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://dss.naad-adna.pelmorex.com/
- 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 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="" 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" Profile="">
        <InputDocuments>
                <Document ID="xs:ID">
                        <!--dss:Base64XML/ this is default, not required to specify. We will add the signed alert here. -->
                </Document>
        </InputDocuments>
        <OptionalInputs>
                <SignaturePlacement WhichDocument=" Document ID " CreateEnvelopedSignature="true"/>
        </OptionalInputs>
        <SignatureObject>
                <SignaturePtr WhichDocument="InputDocuments Document ID"
                        XPath=<!-- XPath will include the path to the NAADS Signature node in the alert -->
                </SignaturePtr>
        </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>
```

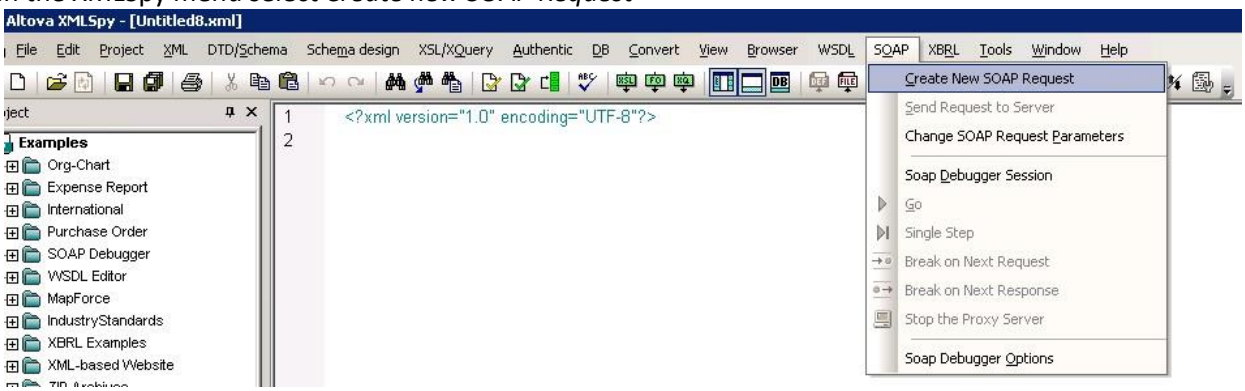
Verify alerts on NAADS DSS web service using Altova XMLSpy

Altova XMLSpy

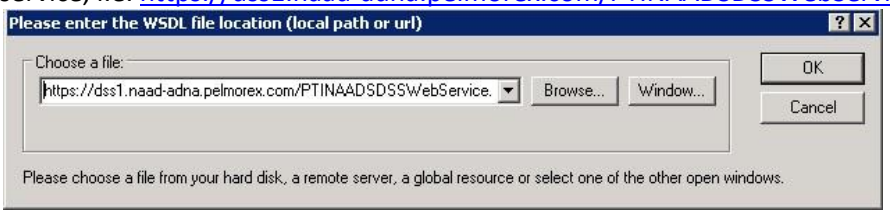
Altova`s XMLSpy is an XML editor that provides various features for XML based services and tools. XMLSpy includes, in the Enterprise edition, a SOAP client that can send transactions through HTTP and HTTPS.
XMLSpy with full feature support is available in a 30 days trial version. For more information follow the link below: http://www.altova.com/xmlspy.html

Create the SOAP request

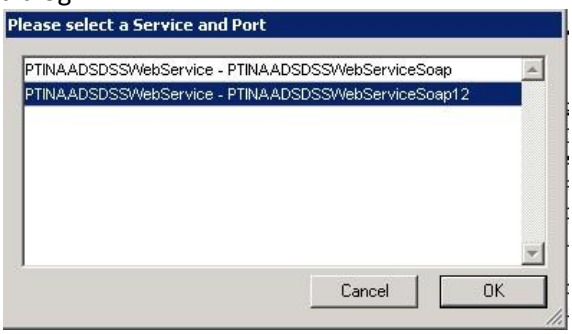
In the XMLSpy menu select *Create new SOAP Request*



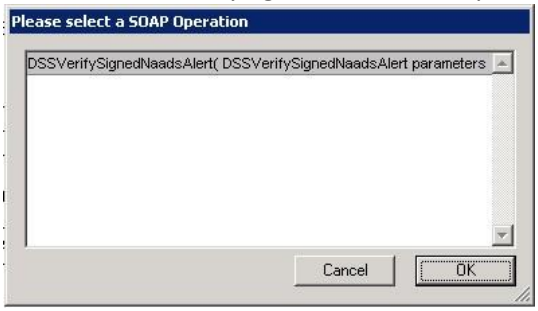
..the dialog below will pop-up. In the edit box type the path to the WSDL file of the NAADS DSS web service, i.e. https://dss1.naad-adna.pelmorex.com/PTINAADSDSSWebService.asmx?WSDL



Select OK and then select PTINAADSDSSWebService – PTINAADSDSSWebService12 from the following dialog:



Select the DSSVerifySignedNaadsAlert 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-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope" xmlns:SOAP-ENC="http://www.w3.org/2003/05/soapencoding"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <SOAP-ENV:Body>
                <m:DSSVerifySignedNaadsAlert xmlns:m="https://dss1.naad-adna.pelmorex.com/">
                        <m:DSSMessageWithSignedAlertStr>String</m:DSSMessageWithSignedAlertStr>
                </m:DSSVerifySignedNaadsAlert>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Prepare the DSS verification request

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

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
        <identifier>84290443-E9CB-DF43-EB55-392A71E787DB</identifier>
        <sender>ChrisPittens</sender>
        <sent>2011-02-14T11:35:33-05:00</sent>
        <status>Actual</status>
        <msgType>Alert</msgType>
        <scope>Public</scope>
        <code>profile:CAP-CP:0.3</code>
        <info>
                <language>fr-CA</language>
...
        </info>
        <Signature Id="NAADS Signature" xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>/3BndiNt1QQf0zcZVm1yHsgDoqY=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>EuJVQ6fzB3/rirP9Jc/  ...  +FA==</SignatureValue>
                <KeyInfo>
                        <X509Data>
        <X509Certificate>MIIFTzCCBDegAwIBAgIQZOLNSjzKVXQLZww/ ... 1rpRWwc9X8X/hriz1Vaf2nyFOim5PGXSWNA==</X509Certificate>
                        </X509Data>
                </KeyInfo>
                <Object xmlns="">
                        <SignatureProperties>
                                <SignatureProperty Id="NAADS-DSS1" Target="https://dss1.naad-adna.pelmorex.com">
```

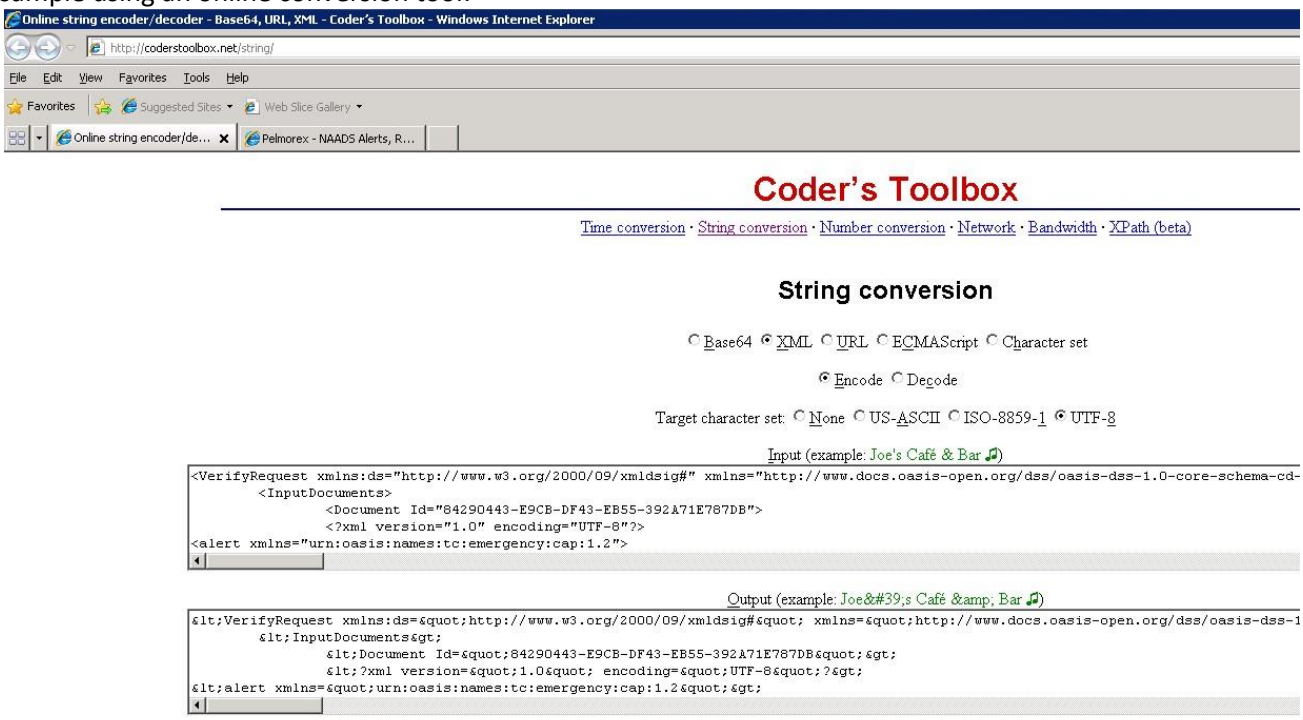
```
                                        <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd"/>
                                    </SignatureProperty>
                                    <SignatureProperty Id="NAADS-DSS2" Target="https://dss2.naad-adna.pelmorex.com">
                                        <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd"/>
                    </SignatureProperty>
                        </SignatureProperties>
                    </Object>
            </Signature>
</alert>
```

Create the OASIS DSS standard verification request, as presented above, and include the alert in the Document element:

```
<VerifyRequest 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" RequestID="6944B0BD-F050-4B84-2E50-C3A52AA3C7CA" Profile="...">
            <InputDocuments>
                    <Document ID="84290443-E9CB-DF43-EB55-392A71E787DB">
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
            <identifier>84290443-E9CB-DF43-EB55-392A71E787DB</identifier>
            <sender>ChrisPittens</sender>
            <sent>2011-02-14T11:35:33-05:00</sent>
            <status>Actual</status>
            <msgType>Alert</msgType>
            <scope>Public</scope>
            <code>profile:CAP-CP:0.3</code>
            <info>
                    <language>fr-CA</language>
....
            </info>
            <Signature Id="NAADS Signature" xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <SignedInfo>
                            <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                            <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                            <Reference URI="">
                                    <Transforms>
                                            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature"/>
                                    </Transforms>
                                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                    <DigestValue>/3BndiNt1QQf0zcZVm1yHsgDoqY=</DigestValue>
                            </Reference>
                    </SignedInfo>
                    <SignatureValue>EuJVQ6fzB3/  ...  +FA==</SignatureValue>
                    <KeyInfo>
                            <X509Data>
            <X509Certificate>MIIFTzCCBDegAwIBAgIQZOLNSjzKVXQLZww/  .... /hriz1Vaf2nyFOim5PGXSWNA==</X509Certificate>
                            </X509Data>
                    </KeyInfo>
                    <Object xmlns="">
                            <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="6944B0BD-F050-4B84-2E50-C3A52AA3C7CA"
CreateEnvelopedSignature="true"/>
        </OptionalInputs>
        <SignatureObject>
                <SignaturePtr WhichDocument="6944B0BD-F050-4B84-2E50-C3A52AA3C7CA" XPath="//cs:Signature[Id = &quot;NAADS
Signature&quot;]" xmlns:cs="urn:oasis:names:tc:emergency:cap:1.2"/>
        </SignatureObject>
</VerifyRequest>
```

Convert the DSS verification request from XML format to the UTF-8 format. Below is a conversion sample using an online conversion tool:

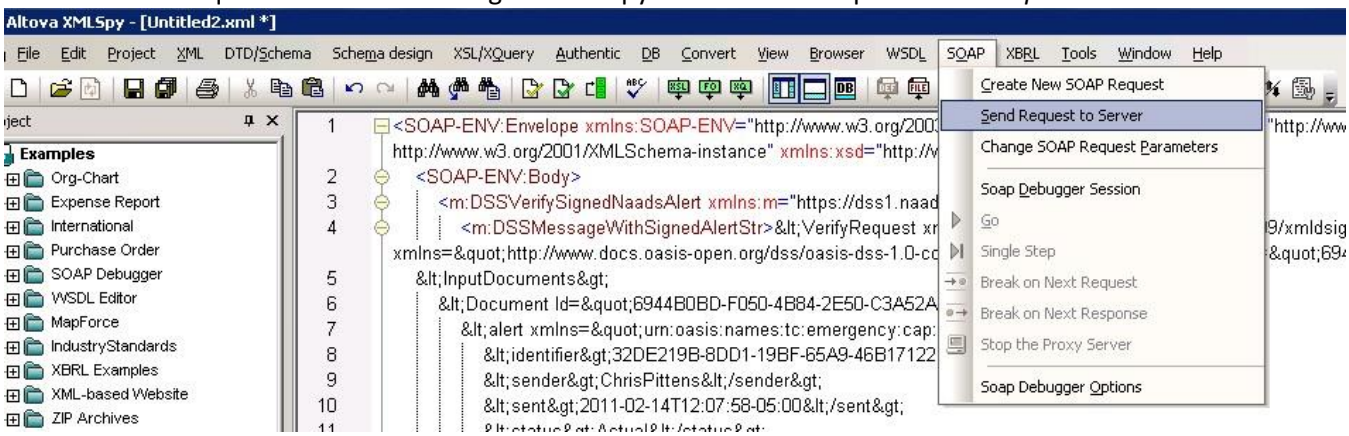


Add the verification request to the SOAP envelope created by the XMLSpy:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope" xmlns:SOAP-ENC="http://www.w3.org/2003/05/soapencoding"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <SOAP-ENV:Body>
                <m:DSSVerifySignedNaadsAlert xmlns:m="https://dss1.naad-adna.pelmorex.com/">
                        <m:DSSMessageWithSignedAlertStr>&lt;VerifyRequest
xmlns:ds=&quot;http://www.w3.org/2000/09/xmldsig#&quot; xmlns=&quot;http://www.docs.oasis-open.org/dss/oasis-dss-1.0-
coreschema-cd-02.xsd&quot; RequestID=&quot;6944B0BD-F050-4B84-2E50-C3A52AA3C7CA&quot; Profile=&quot;&quot;&gt;
        &lt;InputDocuments&gt;
                &lt;Document ID=&quot;6944B0BD-F050-4B84-2E50-C3A52AA3C7CA&quot;&gt;
                        &lt;alert xmlns=&quot;urn:oasis:names:tc:emergency:cap:1.2&quot;&gt;
                                &lt;identifier&gt;32DE219B-8DD1-19BF-65A9-46B17122146D&lt;/identifier&gt;
                                &lt;sender&gt;ChrisPittens&lt;/sender&gt;
....
xmlns:cs=&quot;urn:oasis:names:tc:emergency:cap:1.2&quot;/&gt;
        &lt;/SignatureObject&gt;
&lt;/VerifyRequest&gt;</m:DSSMessageWithSignedAlertStr>
                </m:DSSVerifySignedNaadsAlert>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Submit the SOAP request to NAADS DSS

Send the SOAP request to the server using the XMLSpy. Use the menu option *Send Request to Server*:



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

```
<?xml version="1.0" encoding="utf-8"?>
<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>&lt;VerifyResponse RequestID="6944B0BD-F050-4B84-2E50-
C3A52AA3C7CA" Profile="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.docs.oasis-open.org/dss/oasis-dss-
1.0core-schema-cd-
02.xsd"&gt;&lt;Result&gt;&lt;ResultMajor&gt;urn:oasis:names:tc:dss:1.0:resultmajor:Success&lt;/ResultMajor&gt;&lt;ResultMinor
/&gt;&lt;ResultMessage /&gt;&lt;/Result&gt;&lt;/VerifyResponse&gt;</DSSVerifySignedNaadsAlertResult>
                </DSSVerifySignedNaadsAlertResponse>
        </soap:Body>
</soap:Envelope>
```

Get the NAADS DSS verification response from the DSSVerifySignedNaadsAlertResult and use the decoder tool to convert from UTF-8 to XML.

```
<VerifyResponse RequestID="6944B0BD-F050-4B84-2E50-C3A52AA3C7CA" Profile="" 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>
                <ResultMinor/>
                <ResultMessage/>
        </Result>
</VerifyResponse>
```

Appendix A

DSS Verification Request template

```
<VerifyRequest xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.docs.oasis-open.org/dss/oasis-dss-1.0-core-schema-cd02.xsd" RequestID="" Profile="">
 <InputDocuments>
  <Document ID="">
</Document>
 </InputDocuments>
 <OptionalInputs>
  <SignaturePlacement WhichDocument="" CreateEnvelopedSignature="true" />
</OptionalInputs>
 <SignatureObject>
  <SignaturePtr WhichDocument="" XPath="//cs:Signature[Id = &quot;NAADS Signature&quot;]" xmlns:cs="urn:oasis:names:tc:emergency:cap:1.2" />
 </SignatureObject>
</VerifyRequest>
```