Author: Suresh Palanisamy

Date: 22-02-2017

Email: [suresh.p.apl@gmail.com](mailto:suresh.p.apl@gmail.com)

# WS – Security | SOAP Message Element Level Encryption

This document covers the HTTPs transport level security and WS-Security with Message Element level Encryption for the SOAP Message

# SSL Certificate Creation:

1. Open cmd prompt
2. Navigate to Java Keytool

<Java Home Dir>/<Jre Dir>/bin

1. Execute the below commands based on the requirement.

keytool -genkey -keyalg RSA -alias keystoreclient -keystore keystoreclient.jks -storepass manage -validity 365 -keysize 2048

keytool -genkey -keyalg RSA -alias keystoreserver -keystore keystoreserver.jks -storepass manage -validity 365 -keysize 2048

copy keystoreserver.jks truststore.jks

keytool -export -keystore keystoreclient.jks -alias keystoreclient -file client.cer

keytool -importcert -file client.cer -keystore truststore.jks -alias keystoreclient

keytool -export -keystore keystoreserver.jks -alias keystoreserver -file server.cer

keytool -list -keystore keystoreclient.jks

keytool -list -keystore keystoreserver.jks

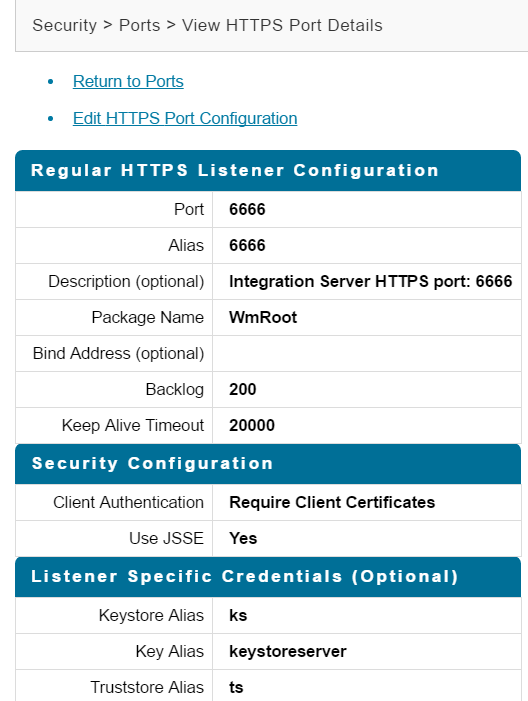
keytool -list -keystore truststore.jks

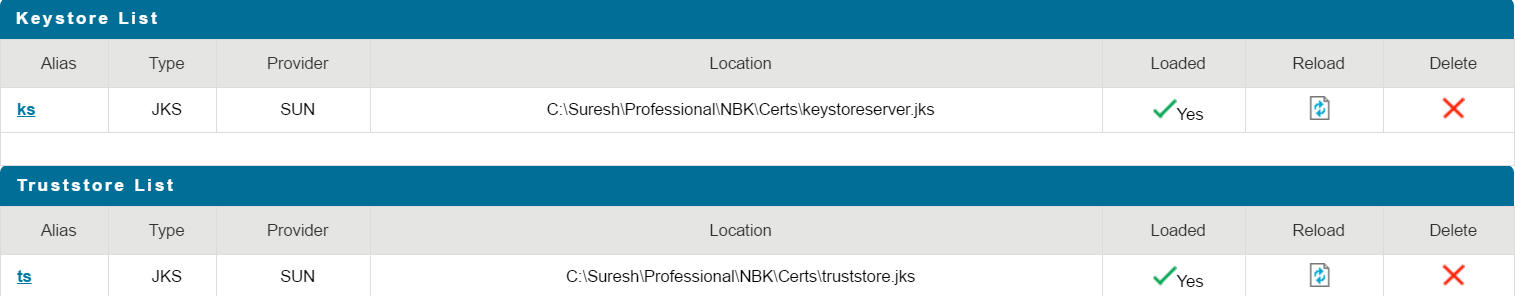
Note : Use client.cer & keystoreclient.jks as client certificate & client keystore respectively

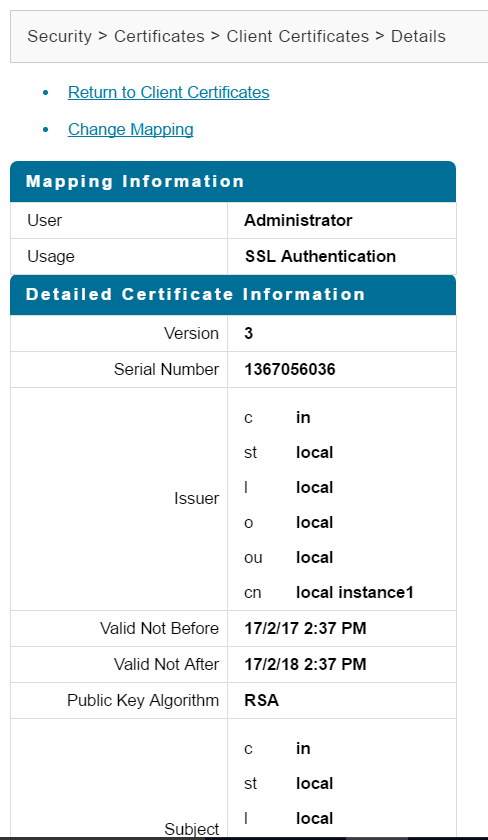
Use server.cer & keystoreserver.jks as server certificate & server keystore respectively

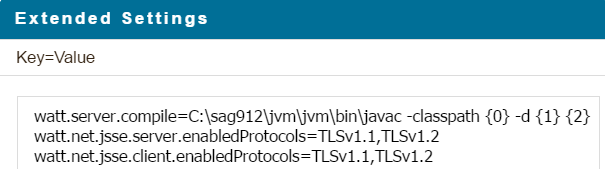
User truststore.jks as truststore

## Provider IS side configurations



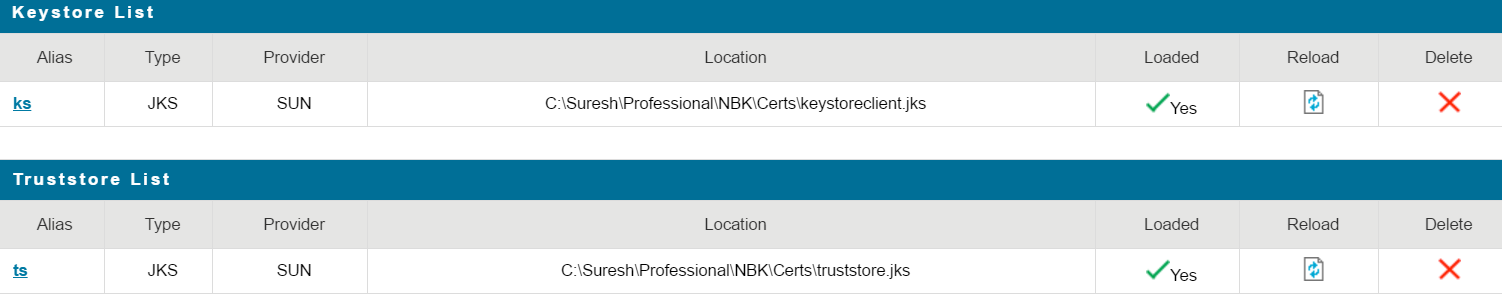




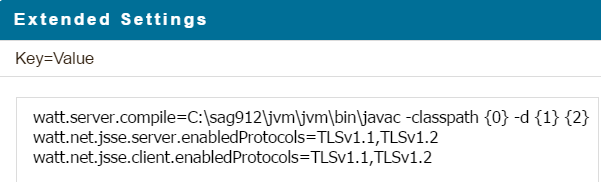


This setting is for JSSE/TLS enablement

## Consumer IS side configurations

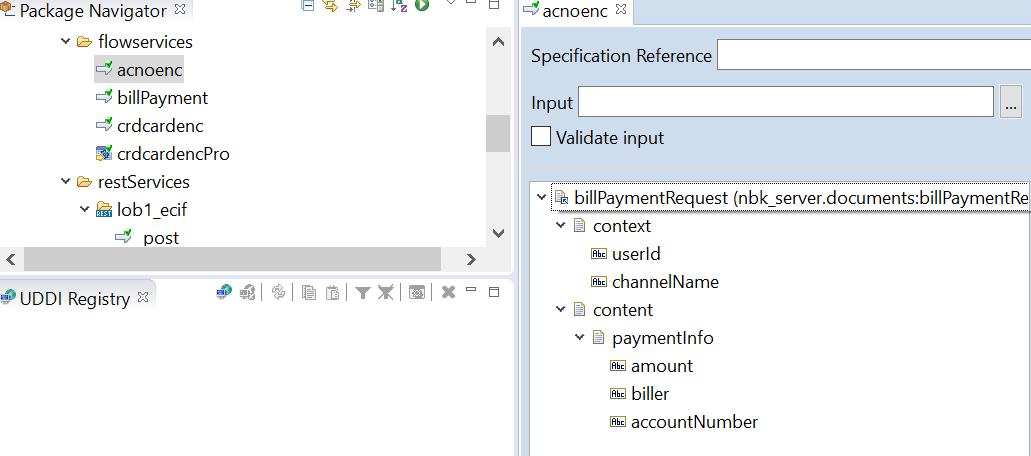




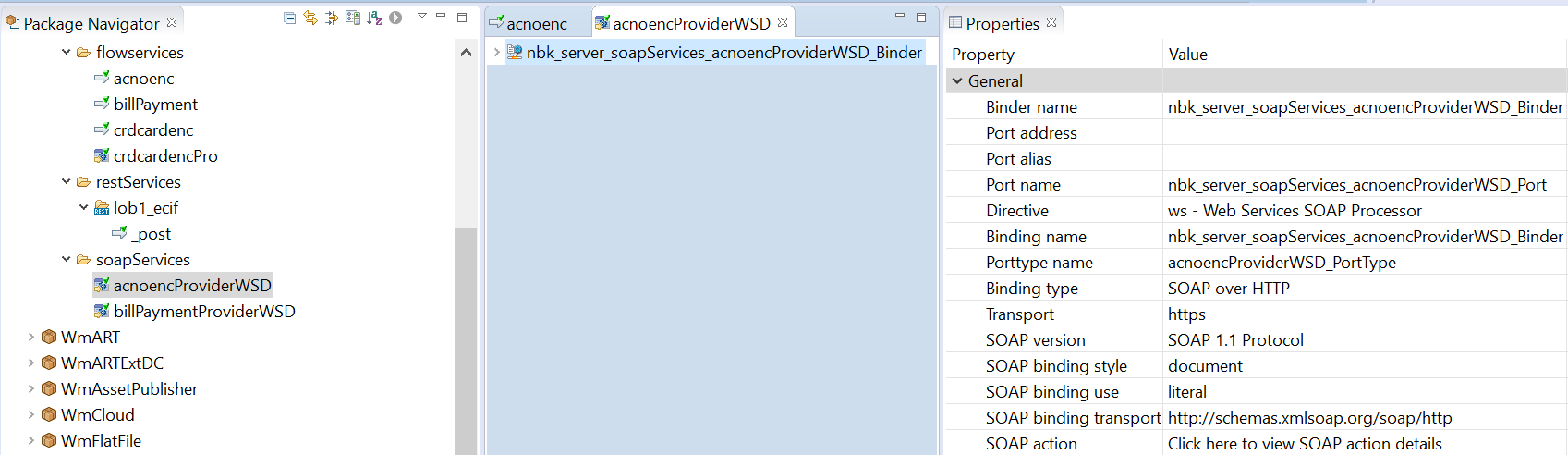


Now, Assume you have a service as below where you want need to encrypt only the accountNumber

Note : for Encryption , SSL key configuration alone is sufficient .



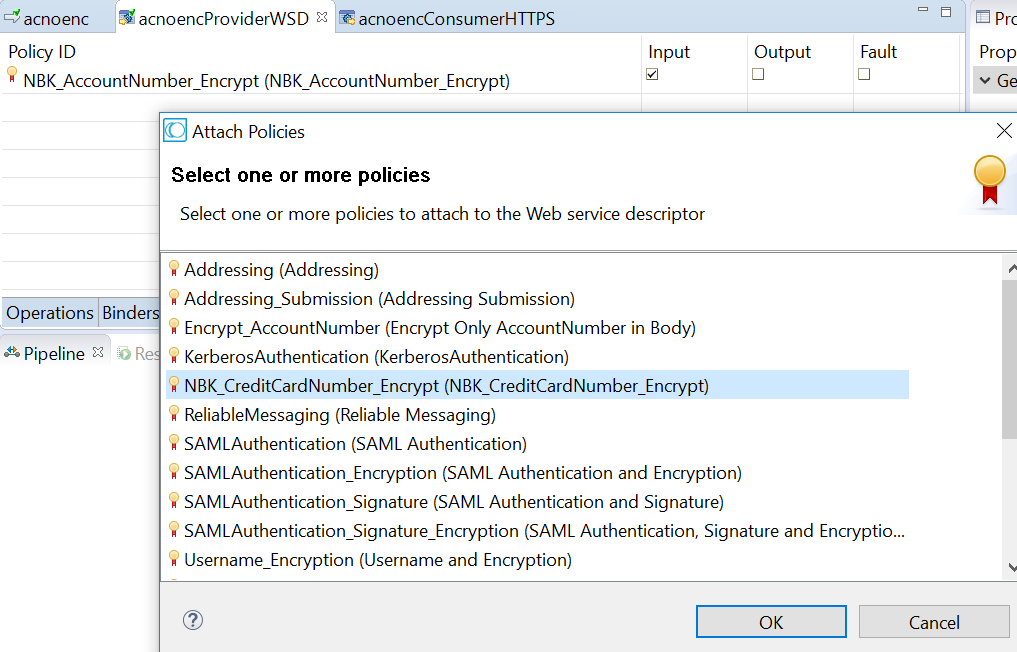
Go ahead and create Provider WSD as below



Now, we need to attache the Custom Policy file to the WSD



Don’t ask me how I created this policy file… I broke my head for 3 days to find out this … and that is WS-Security madness 😊



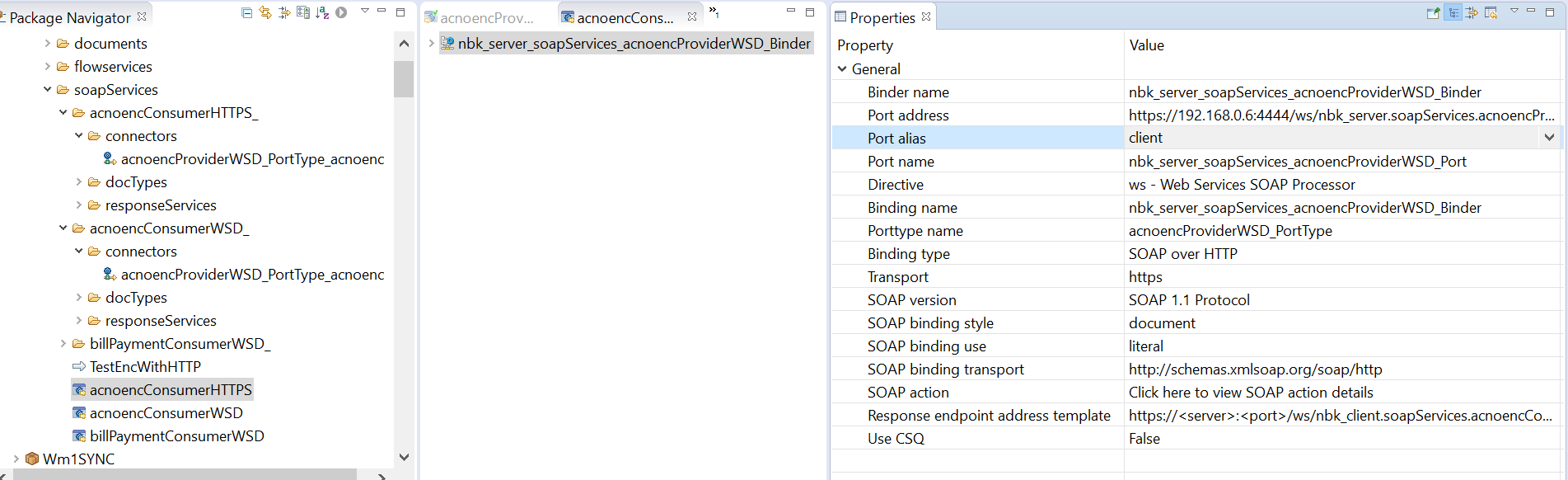
The important part of custom policy file is as below



Where the XPATH for the field accountNumber is provided

**Now at Consumer Side :**

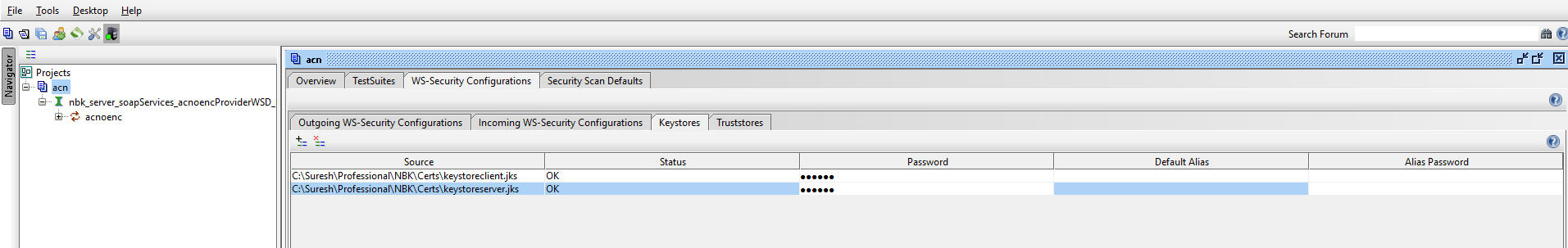
Copy the Provider WSDL url and create a Consumer WSD

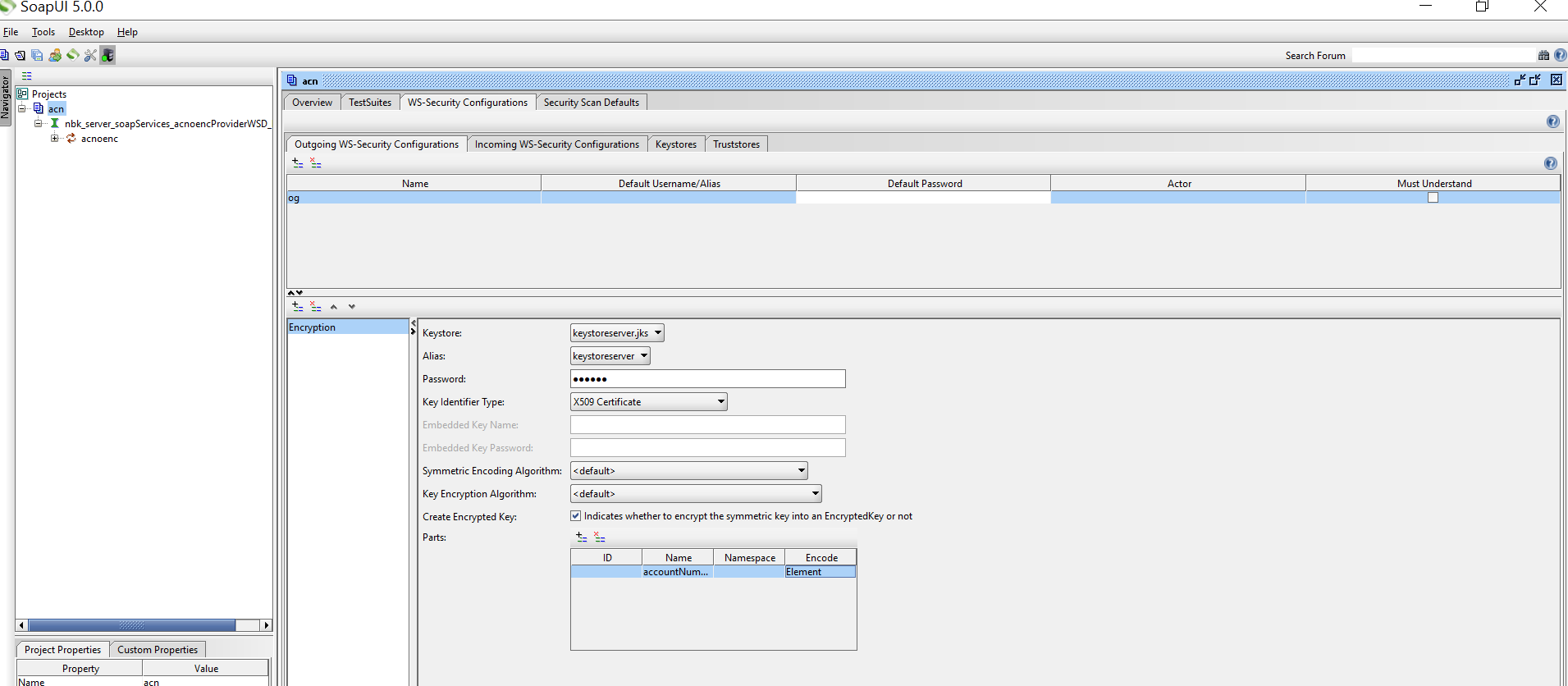


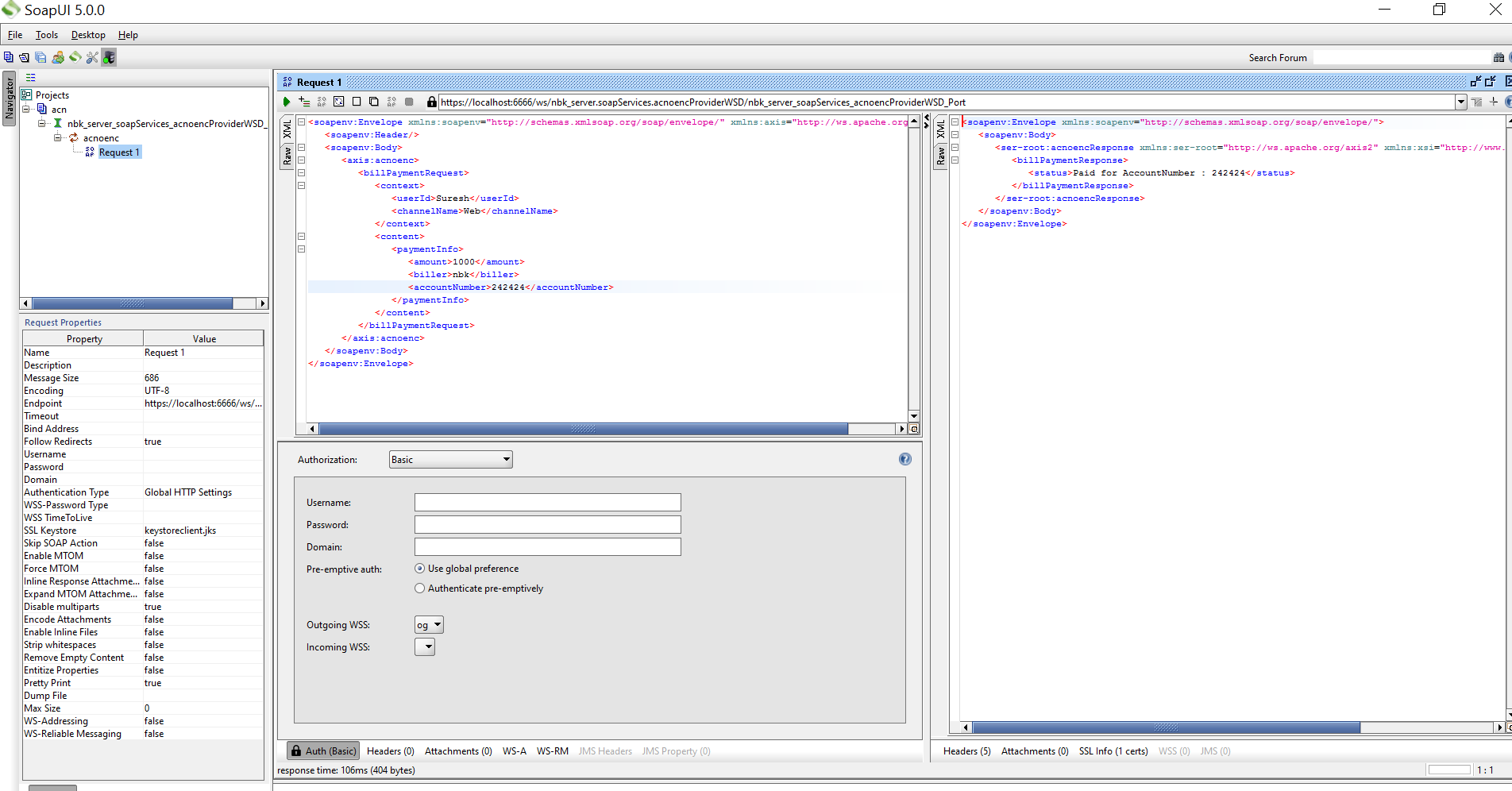
Execute the connector and check for result …

You can also Test the same in SOAP UI

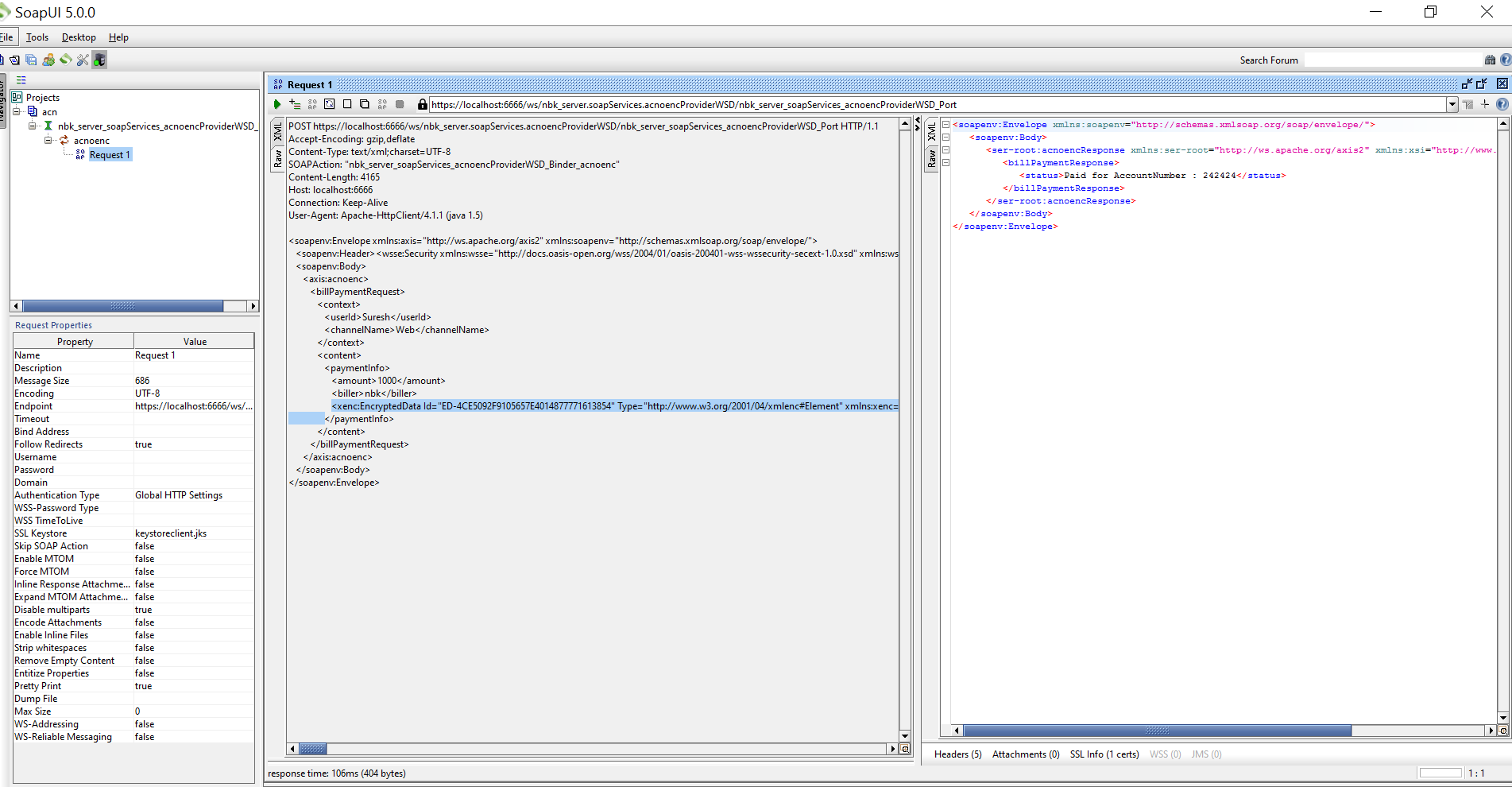
Create a soap project using the wsdl and configure as below







See below soap request, only AccountNumber is encrypted … I have not configured any policy for Response so you will see plain text..

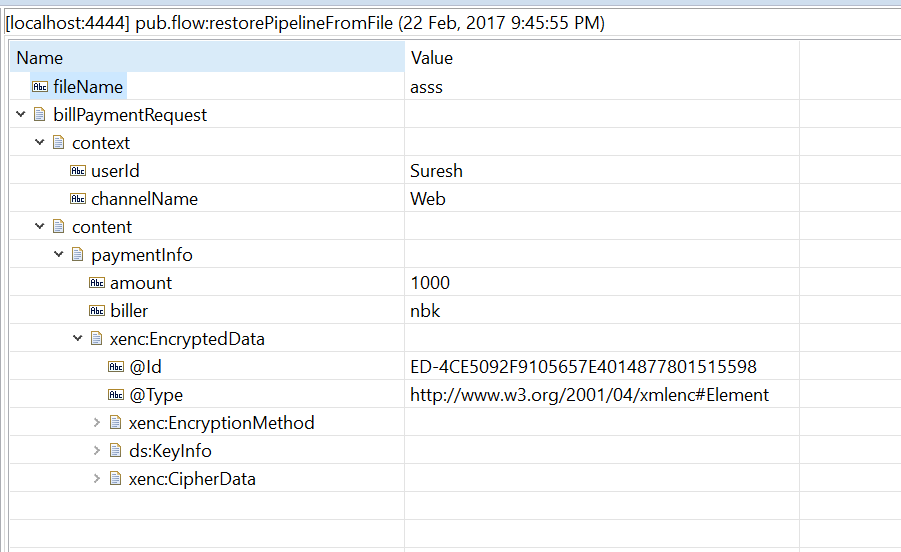


Now, you can test the same by removing the Policy file at Consumer WSD …

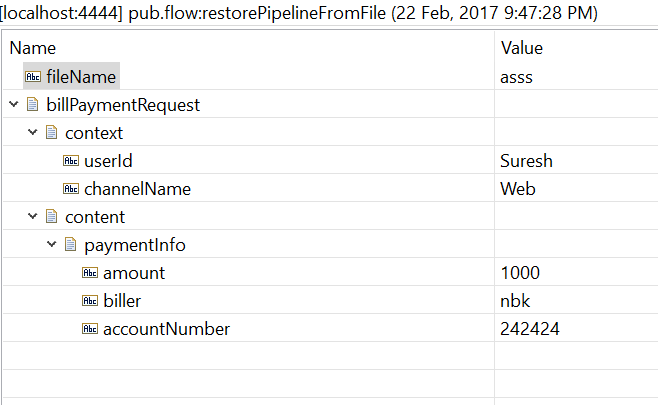
Keep a savepipline step in provider flow service to see how you get the request .

This is to ensure that the policy file has effect …

When policy file is removed in ProviderWSD , the request pipeline to the provider service looks like below

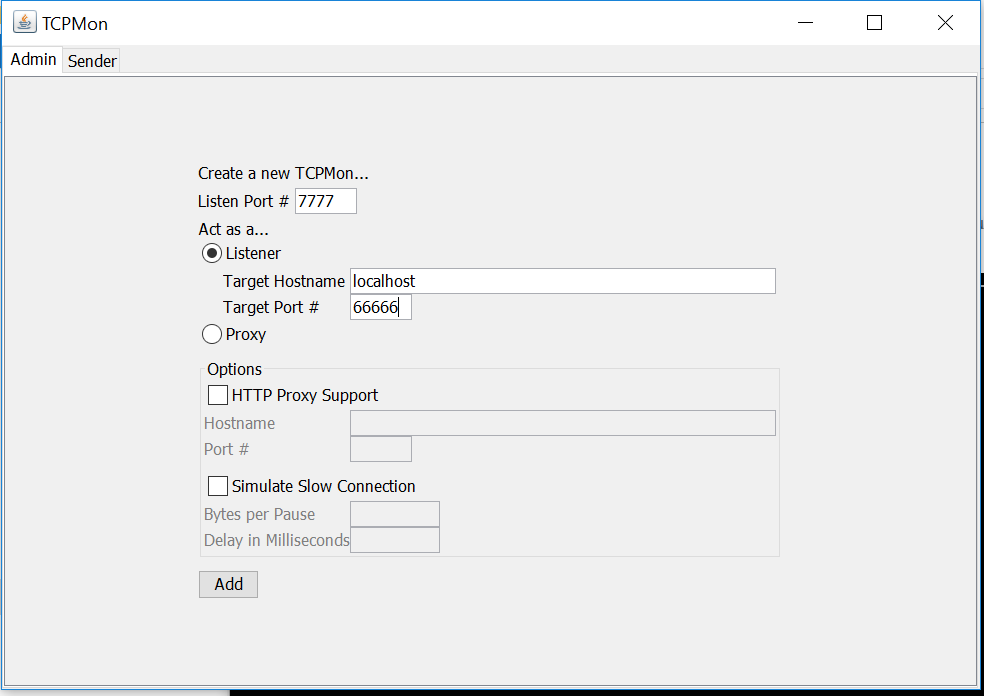


When policy file added then it appears below

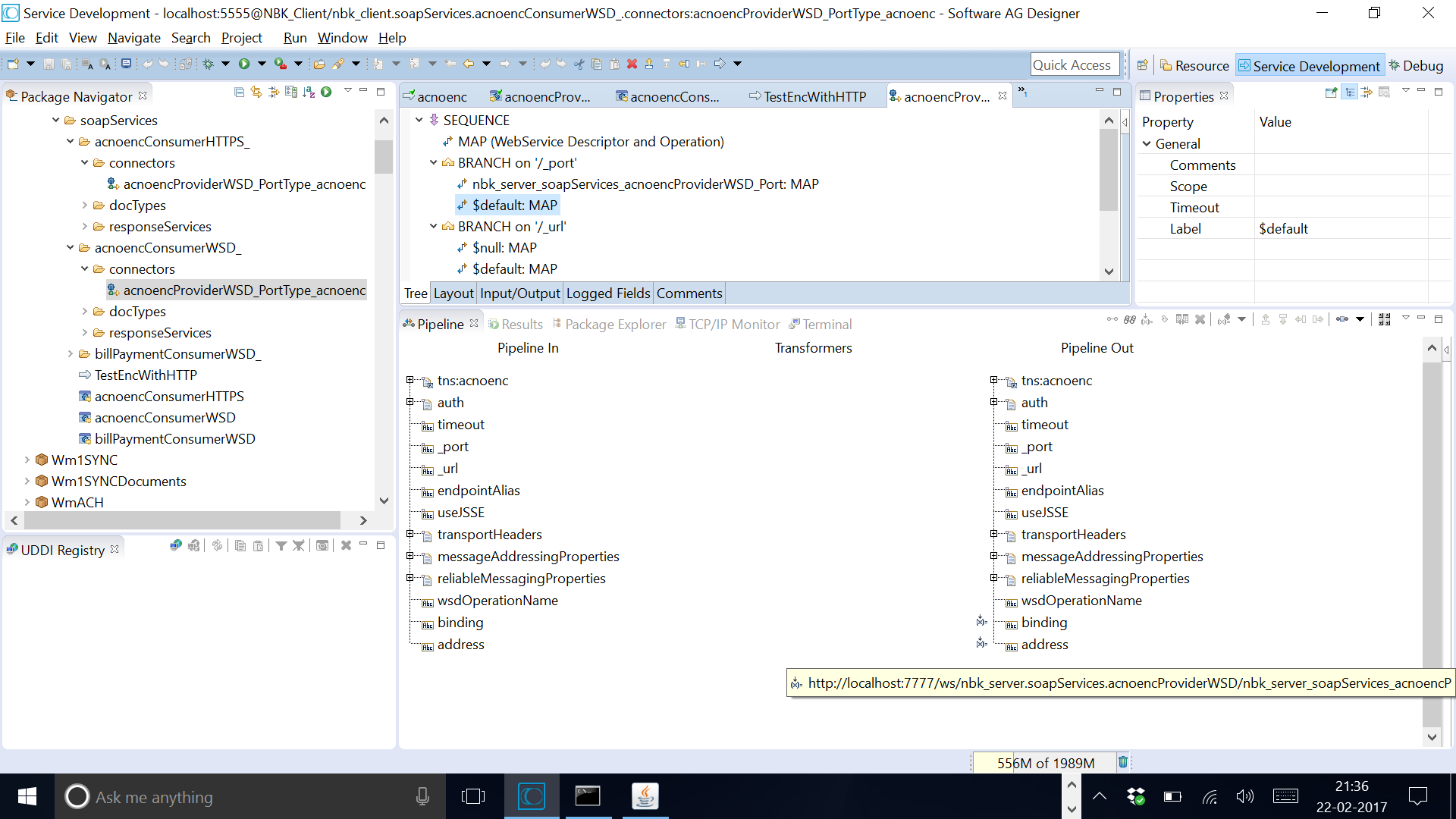


To Test and see how the Request lookslike when you run the connector from Designer/IS ,

You can launch tcpmonitor as below …



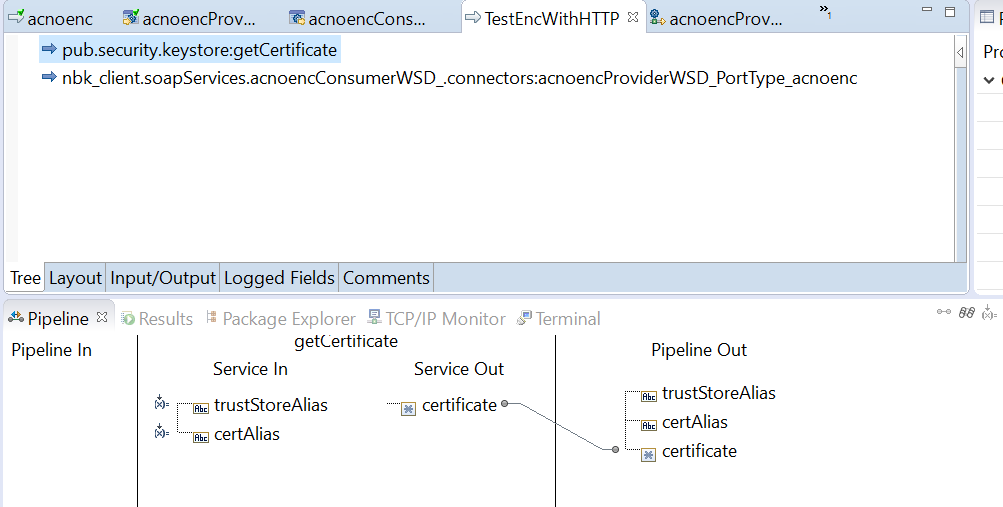
Now in the connector url , change the protocol to http and port to 7777 (tcpmon) port as below



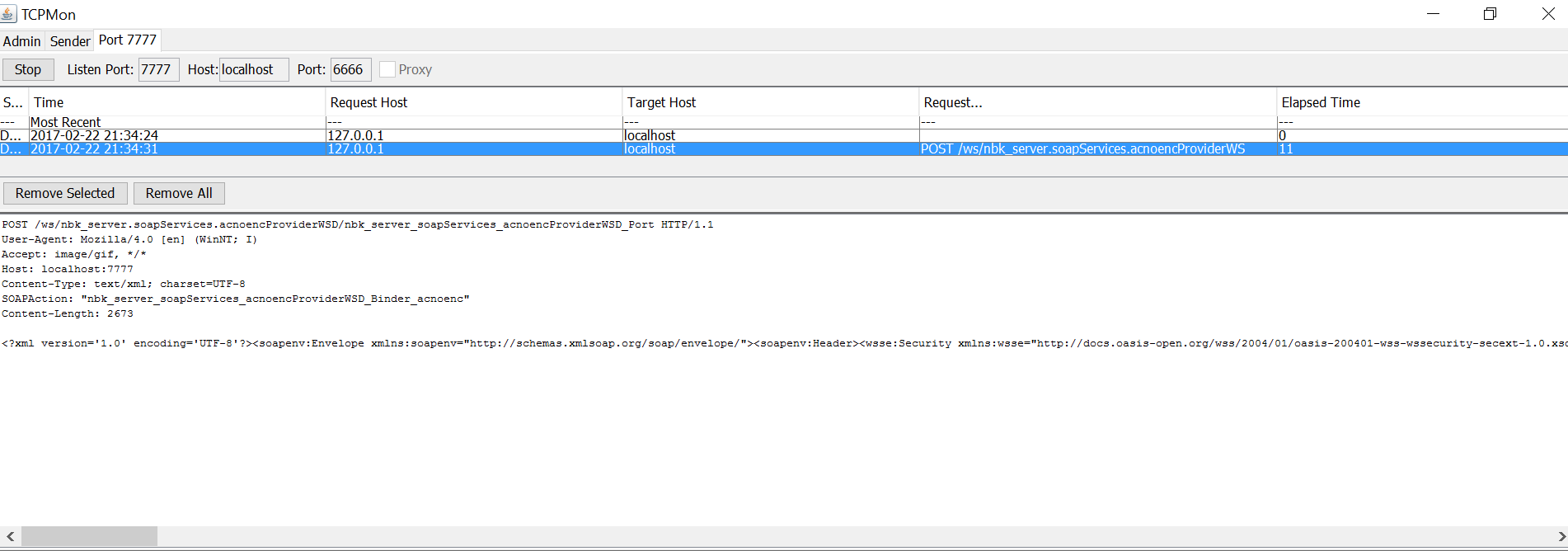
Sometimes, you may need to change the transport in the provider wsd to http from https and then use the wsdl to create a providerWSD so the Transport becomes http on the Consumer side too …( This is only to Test and see how the Request is formed and sent to the Provider service )

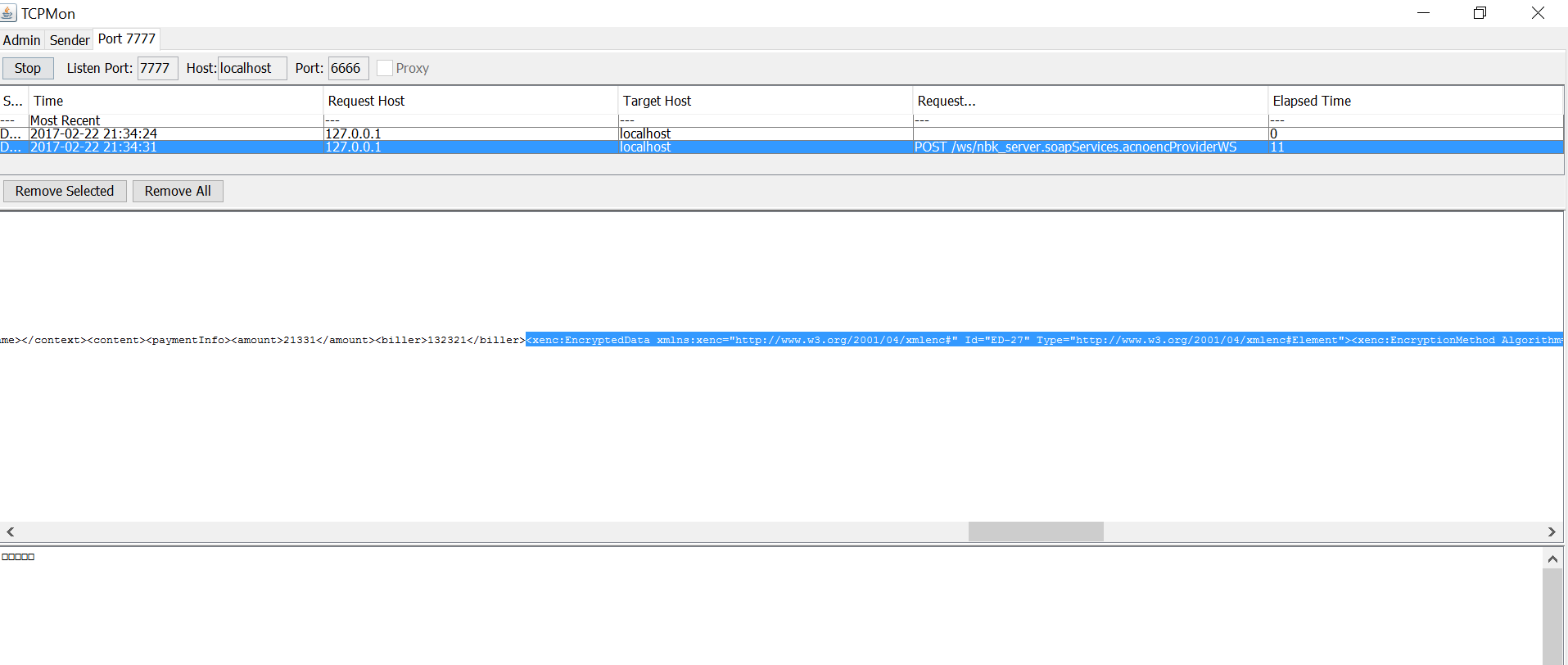
You can not the see the request in tcpmon if you use https protocol …

Create a wrapper service to pass the partner cert for encryption purpose by IS as below and invoke the connector



The service will error but you can see the request as below in tcpmon console



The accountNumber is encrypted as below 

This concludes that the AccountNumber in the soap message body is encrypted in the request by the consumer and the same is decrypted by provider ….

Hope this is useful!!! 😊 Sorry for my limited texts … was bit lazy to document the whole concept …