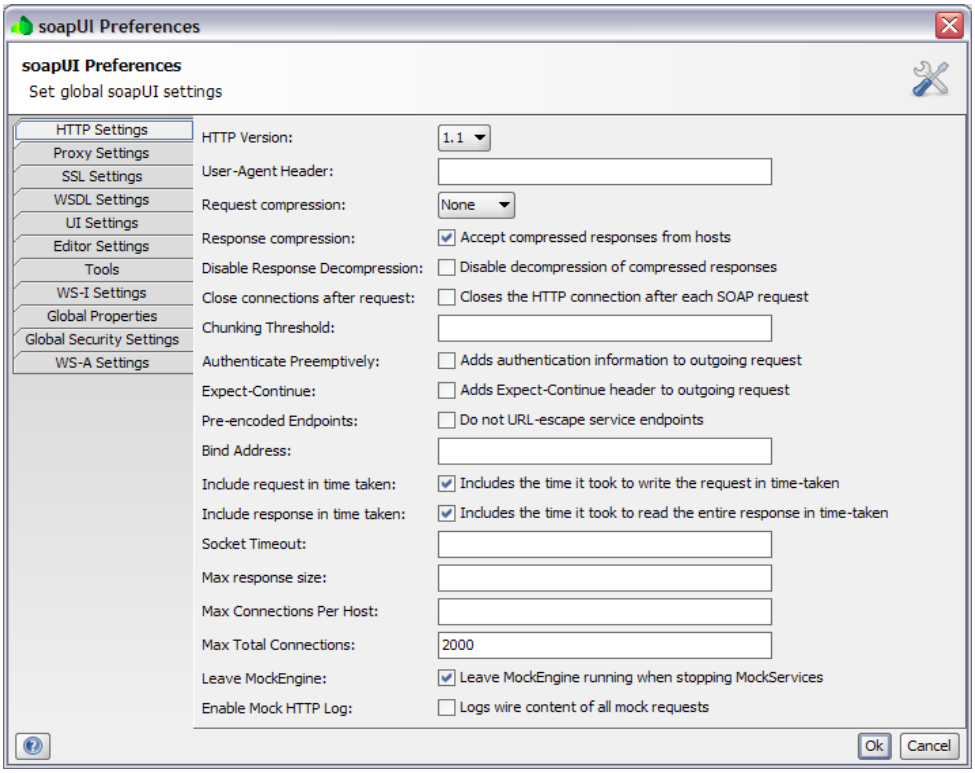
soapUI will load the Starter Kit project.

3 SSL Configuration

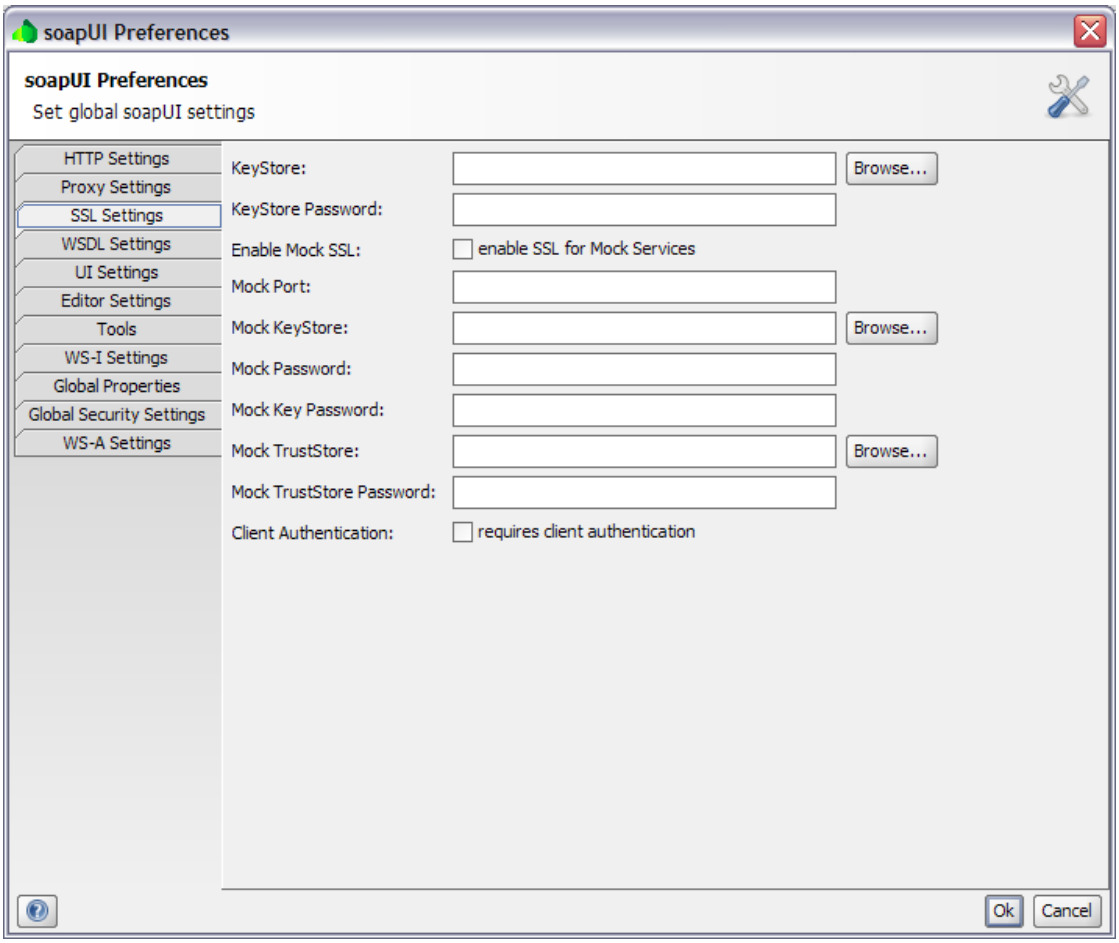
Launch SoapUI and click on File -> Preferences as shown below.



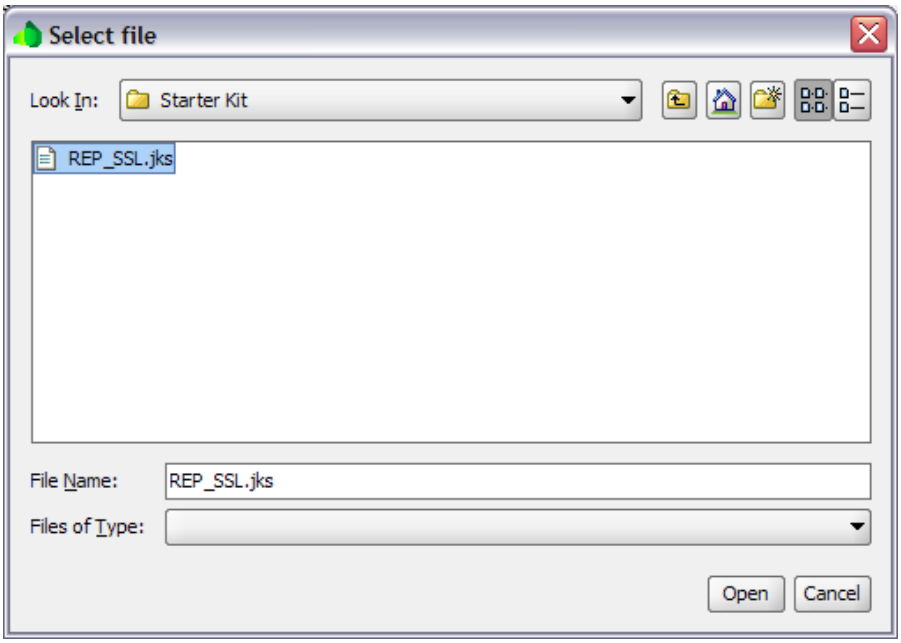
The soapUI Preferences will pop-up in a separate window.



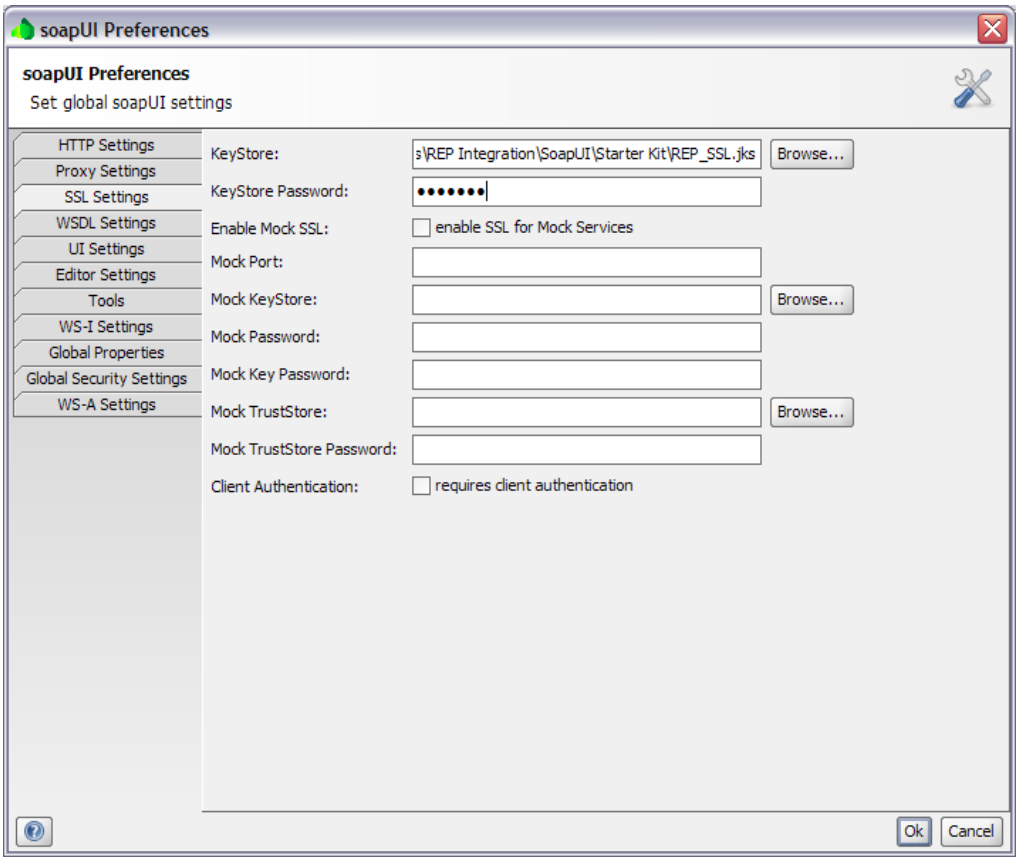
Select SSL Settings on the left navigation bar.



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



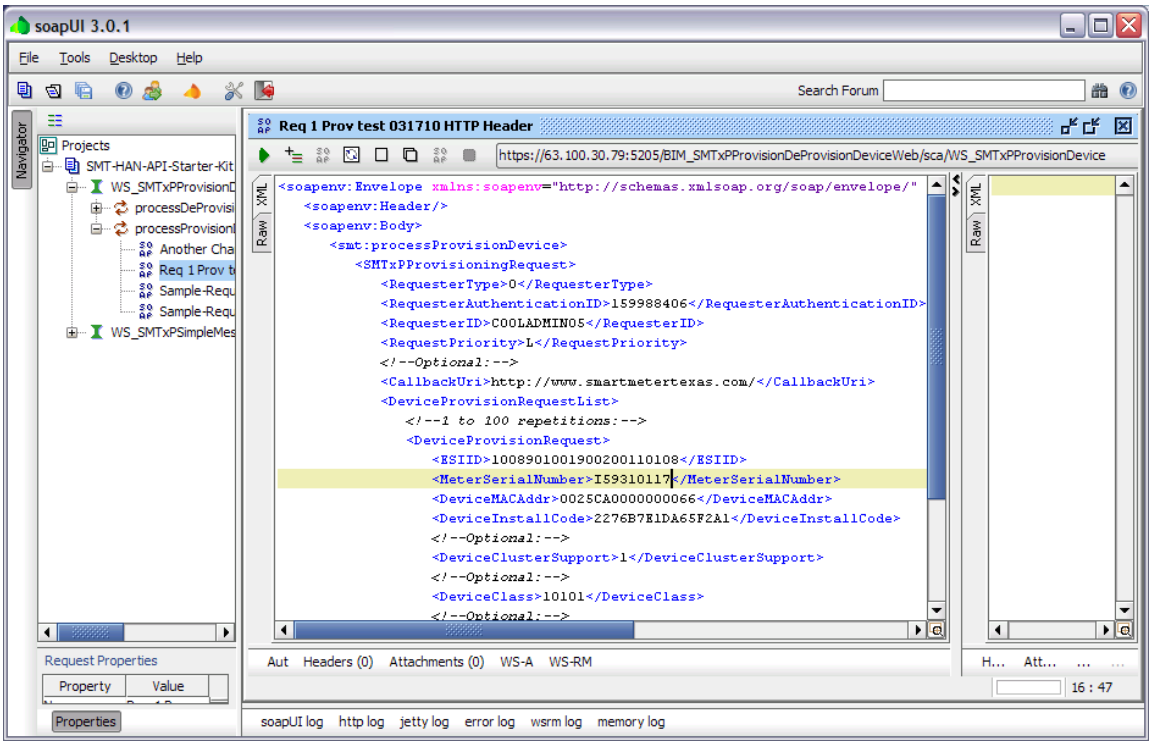
Input your Keystore password, for example, SMT1234, and click Ok.



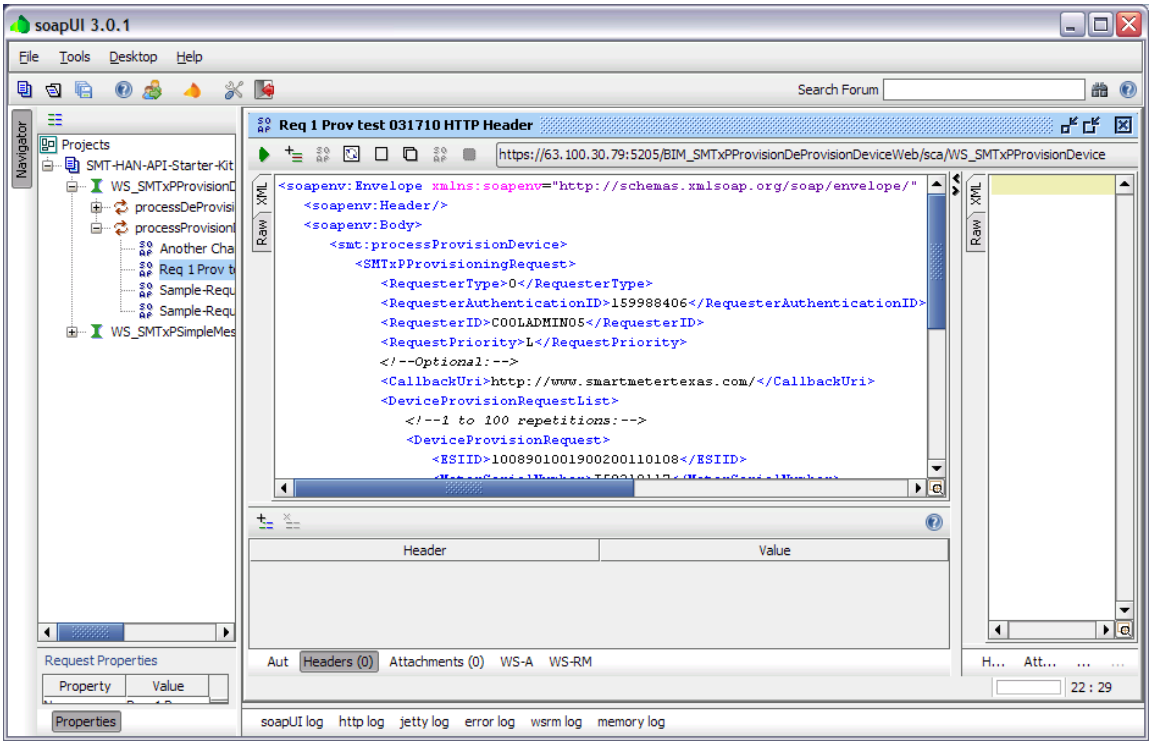
4 HTTP Header Configuration

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 that is submitting the request.

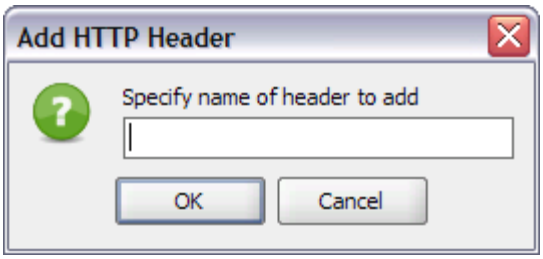
To add a HTTP header, locate the Headers field at the bottom middle of a request window as depicted below.



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

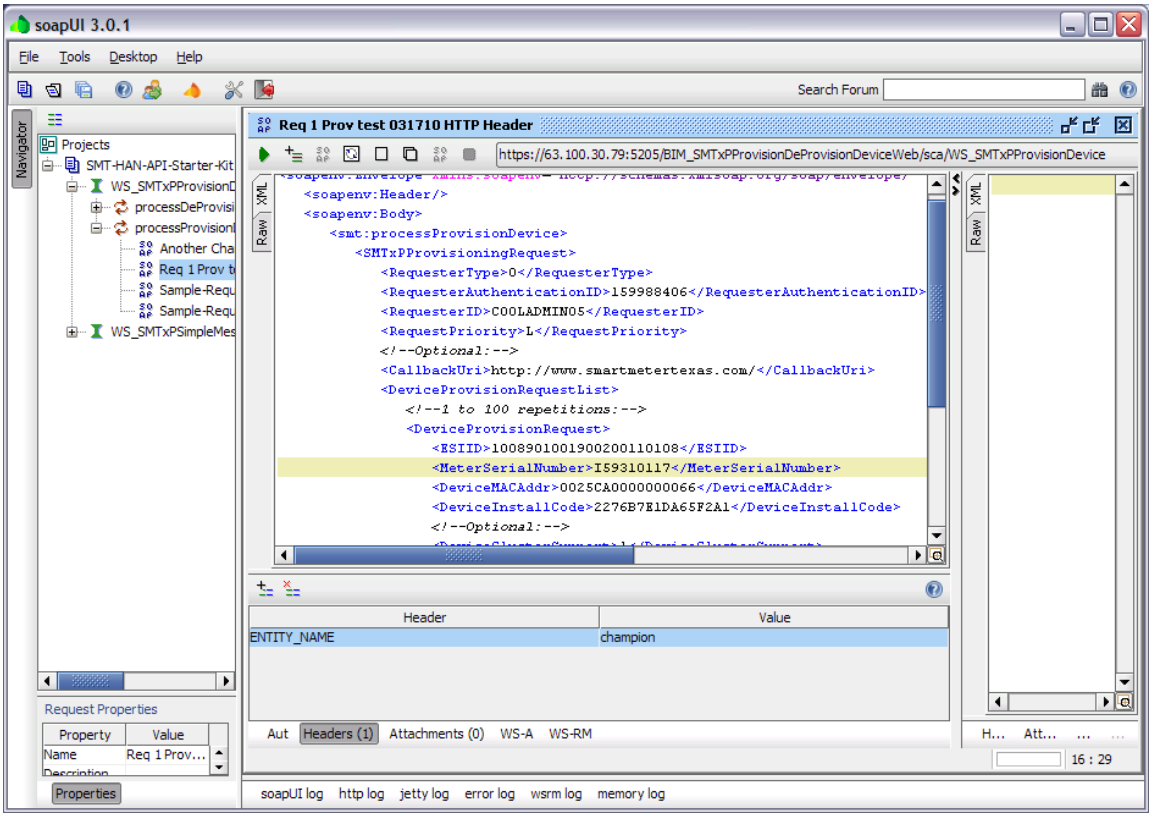


Clicking the + sign above the Headers information box to obtain a HTTP headers name input box as seen below.



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 1.4.1.

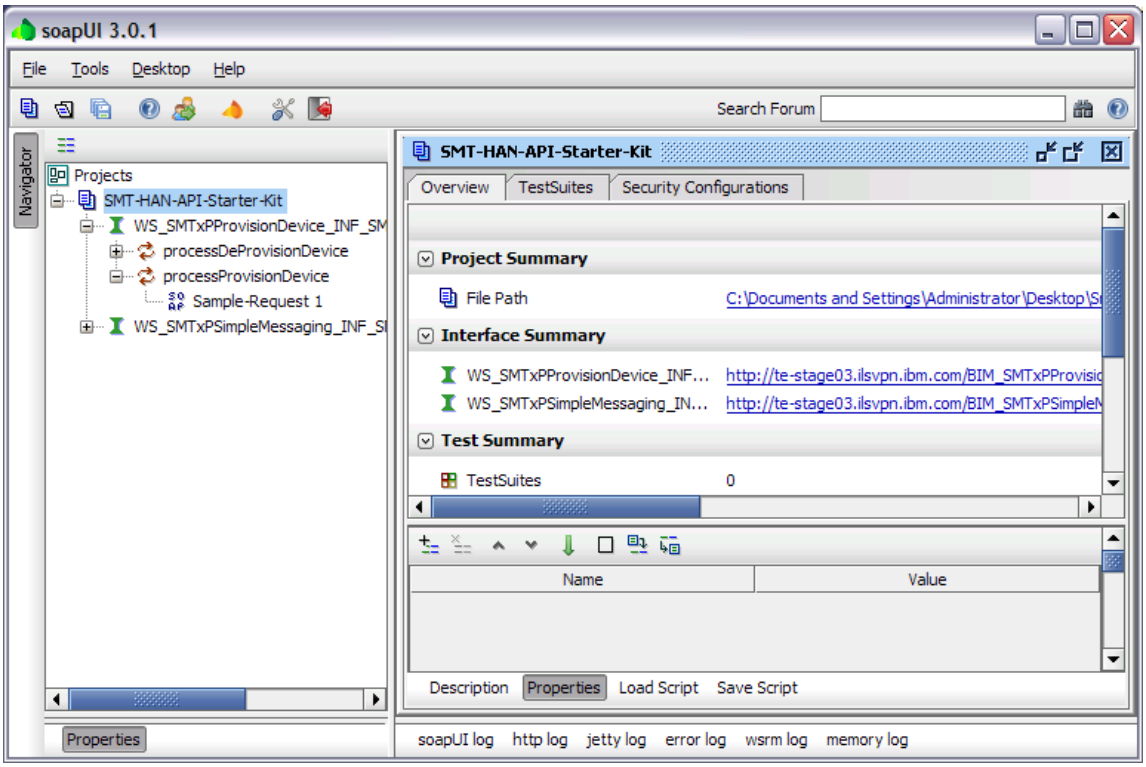


The above configuration allows SMT to determine source or origination of the request.

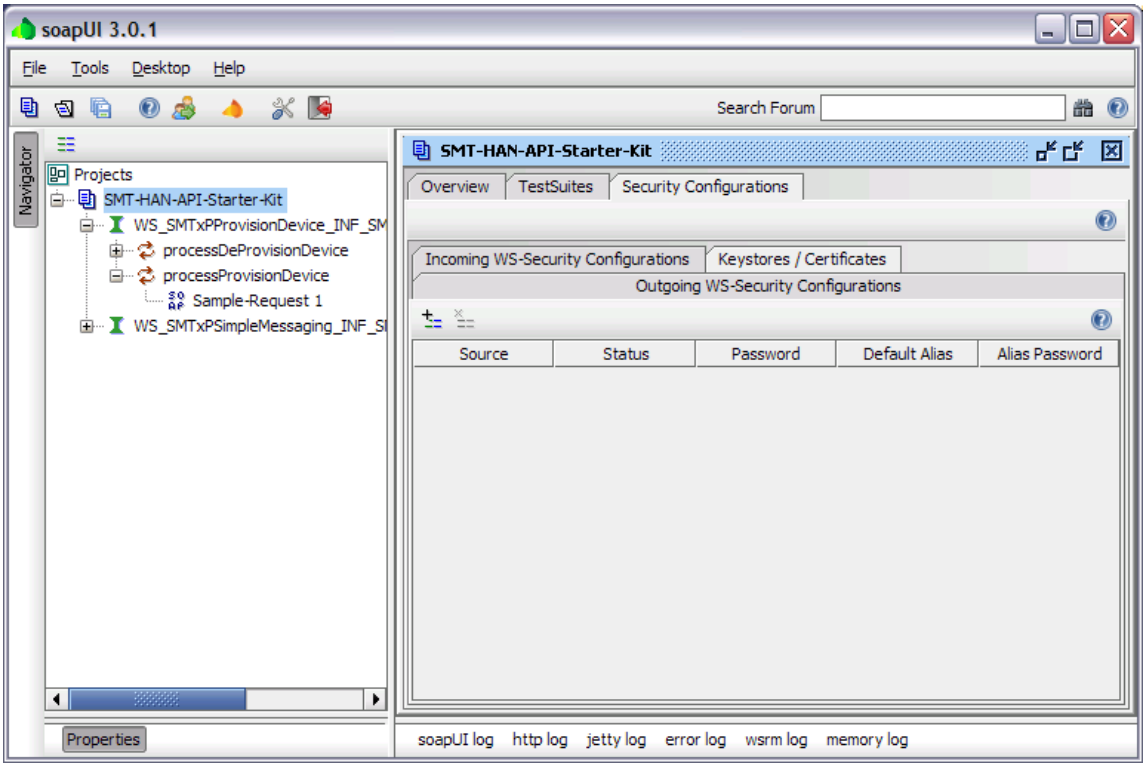
5 WS-Security Configuration

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.

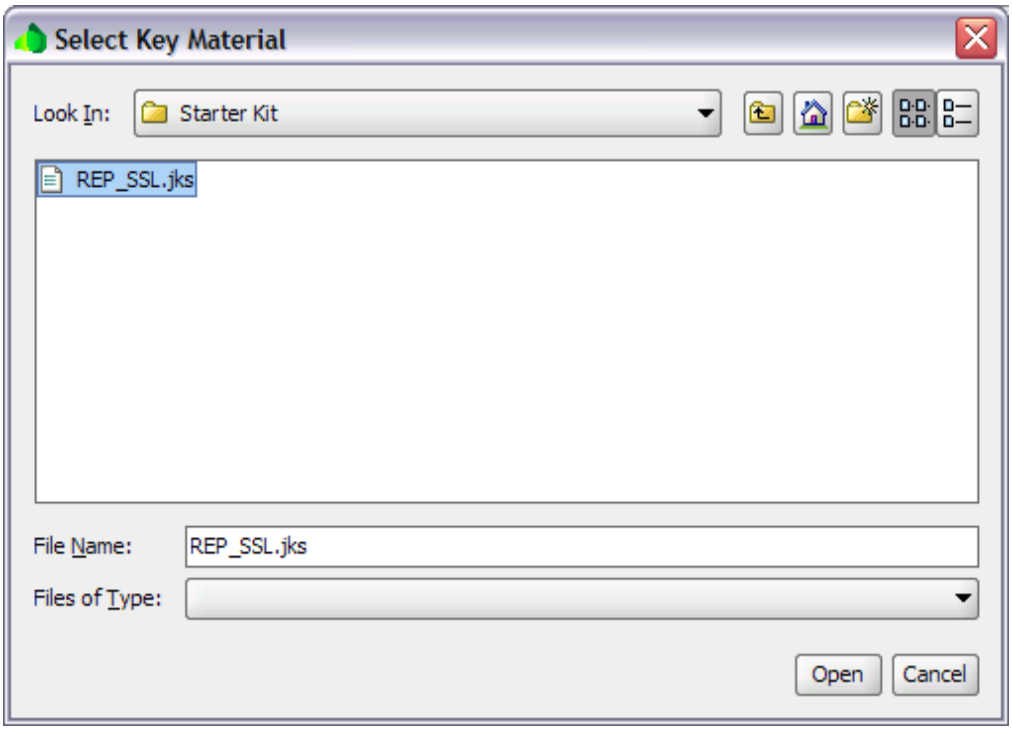
Select soapUI project and double click.



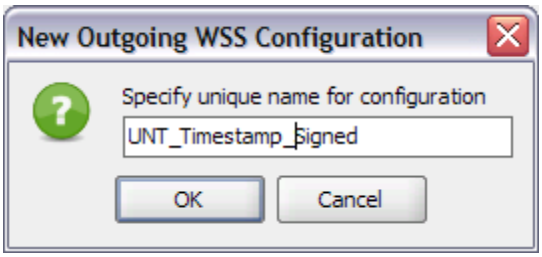
Select the Security Configurations tab and then the Keystore/Certificates tab as pictured below.



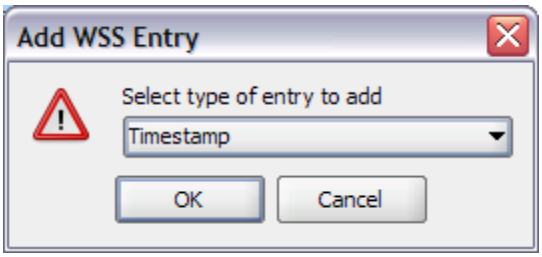
Click on + sign to specify Keystore/Certificate.



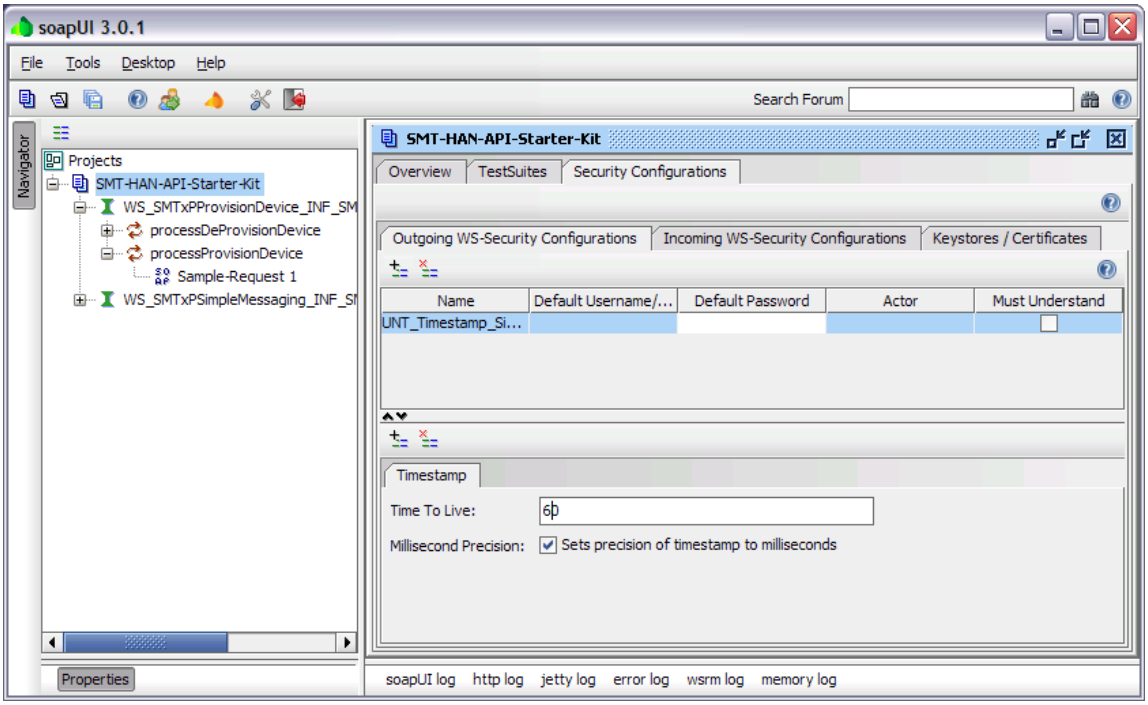
Now, click on Outgoing WS-Security Configuration tab. Then click on + sign and enter a unique configuration name. Below, UNT_Timestamp_Signed is used to represent: user name token, timestamp, and signed.



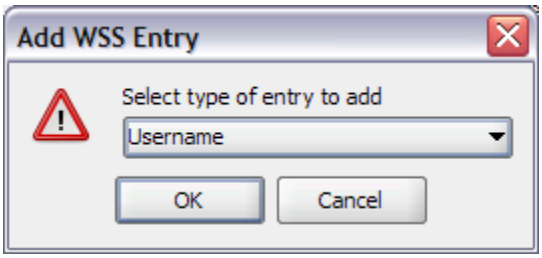
In the lower half panel. Click on + sign and select Timestamp as type of entry to add.



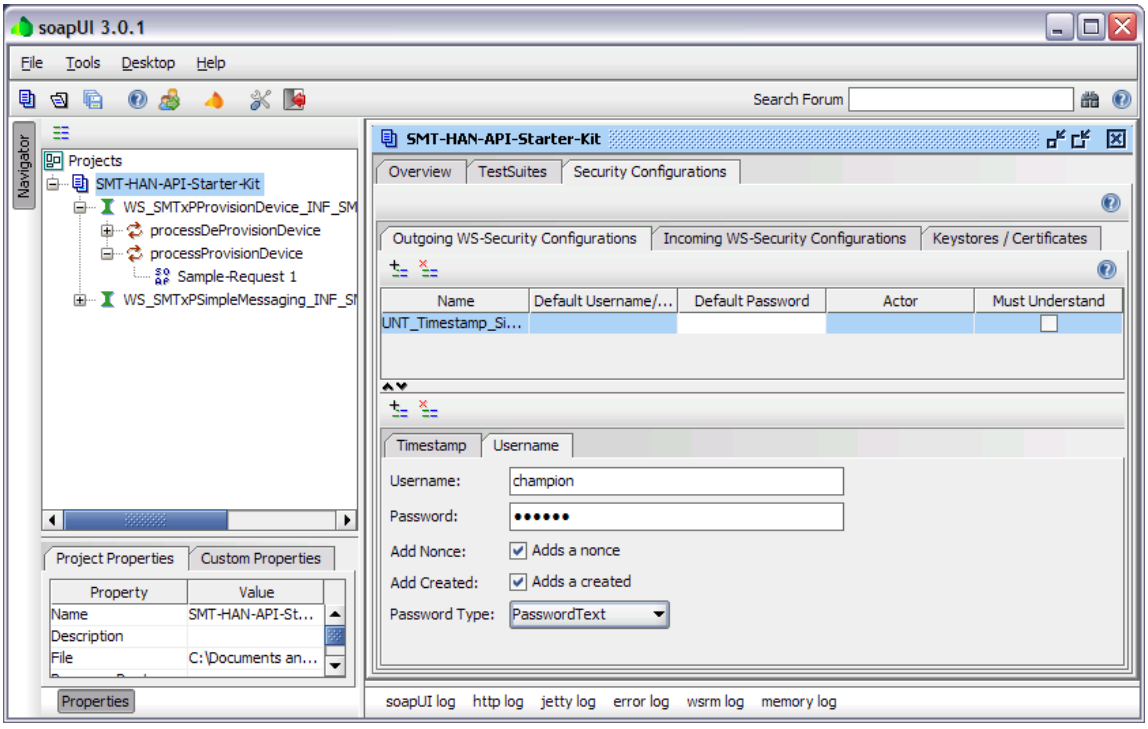
Enter Time to live value, for example, 60.



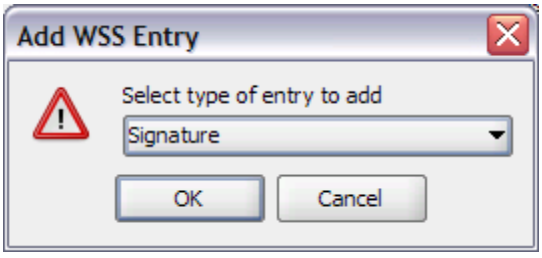
Select + again in lower half panel and select Username as type of entry to add.



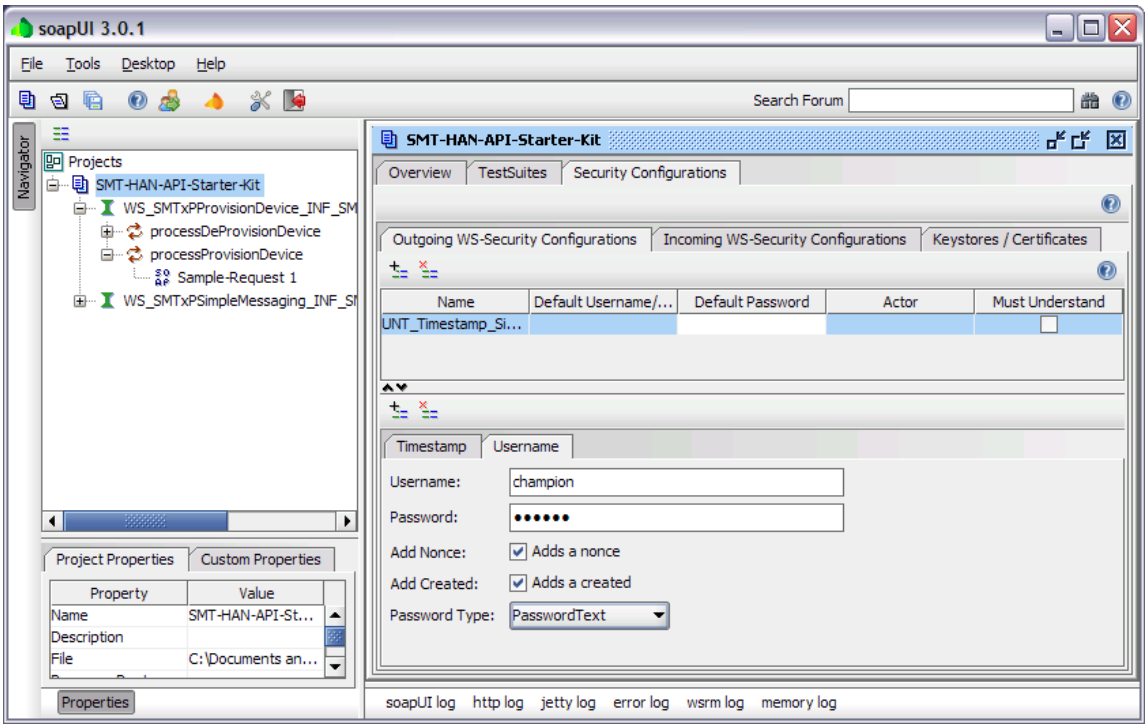
Specify Username, password and PasswordText as type of password to add. (Specifying password is mandatory).



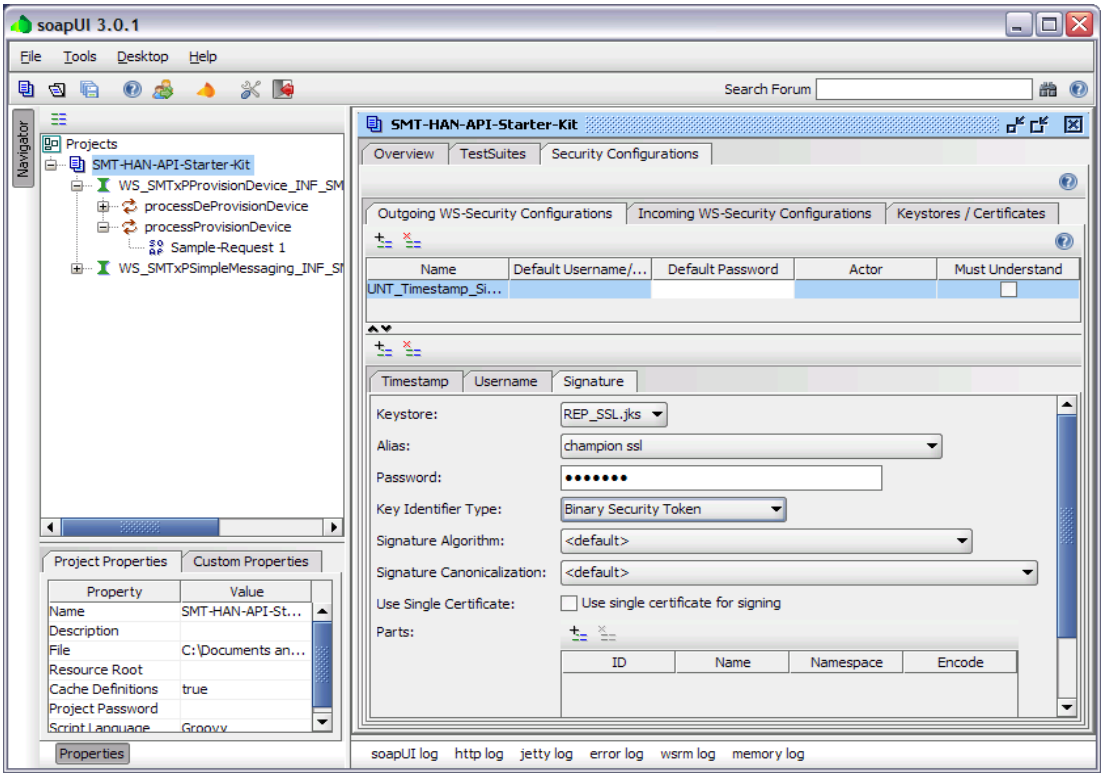
Now, select + sign at the lower half panel and specify Signature as type of entry to add.



Specify Keystore, Alias and Keystore Password.

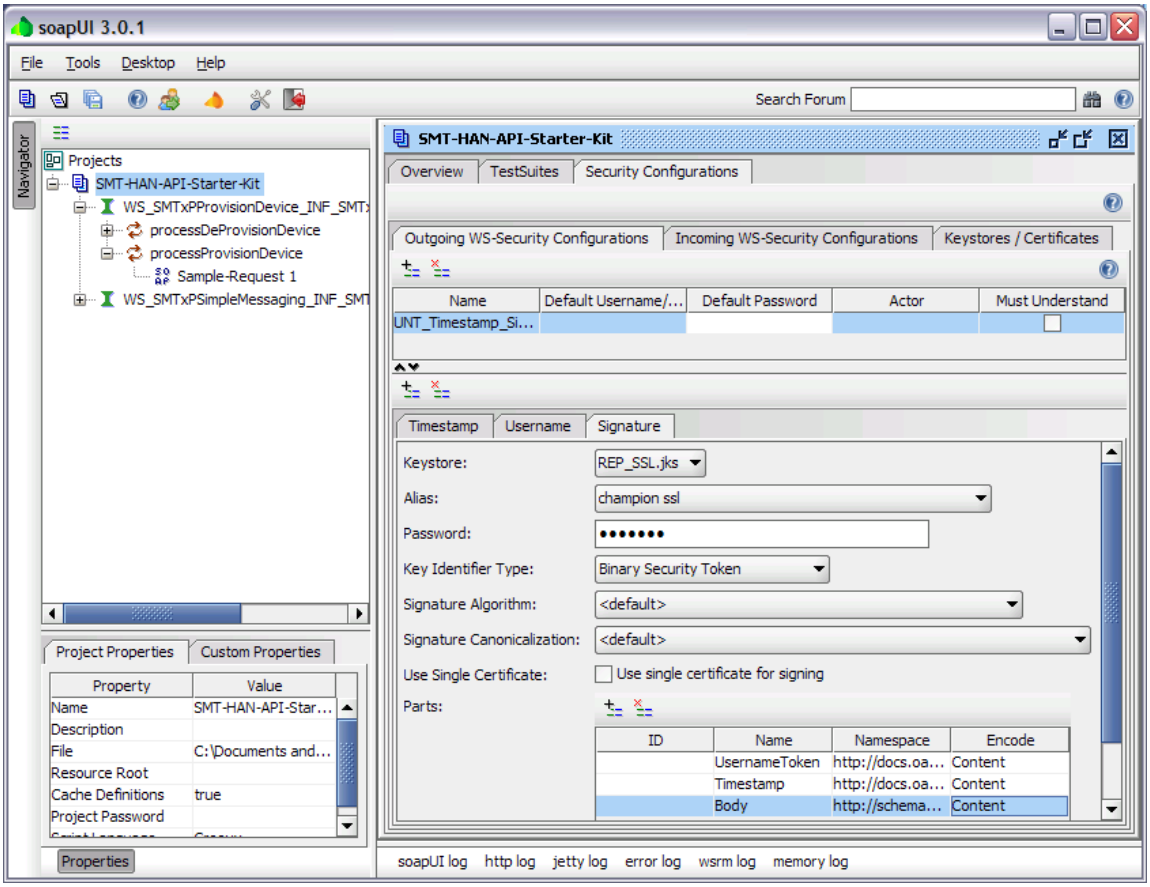


Then, select the correct Binary Security Token in Key Identifier Type field.



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 Invoking Web Service

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

6.1 URLs for invoking In-Home Device Queries

The In-Home Device Start Kit comes with Production URLs defined in the soapUI project. Users must select the correct URL when sending a request to Production

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

6.1.1 Production URLs

- Provisioning / De-provisioning

  http:// 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

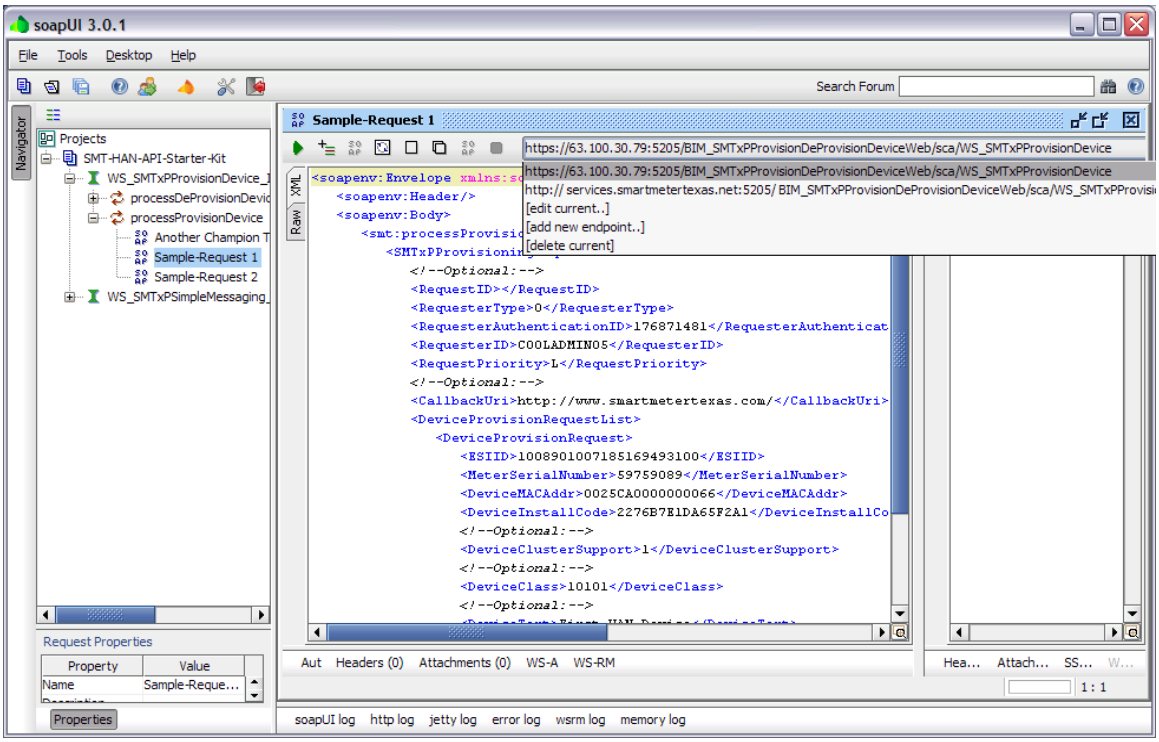
    https:// services.smartmetertexas.net:5206//BIM_SMTxPCancelAllLCEMessaging
  - Price Signal

    https:// services.smartmetertexas.net:5206/BIM_SMTxPPriceSignal

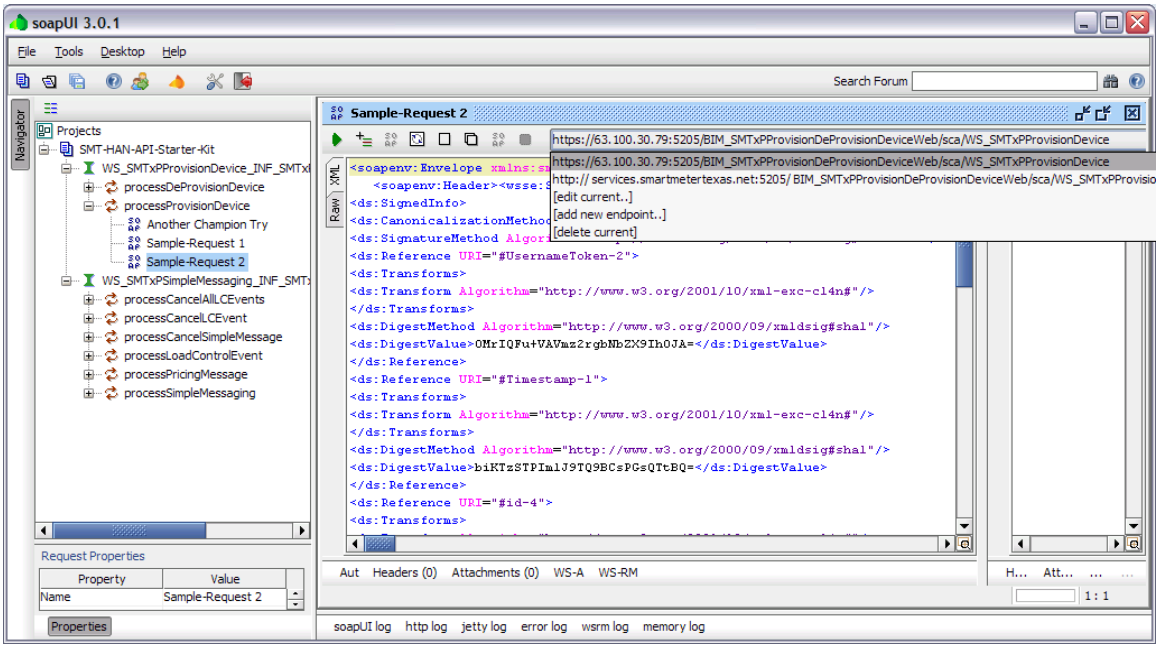
6.2 Selecting the appropriate URL when sending In-Home Device Requests

The appropriate Production URLs for In-Home Device provisioning and Smart Energy Profile (SEP) 1.0 messaging are provided in Section 6.1. This section shows how to select the correct URL from within soapUI.

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.



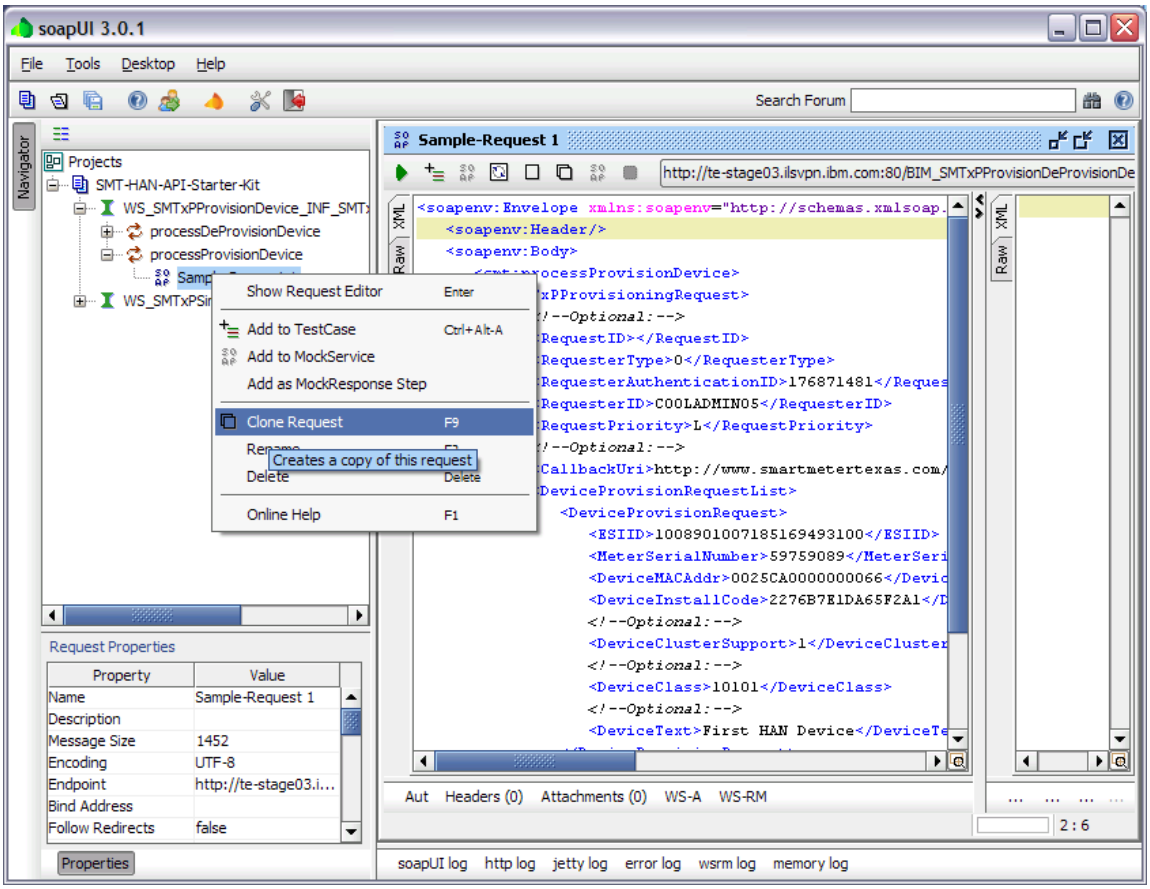
NOTE: A total of 12 endpoints have been defined in the soapUI project for Smart Energy Profile 1.0 messaging. User should check the current endpoint before submitting requests to make sure the correct endpoint is selected. The correct endpoint must match the preferred environment and SEP message type.



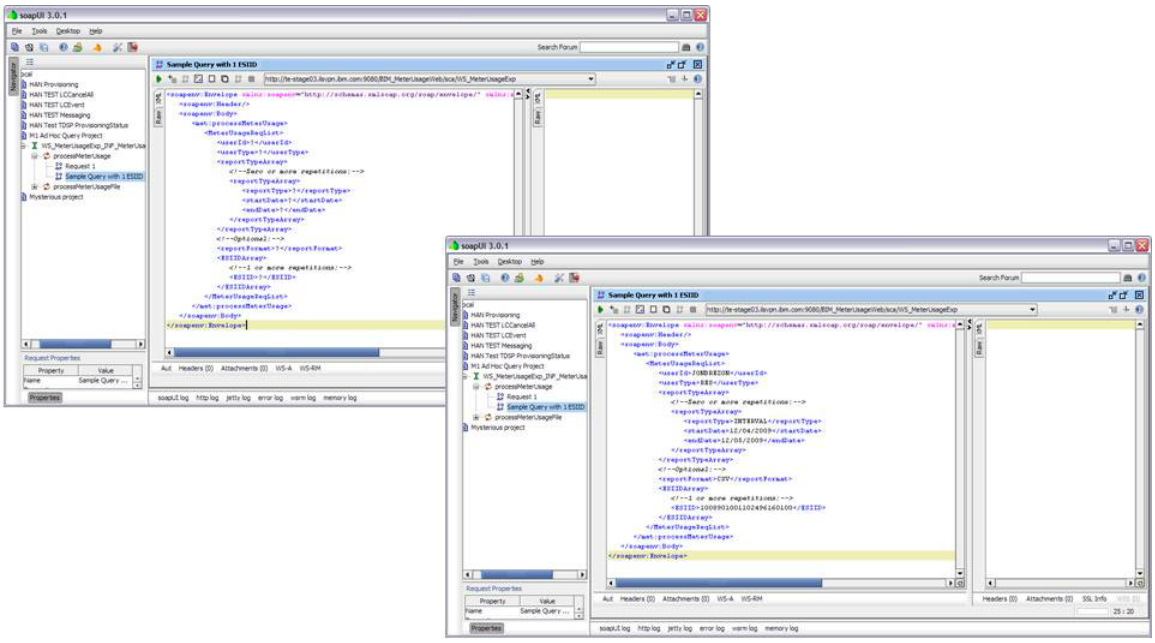
6.3 Applying a Web Services Signature to an Outgoing Request

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, selects the Clone Request option, and rename the request as depicted below.



Next, enter the appropriate API data in the request by consulting the API document provided with the Starter Kit.

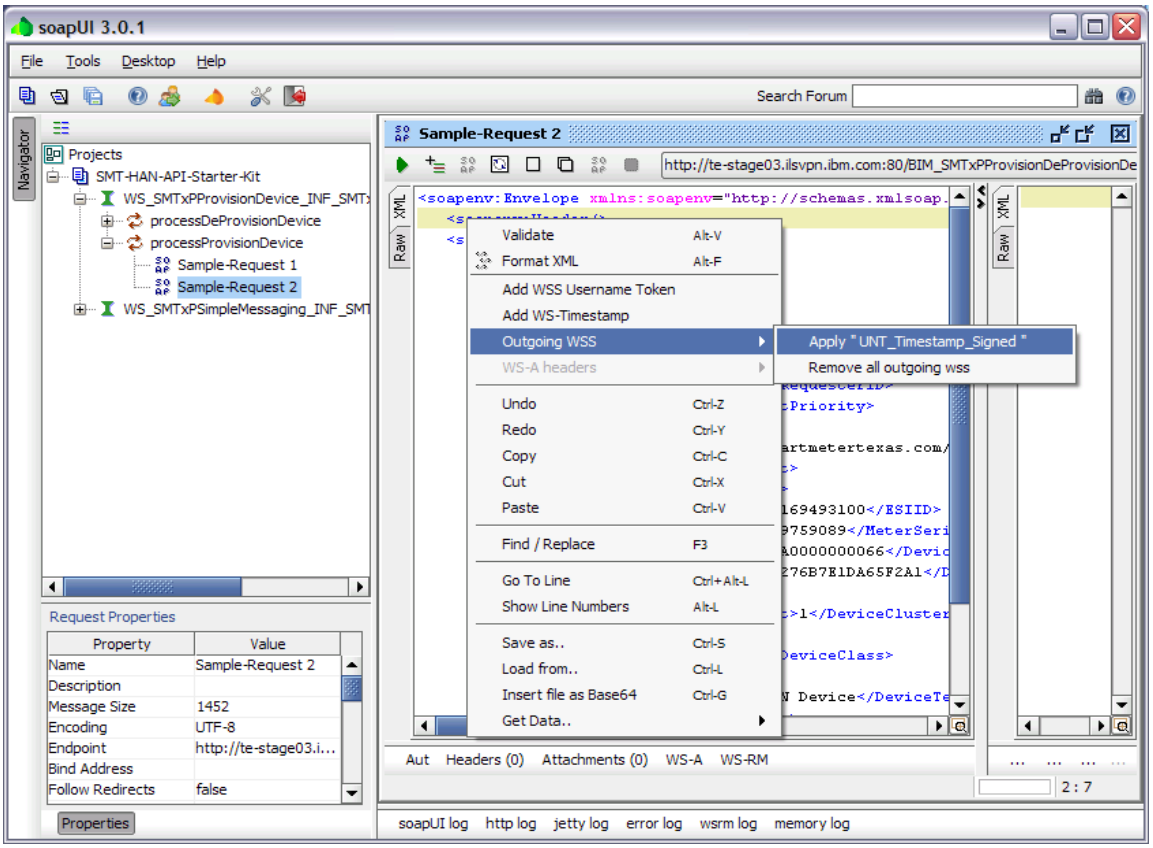


Refer to the API document that is included in this Starter Kit. An example SOAP request appears below.

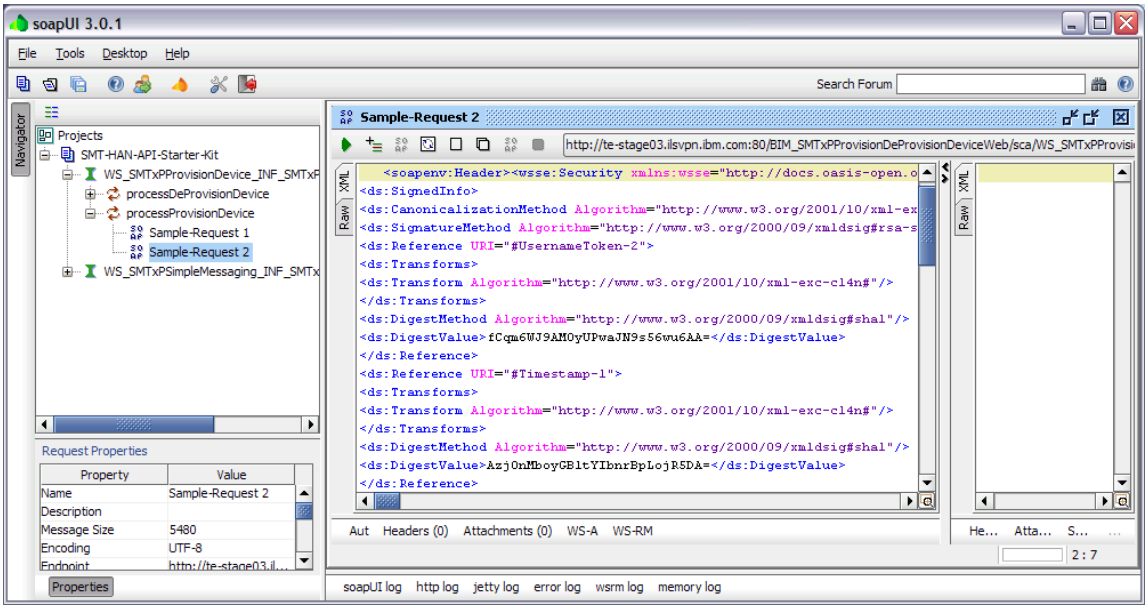
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://schemas.esb.ams.com/smtxpprovisiondevice">
  <soapenv:Header/>
  <soapenv:Body>
    <smt:processProvisionDevice>
      <SMTxPProvisioningRequest>
        <!--Optional:-->
        <RequestID></RequestID>
        <RequesterType>3</RequesterType>
        <RequesterAuthenticationID>176871481</RequesterAuthenticationID>
        <RequesterID>COOLADMIN05</RequesterID>
        <RequestPriority>L</RequestPriority>
        <!--Optional:-->
        <CallbackUri>http://www.smartmetertexas.com/</CallbackUri>
        <DeviceProvisionRequestList>
          <DeviceProvisionRequest>
            <ESIID>1008901007185169493100</ESIID>
            <MeterSerialNumber>59759089</MeterSerialNumber>
            <DeviceMACAddr>0025CA0000000066</DeviceMACAddr>
            <DeviceInstallCode>2276B7E1DA65F2A1</DeviceInstallCode>
            <!--Optional:-->
            <DeviceClusterSupport>1</DeviceClusterSupport>
            <!--Optional:-->
            <DeviceClass>10101</DeviceClass>
            <!--Optional:-->
            <DeviceText>First In-Home Device 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.



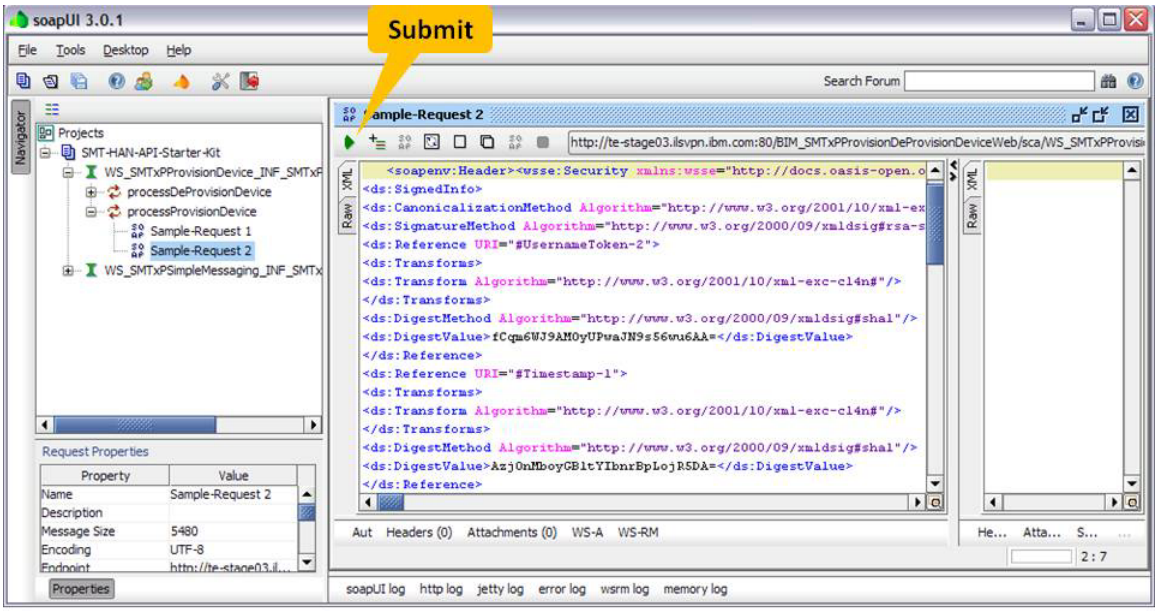
The last step signs the message as pictured below.



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.



7 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.

- Check if you can ping the SMT Server 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 from the machine where the SOAPUI client is running?
  If telnet succeeds, it means you are able to communicate to the server using port.
  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 using information provided in Sections 6.1 and 6.2.

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.