NAADS DSS web service usage

Contents

NAADS DSS Service

NAADS DSS web service presentation

NAADS DSS web service provides the third party with the option to verify the NAADS signature of the alerts issued through NAADS. NAADS DSS web service is a digital signing service that was developed according to the OASIS DSS standards for digital signature. http://docs.oasis-open.org/dss/v1.0/oasisdss-core-spec-v1.0-os.html

NAADS DSS is SOAP on HTTPS service that is located at the following URLs:

- https://dss1.naad-adna.pelmorex.com/
- https://dss2.naad-adna.pelmorex.com/

NAADS DSS verification request

A NAADS DSS verification request for alert signature verification is a DSS request enveloped into a SOAP message sent through HTTPS to one of the URLs mentioned above. These URLs are specified in the alert's NAADS signature under the *SignatureProperty* tag.

The DSS verification request should have the following structure:

```
<VerifyRequest RequestID="UNIQUE IDENTIFIER"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.docs.oasis-
open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd" Profile="REQUEST ISSUER">
        <InputDocuments>
                <Document ID="ALERT ID">
                        <!-- dss:Base64XML/ this is default, not required to specify.
                        We will add the signed alert here. -->
                </Document>
        </InputDocuments>
        <OptionalInputs>
                <SignaturePlacement WhichDocument="ALERT ID"
CreateEnvelopedSignature="true"/>
        </OptionalInputs>
        <SignatureObject>
                <SignaturePtr WhichDocument="ALERT ID"
                        XPath="//cs:Signature[Id = &amp;quot;NAADS Signature&amp;quot;]" />
        </SignatureObject>
</VerifyRequest>
```

The *VerifyRequest* element is the OASIS DSS standard request for the signature verification. NAADS DSS will read the *RequestID* attribute to identify the verification request received and the *Profile* attribute to identify the request issuer. These values will be returned in the verification response.

The *InputDocuments* element encloses the documents submitted for verification. Currently NAADS DSS can process only one document per request.

The *Document* element contains the signed alert submitted for verification. The *ID* attribute of the element will identify the document submitted for verification, identification that will be used later in the verification request.

The *SignaturePlacement* element inside the *OptionalInputs* element will specify the type of signature (enveloped or enveloping) through the *CreateEnvelopedSignature* attribute. The *WhichDocument* attribute will identify the document in the InputDocuments element. Currently NAADS DSS is processing only enveloped signatures.

The *XPath* attribute of the SignaturePtr element inside the SignatureObject object provides the path to the signature inside the signed alert, *XPath="//cs:Signature[Id = "NAADS Signature"]"*. The *WhichDocument* attribute will identify the signed alert in the InputDocuments element.

NAADS DSS verification response

A NAADS DSS verification response for alert signature verification is DSS response to the DSS a request, as presented above, enveloped into a SOAP message received through HTTPS.

The DSS verification response should have the following structure:

```
<dss:VerifyResponse RequestID="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:dss="http://www.docs.oasisopen.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd" Profile="">
        <Result>
                <ResultMajor/>
                <ResultMinor/>
                <ResultMessage/>
        </Result>
</dss:VerifyResponse>
```

The *VerifyResponse* element is the OASIS DSS standard response to a signature verification request. NAADS DSS will write into the *RequestID* attribute the identity of the verification request received and into the Profile attribute to identify the request issuer.

The *Result* element provides the signature verification result in three items: *ResultMajor*, *ResultMinor* and *ResultMessage*. The *ResultMajor* element provides the generic information on the result: success or error, in an OASIS DSS standard string format. The *ResultMinor* element provides more detailed information in case the verification failed, in an OASIS DSS standard string format. *ResultMessage* provides details string with logging information on why the verification failed.

Currently NAADS DSS has two result values for the *ResultMajor* and *ResultMinor*.

For successful verification:

```
<VerifyResponse RequestID=" " Profile="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://www.docs.oasisopen.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd">
 <Result>
  <ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</ResultMajor>
  <ResultMinor />
  <ResultMessage />
 </Result>
</VerifyResponse>
```

For error on verification:

```
<VerifyResponse RequestID=" " Profile="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://www.docs.oasisopen.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd">
 <Result>
```

```
  <ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError</ResultMajor>
  <ResultMinor>urn:oasis:names:tc:dss:1.0:resultminor:GeneralError</ResultMinor>
  <ResultMessage />
 </Result>
</VerifyResponse>
```

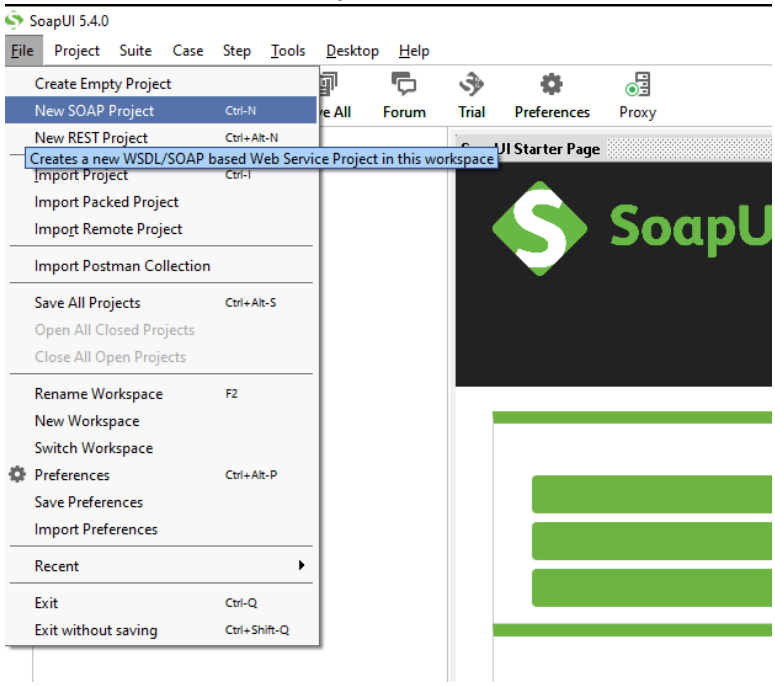
Verify alerts on NAADS DSS web service using SoapUI

SoapUI

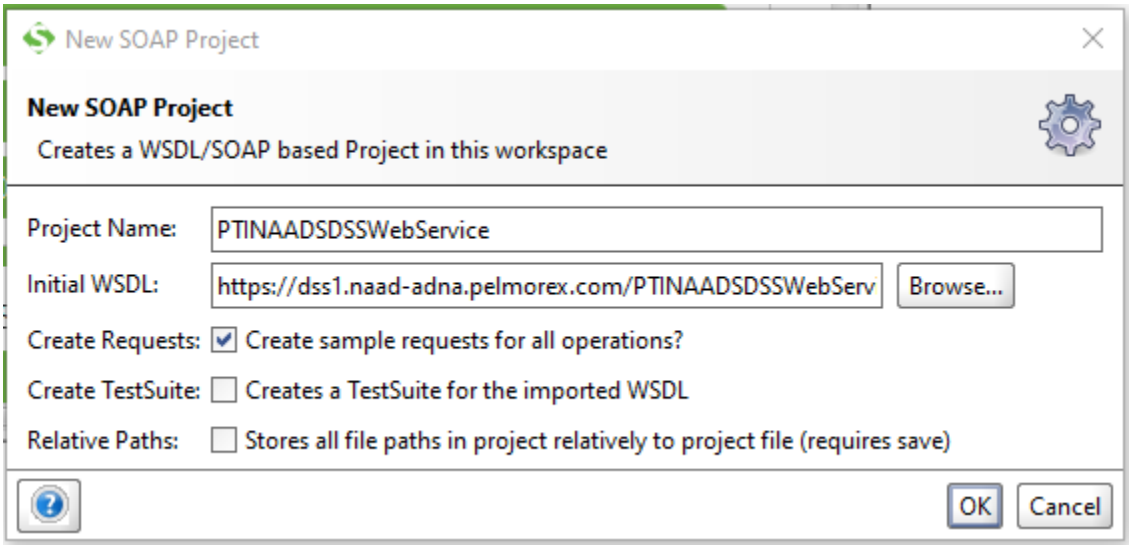
SoapUI is a Functional Testing tool for SOAP and REST testing. As a SOAP client, it allows you to easily and rapidly send transactions through HTTP and HTTPS.
SoapUI is available as a free open-source version. For more information follow the link below:
https://www.soapui.org/downloads/soapui.html

Create the SOAP request

In the SoapUI "File" menu select *"New SOAP Project"*

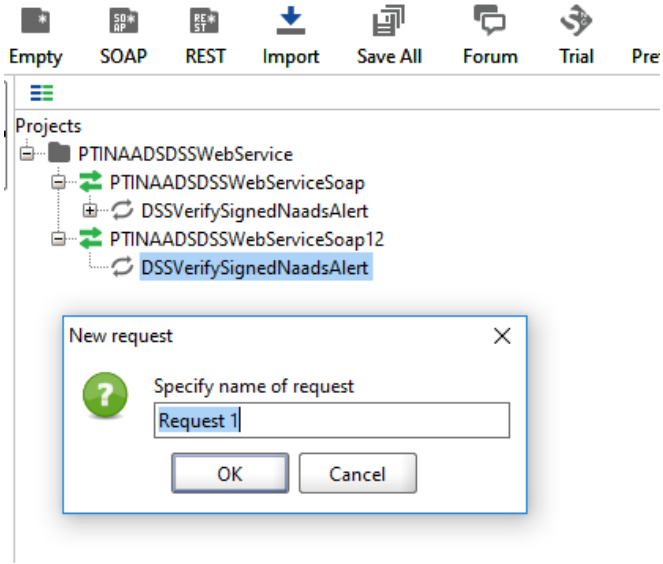


The dialog below will pop-up. In the edit box type the path to the WSDL file of the NAADS DSS web service, i.e. https://dss1.naad-adna.pelmorex.com/PTINAADSDSSWebService.asmx?WSDL

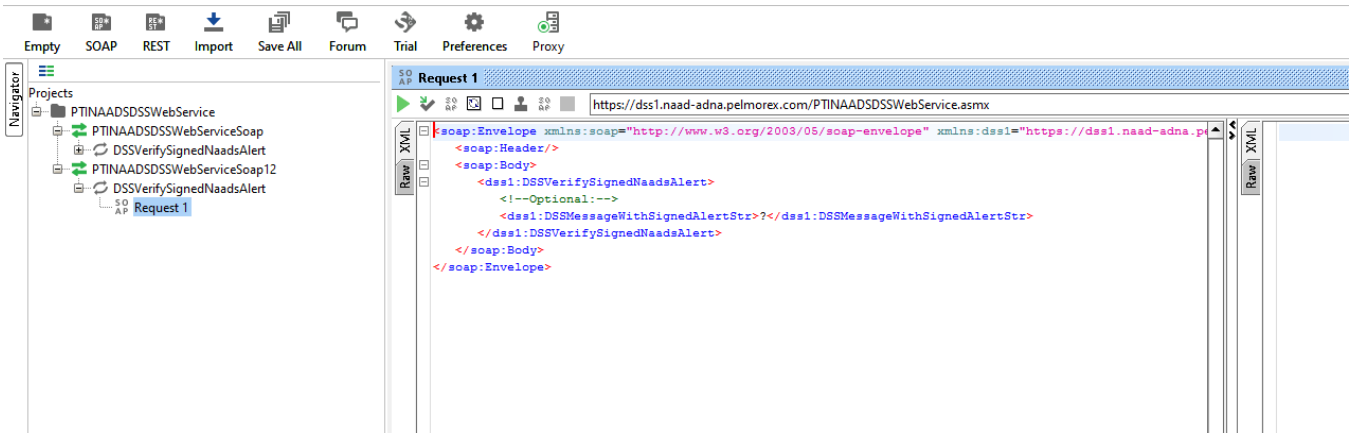


In the Navigator (left panel), expand the “PTINAADSDSSWebService” –> “PTINAADSDSSWebService12” section:

Right-click on the “DSSVerifySignedNaadsAlert” and select “New Request” operation from the following dialog:



The following SOAP envelope will be created.



The String value of the *DSSMessageWithSignedAlertStr* parameter must be replaced with the DSS verification request in UTF-8 format.

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:dss1="https://dss1.naad-adna.pelmorex.com/">
  <soap:Header/>
  <soap:Body>
    <dss1:DSSVerifySignedNaadsAlert>
      <!--Optional:-->
      <dss1:DSSMessageWithSignedAlertStr>?</dss1:DSSMessageWithSignedAlertStr>
    </dss1:DSSVerifySignedNaadsAlert>
  </soap:Body>
</soap:Envelope>
```

Prepare the DSS verification request

1. Get the signed alert to be verified from http://rss.naad-adna.pelmorex.com/. The alert will have a xml CAP format like the one below.

```
<?xml version="1.0" encoding="UTF-8"?>
<alert>
 <identifier>19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70</identifier>
 <sender>Pelmotest</sender>
 <sent>2018-11-28T10:38:24-04:00</sent>
 <status>Actual</status>
 <msgType>Alert</msgType>
 <scope>Public</scope>
 <code>profile:CAP-CP:0.4</code>
 <code>layer:SOREM:1.0</code>
 <info>
  <language>en-CA</language>
  …
 </info>
 <Signature Id="NAADS Signature">
  <SignedInfo>
```

```
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <Reference URI="">
     <Transforms>
      <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     </Transforms>
     <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <DigestValue>tW1E9/TyQcZD1WVT5kykAuxKniEzg5Yn7fYBD0rHTKY=</DigestValue>
    </Reference>
   </SignedInfo>
   <SignatureValue>T4ZPcG6bguq2j4gyCrLztKsIC5f5CWfKvxexyDg ... OgJiGiTkzAVhl3A==</SignatureValue>
   <KeyInfo>
    <X509Data>
     <X509Certificate>MIIGtjCCBZ6gAw ... STl7jJ0sPtTrvz+r8X</X509Certificate>
    </X509Data>
   </KeyInfo>
   <Object>
    <SignatureProperties>
     <SignatureProperty Id="NAADS-DSS1" Target="https://dss1.naad-adna.pelmorex.com"/>
                    <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd" />
     <SignatureProperty Id="NAADS-DSS2" Target="https://dss2.naad-adna.pelmorex.com"/>
                    <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd" />
    </SignatureProperties>
   </Object>
  </Signature>
</alert>
```

2. Create the OASIS DSS standard verification request, by using the template presented in the *NAADS DSS verification request* section.

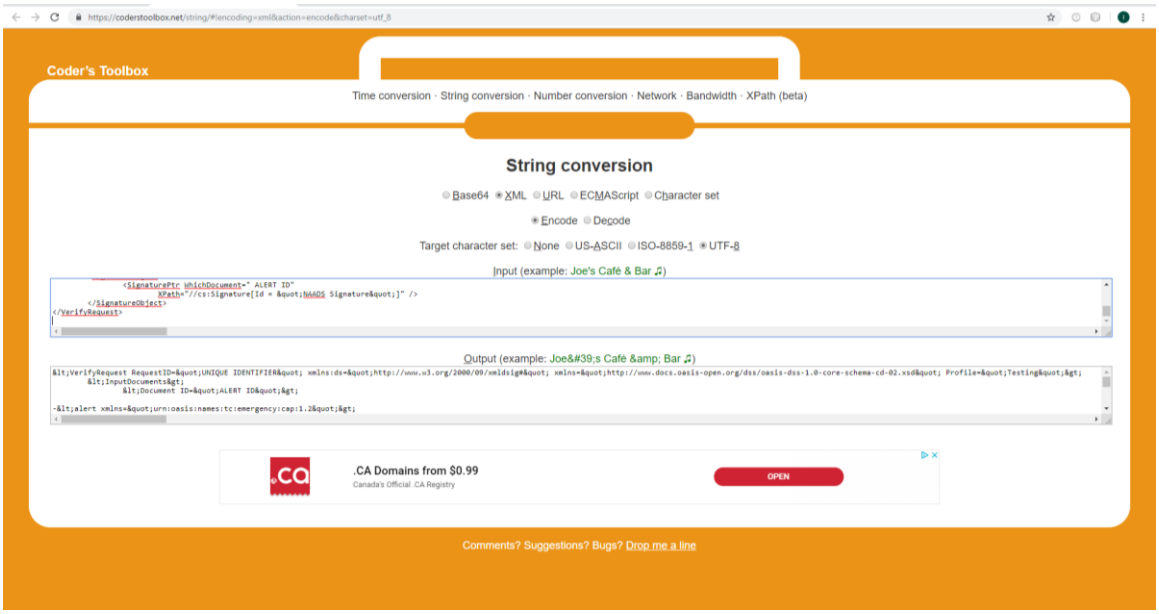
3. In the template, update text highlighted in yellow with the correct values:
   - "UNIQUE IDENTIFIER"
   - "REQUEST ISSUER"
   - "ALERT ID"

4. Copy the CAP alert **without** the first line (<?xml version="1.0" encoding="UTF-8"?>) and include the alert in the Document element.

```
<VerifyRequest RequestID="6944B0BD-F050-4B84-2E50-C3A52AA3C7CA "
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.docs.oasis-
open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd" Profile="Testing">
        <InputDocuments>
                <Document ID="19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70">
                    <alert>
                     <identifier>19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70</identifier>
                     <sender>Pelmotest</sender>
                     <sent>2018-11-28T10:38:24-04:00</sent>
                     <status>Actual</status>
                     <msgType>Alert</msgType>
                     <scope>Public</scope>
                     <code>profile:CAP-CP:0.4</code>
                     <code>layer:SOREM:1.0</code>
                     <info>
```

```
                        <language>en-CA</language>
                           …
                        </info>
                      <Signature Id="NAADS Signature">
                        <SignedInfo>
                          <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
                      20010315"/>
                          <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                          <Reference URI="">
                           <Transforms>
                                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                           </Transforms>
                           <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                           <DigestValue>tW1E9/TyQcZD1WVT5kykAuxKniEzg5Yn7fYBD0rHTKY=</DigestValue>
                          </Reference>
                        </SignedInfo>
                    <SignatureValue>T4ZPcG6bguq2j4gyCrLztKsIC5f5CWfKvxexyDg ...
                  OgJiGiTkzAVhl3A==</SignatureValue>
                    <KeyInfo>
                          <X509Data>
                                <X509Certificate>MIIGtjCCBZ6gAw ... STl7jJ0sPtTrvz+r8X</X509Certificate>
                           </X509Data>
                   </KeyInfo>
                   <Object>
                      <SignatureProperties>
                          <SignatureProperty Id="NAADS-DSS1" Target="https://dss1.naad-adna.pelmorex.com"/>
                                <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd" />
                          </SignatureProperty>
                           <SignatureProperty Id="NAADS-DSS2" Target="https://dss2.naad-adna.pelmorex.com"/>
                                <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd" />
                          </SignatureProperty>
                      </SignatureProperties>
                  </Object>
              </Signature>
            </alert>
          </Document>
            </InputDocuments>
            <OptionalInputs>
                    <SignaturePlacement WhichDocument="19ACDB8E-8F79-6725-9D6B-
1A2D95BDBD70" CreateEnvelopedSignature="true"/>
            </OptionalInputs>
            <SignatureObject>
                    <SignaturePtr WhichDocument="19ACDB8E-8F79-6725-9D6B-
1A2D95BDBD70"
                          XPath="//cs:Signature[Id = &amp;quot;NAADS Signature&amp;quot;]" />
            </SignatureObject>
</VerifyRequest>
```

5. **Encode** this new DSS verification request **from XML format to the UTF-8 format**. Below is a conversion sample using an online conversion tool:

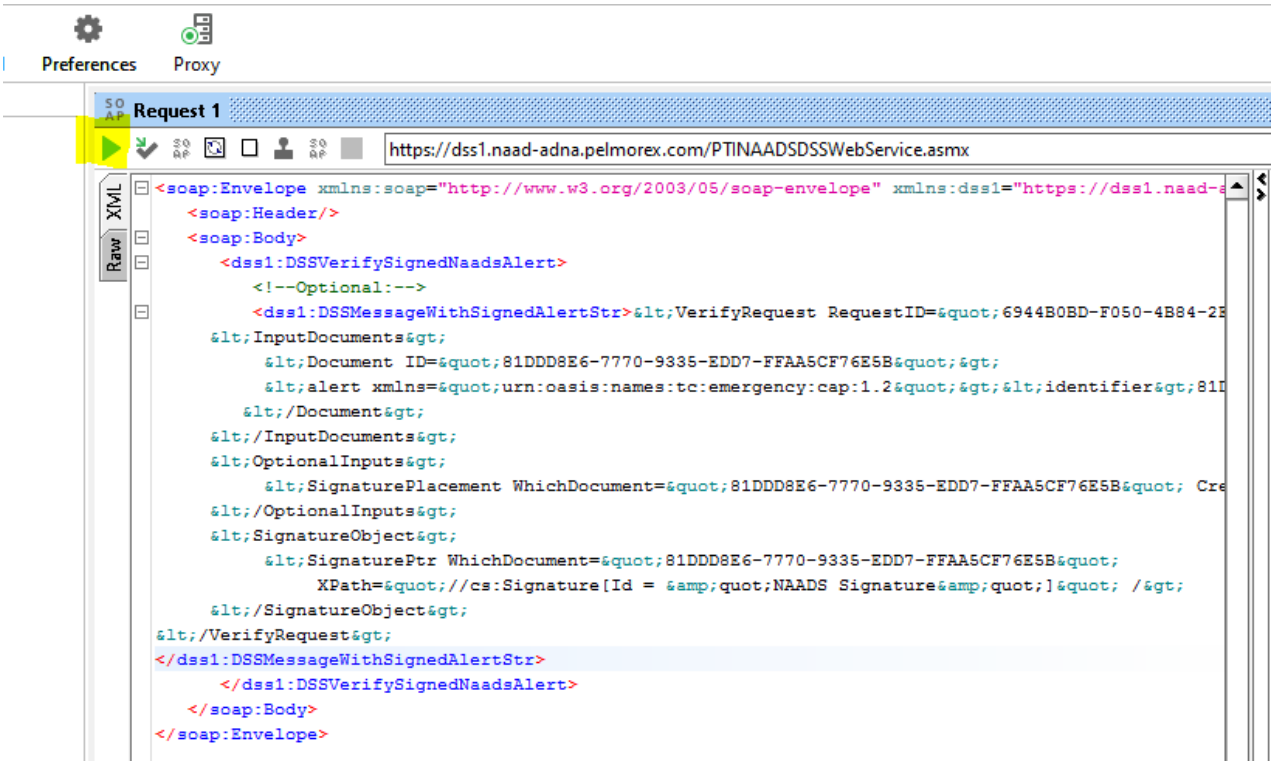


6. Copy the output and add the verification request to the SOAP envelope created by the SoapUI client (replace the question mark "?", after **<dss1:DSSMessageWithSignedAlertStr>**):

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:dss1="https://dss1.naad-adna.pelmorex.com/">
  <soap:Header/>
  <soap:Body>
    <dss1:DSSVerifySignedNaadsAlert>
      <!--Optional:-->
      <dss1:DSSMessageWithSignedAlertStr>&lt;VerifyRequest RequestID=&quot;6944B0BD-F050-4B84-2E50-C3A52AA3C7CA &quot; xmlns:ds=&quot;http://www.w3.org/2000/09/xmldsig#&quot; xmlns=&quot;http://www.docs.oasis-open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd&quot; Profile=&quot;Testing&quot;&gt;
          &lt;InputDocuments&gt;
              &lt;Document ID=&quot;19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70&quot;&gt;
&lt;alert&gt;
 &lt;identifier&gt;19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70&lt;/identifier&gt;
 &lt;sender&gt;Pelmotest&lt;/sender&gt;
 …
          &lt;OptionalInputs&gt;
              &lt;SignaturePlacement WhichDocument=&quot;19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70&quot; CreateEnvelopedSignature=&quot;true&quot;/&gt;
          &lt;/OptionalInputs&gt;
          &lt;SignatureObject&gt;
              &lt;SignaturePtr WhichDocument=&quot;19ACDB8E-8F79-6725-9D6B-1A2D95BDBD70&quot;
                  XPath=&quot;//cs:Signature[Id = &amp;quot;NAADS Signature&amp;quot;]&quot;
/&gt;
          &lt;/SignatureObject&gt;
&lt;/VerifyRequest&gt;</dss1:DSSMessageWithSignedAlertStr>
    </dss1:DSSVerifySignedNaadsAlert>
  </soap:Body>
</soap:Envelope>
```

Submit the SOAP request to NAADS DSS

Send the SOAP request to the server using submit button in SoapUI:



A successful SOAP response from the NAADS DSS will be as follow:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <DSSVerifySignedNaadsAlertResponse xmlns="https://dss1.naad-adna.pelmorex.com/">
      <DSSVerifySignedNaadsAlertResult><![CDATA[<VerifyResponse RequestID="6944B0BD-F050-
4B84-2E50-C3A52AA3C7CA" Profile="Testing" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://www.docs.oasis-open.org/dss/oasis-dss-1.0-core-schema-cd-
02.xsd"><Result><ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</ResultMajor><Res
ultMinor /><ResultMessage /></Result><Response
/></VerifyResponse>]]></DSSVerifySignedNaadsAlertResult>
    </DSSVerifySignedNaadsAlertResponse>
  </soap:Body>
</soap:Envelope>
```

Appendix A

DSS Verification Request template

```
<VerifyRequest RequestID="UNIQUE IDENTIFIER"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.docs.oasis-
open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd" Profile="REQUEST ISSUER">
        <InputDocuments>
                <Document ID="ALERT ID">
                        <!-- dss:Base64XML/ this is default, not required to specify. We
                        will add the signed alert here. -->
                </Document>
        </InputDocuments>
        <OptionalInputs>
                <SignaturePlacement WhichDocument="ALERT ID"
CreateEnvelopedSignature="true"/>
        </OptionalInputs>
        <SignatureObject>
                <SignaturePtr WhichDocument="ALERT ID"
                        XPath="//cs:Signature[Id = &amp;quot;NAADS Signature&amp;quot;]" />
        </SignatureObject>
</VerifyRequest>
```

SOAP Envelope template

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:dss1="https://dss1.naad-
adna.pelmorex.com/">
  <soap:Header/>
  <soap:Body>
    <dss1:DSSVerifySignedNaadsAlert>
      <!--Optional:-->
      <dss1:DSSMessageWithSignedAlertStr>?</dss1:DSSMessageWithSignedAlertStr>
    </dss1:DSSVerifySignedNaadsAlert>
  </soap:Body>
</soap:Envelope>
```