Utilisation du service Web DSS du système ADNA

Contenu

Services de signature numérique (DSS) du système ADNA

Présentation du service Web DSS du système ADNA

Le service Web DSS du système ADNA offre à une tierce partie la possibilité de vérifier la signature des alertes émises via le système ADNA. Le service Web DSS du système ADNA est un service de signature numérique qui a été développé conformément aux normes OASIS pour la signature numérique. http://docs.oasis-open.org/dss/v1.0/oasisdss-core-spec-v1.0-os.html

Le DSS du système ADNA utilise une requête SOAP transmise sur le protocole HTTPS accessible aux adresses suivantes:

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

Demande de vérification du DSS du système ADNA

Une demande de vérification de la signature numérique d'une alerte du système ADNA est une requête DSS enveloppée dans un message SOAP envoyé via HTTPS vers l'une des URLs ci-dessus. Ces URLs sont spécifiées dans la signature de l'alerte du système ADNA sous la balise SignatureProperty

La demande de vérification DSS doit avoir la structure suivante:

```
<VerifyRequest RequestID="IDENTIFIANT UNIQUE"
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="ÉMETTEUR DE REQUETE">
        <InputDocuments>
                <Document ID="IDENTIFIANT ALERTE">
                        <!-- dss:Base64XML/ valeur par défaut, il n'est pas nécessaire
                        de la spécifier. Nous allons ajouter l'alerte signée ici. -->
                </Document>
        </InputDocuments>
        <OptionalInputs>
                <SignaturePlacement WhichDocument="IDENTIFIANT ALERTE"
CreateEnvelopedSignature="true"/>
        </OptionalInputs>
        <SignatureObject>
                <SignaturePtr WhichDocument="IDENTIFIANT ALERTE"
                        XPath="//cs:Signature[Id = &amp;quot;NAADS Signature&amp;quot;]" />
        </SignatureObject>
</VerifyRequest>
```

L'élément *VerifyRequest* est la requête DSS standard de l'OASIS pour la vérification de signature. Le DSS du système ADNA lira l'attribut *RequestID* pour identifier la demande de vérification reçue et l'attribut Profile pour identifier l'émetteur de la demande. Ces valeurs seront renvoyées dans la réponse de vérification.

L'élément *InputDocuments* englobe les documents soumis pour vérification. Actuellement, le DSS du système ADNA ne peut traiter qu'un seul document par demande.

L'élément *Document* contient l'alerte signée soumise pour vérification. L'attribut *ID* de l'élément identifiera le document soumis pour vérification, identification qui sera utilisée ultérieurement dans la demande de vérification.

L'élément *SignaturePlacement* à l'intérieur de l'élément *OptionalInputs* spécifie le type de signature (enveloppé ou enveloppant) via l'attribut *CreateEnvelopedSignature*. L'attribut *WhichDocument* identifiera le document dans l'élément *InputDocuments*. Actuellement, DSS du système ADNA ne traite que les signatures enveloppées.

L'attribut XPath de l'élément *SignaturePtr* dans l'objet *SignatureObject* indique le chemin d'accès à la signature dans l'alerte signée, *XPath="//cs:Signature[Id = "NAADS Signature"]"*. L'attribut *WhichDocument* identifiera l'alerte signée dans l'élément *InputDocuments*.

Réponse de vérification du DSS du système ADNA

Une réponse de vérification du DSS du système ADNA est reçue à la suite de la demande, telle que présentée au-dessus, enveloppée dans un message SOAP reçu via HTTPS.

La réponse devrait avoir la structure suivante:

```
<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>
```

L'élément *VerifyResponse* est la réponse DSS standard de l'OASIS pour la vérification de signature. Le DSS du système ADNA écrira dans l'attribut *RequestID* l'identité de la demande de vérification reçue et dans l'attribut *Profile* pour identifier l'émetteur de la demande.

L'élément *Result* fournit le résultat de la vérification de la signature en trois éléments: *ResultMajor*, *ResultMinor* et *ResultMessage*. L'élément *ResultMajor* fournit les informations génériques sur le résultat: succès ou erreur, dans un format de chaîne de caractères standard DSS de l'OASIS. L'élément *ResultMinor* fournit des informations plus détaillées en cas d'échec de la vérification. *ResultMessage* fournit des détails expliquant pourquoi la vérification a échoué.

Actuellement, Le DSS du système ADNA n'a que deux valeurs de résultat pour *ResultMajor* et *ResultMinor*.

Pour une vérification réussie:

```
<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>
```

Si erreur lors de la vérification:

```
<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>
```

Vérifier les alertes sur le service Web DSS du système ADNA à l'aide de SoapUI

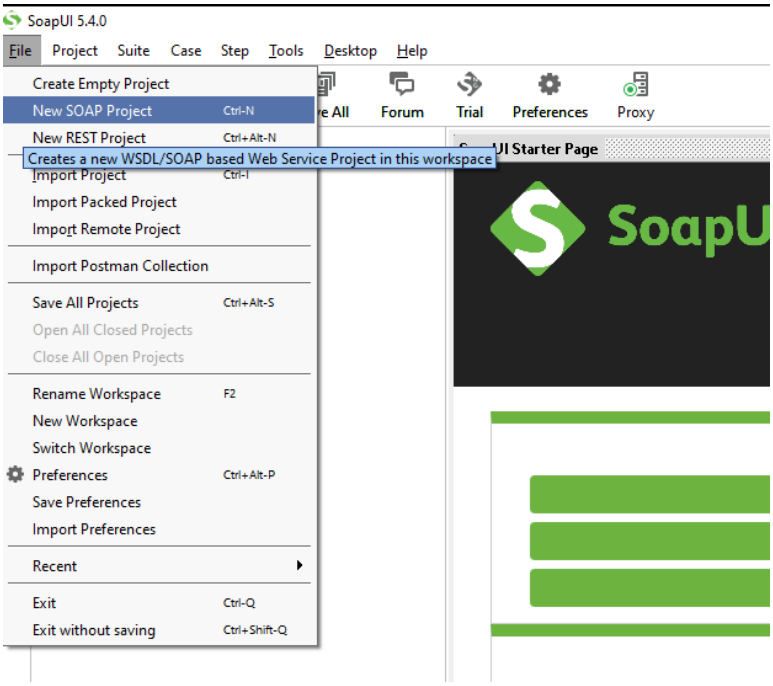
SoapUI

SoapUI est un outil de test fonctionnel pour les tests SOAP et REST. En tant que client SOAP, il vous permet d'envoyer facilement et rapidement des transactions via HTTP et HTTPS.

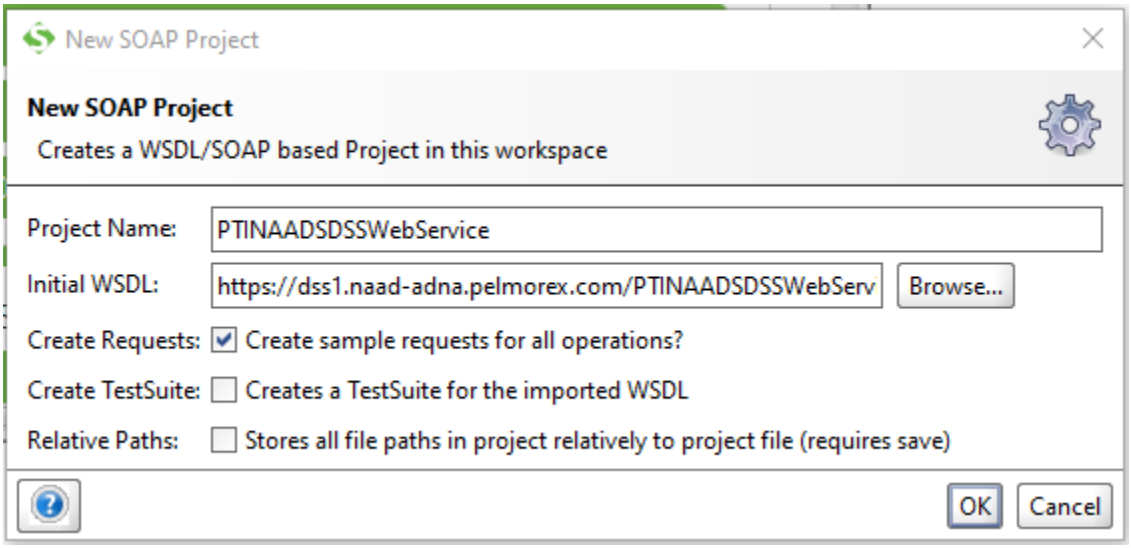
SoapUI est disponible en version open source gratuite. Pour plus d'informations, suivez ce lien : https://www.soapui.org/downloads/soapui.html

Créer la requête SOAP

Dans le menu «Fichier» de SoapUI, sélectionnez «Nouveau projet SOAP».

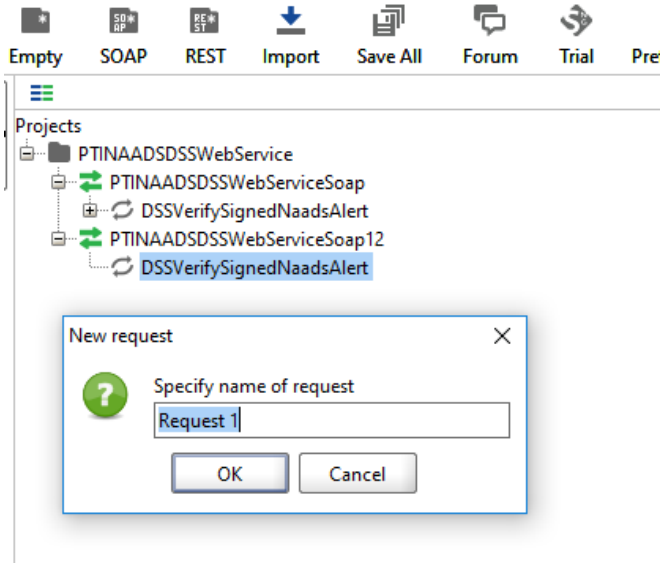


La boîte de dialogue ci-dessous apparaîtra. Dans le champ d'édition, tapez le chemin d'accès au fichier WSDL du service Web NAADS du système ADNA, par exemple https://dss1.naad-adna.pelmorex.com/PTINAADSDSSWebService.asmx?WSDL

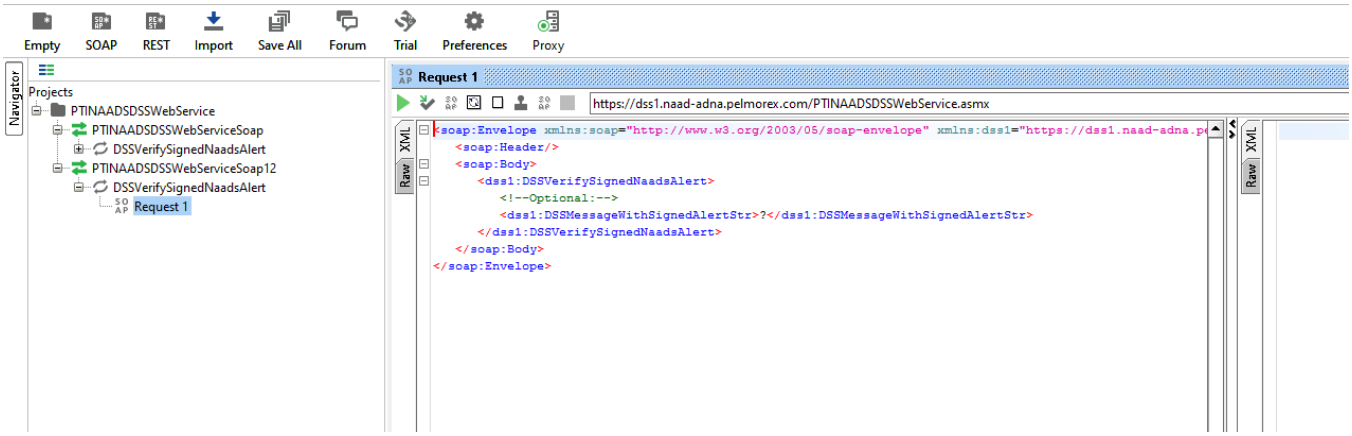


Dans le navigateur (panneau de gauche), développez la “PTINAADSDSSWebService” –> “PTINAADSDSSWebService12”:

Cliquez avec le bouton droit sur «DSSVerifySignedNaadsAlert» et sélectionnez l'opération «Nouvelle demande» dans la boîte de dialogue suivante:



L’enveloppe SOAP suivante sera créée.



La valeur de chaîne du paramètre *DSSMessageWithSignedAlertStr* doit être remplacée par la demande de vérification DSS au format UTF-8.

```
<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>
```

Préparer la demande de vérification DSS

1. Obtenez l’alerte signée à vérifier à l’adresse http://rss.naad-adna.pelmorex.com/. L'alerte aura un format PAC XML comme ci-dessous.

```
<?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. Créez la demande de vérification standard DSS OASIS en utilisant le modèle présenté dans la section « demande de vérification DSS du système ADNA ».

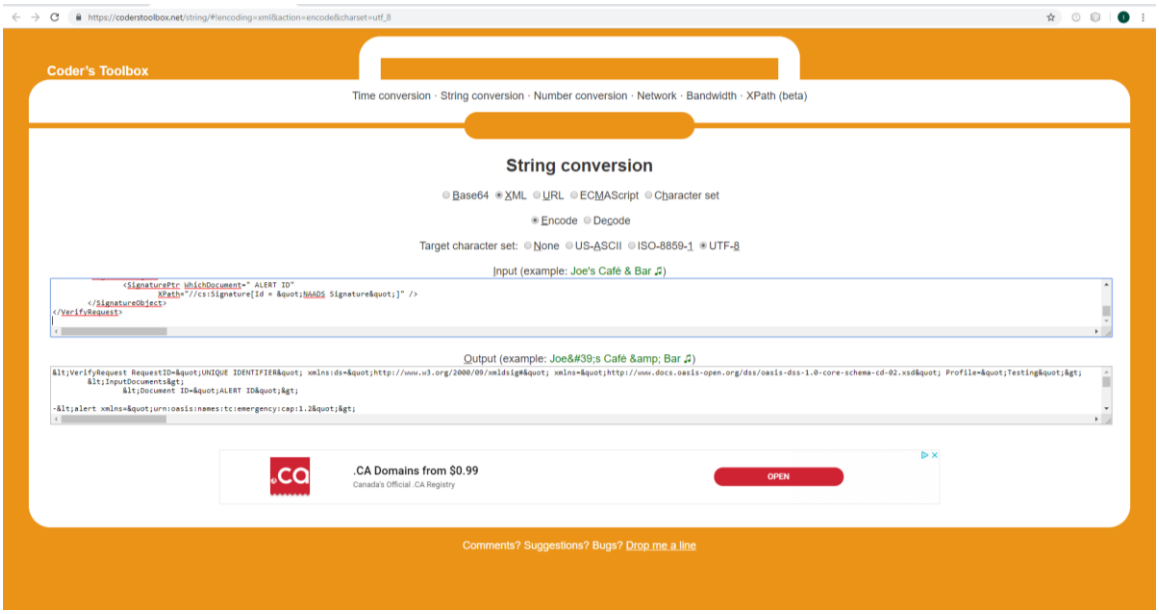
3. Dans le modèle, mettez à jour le texte surligné en jaune avec les valeurs correctes:
   - "IDENTIFIANT UNIQUE"
   - "ÉMETTEUR DE REQUETE"
   - "IDENTIFIANT ALERTE"

4. Copiez l'alerte PAC **sans** la première ligne (<?xml version="1.0" encoding="UTF-8"?>) Et incluez l'alerte dans l'élément *Document*.

```
<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. **Encodez** cette nouvelle demande de vérification DSS **du format XML au format UTF-8**. Vous trouverez ci-dessous un exemple d'outil de conversion en ligne:

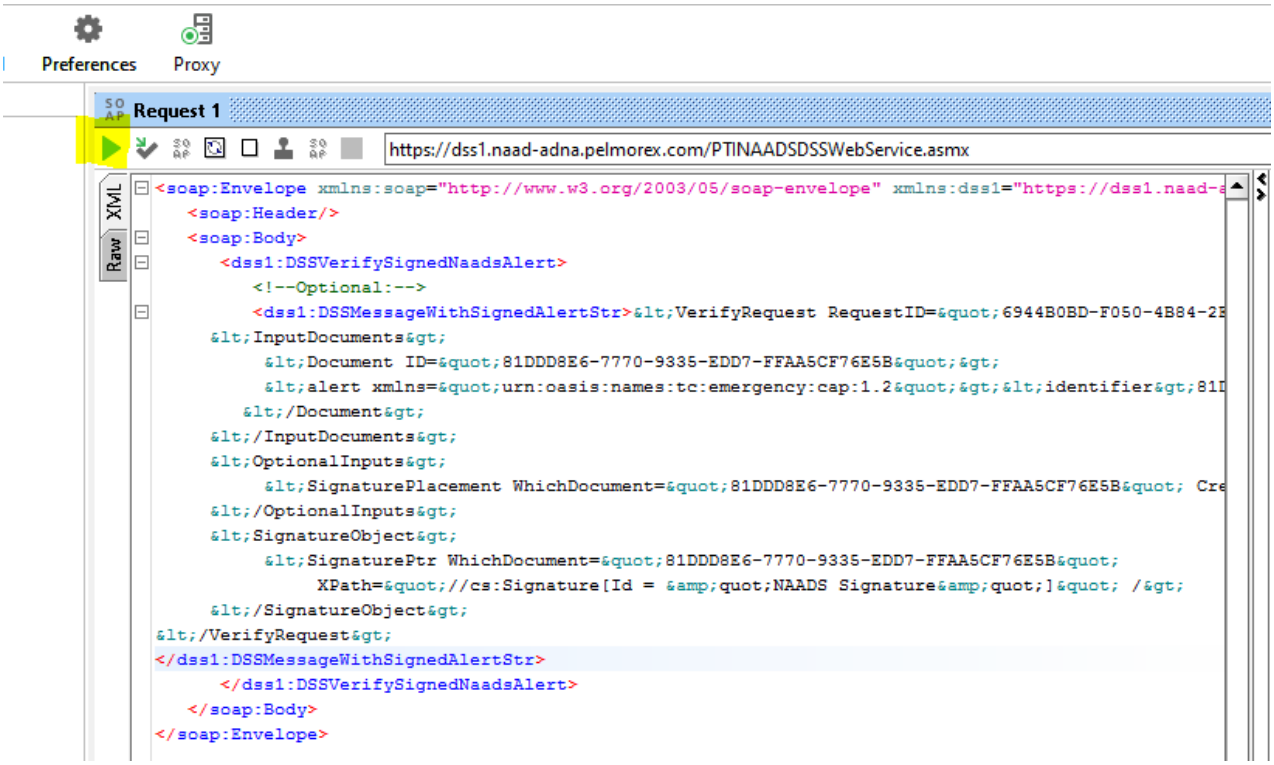


6. Copiez le résultat et ajoutez la demande de vérification à l'enveloppe SOAP créée par le client SoapUI (remplacez le point d'interrogation "?", après **<dss1:DSSMessageWithSignedAlertStr>**):

```
<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>
```

Soumettre la demande SOAP au DSS du système ADNA

Envoyez la demande SOAP au serveur en utilisant le bouton d'envoi de SoapUI:



Une réponse SOAP réussie du DSS du système ADNA sera comme suit:

```
<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>
```

Appendice A

Modèle de demande de vérification DSS

```
<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="IDENTIFIANT ALERTE">
                        <!-- dss:Base64XML/ this is default, not required to specify. We
                        will add the signed alert here. -->
                </Document>
        </InputDocuments>
        <OptionalInputs>
                <SignaturePlacement WhichDocument="IDENTIFIANT ALERTE"
CreateEnvelopedSignature="true"/>
        </OptionalInputs>
        <SignatureObject>
                <SignaturePtr WhichDocument="IDENTIFIANT ALERTE"
                        XPath="//cs:Signature[Id = &amp;quot;NAADS Signature&amp;quot;]" />
        </SignatureObject>
</VerifyRequest>
```

Modèle d'enveloppe SOAP

```
<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>
```