Digitally Signed SPSCertificate message

Overview of prototype of digital signature applied to SPSCertificate message to TRACES

UN/CEFACT Forum Sardinia, Oct 14-18 2013

Overview

Non-signed certificate submission, as demoed earlier is available

- **SPSCertificate, wrapped in TRACES-specific element containing credentials, XMLGate service ID etc.**

How do we apply digital signature?

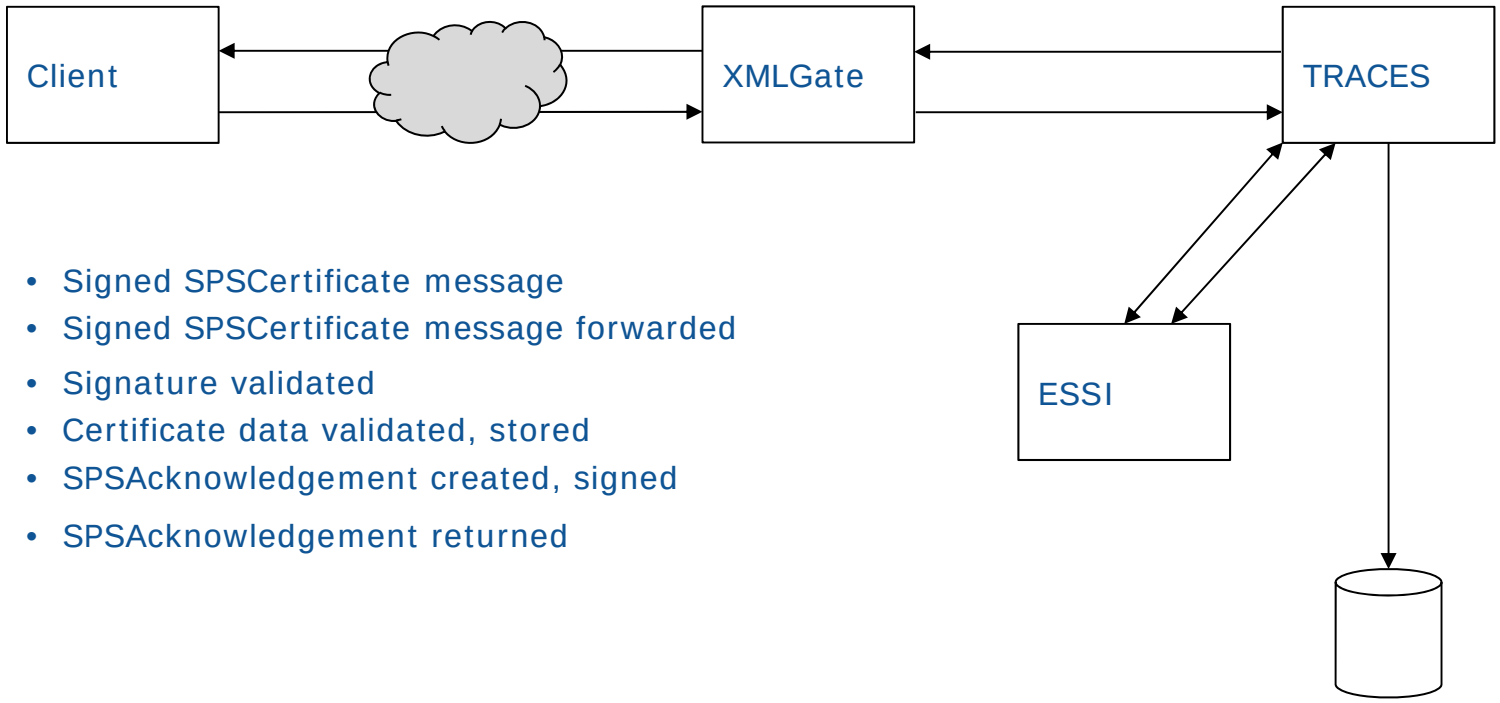
- **On the incoming messages (SPSCertificate)**
- **On the reply (SPSAcknowledge)**
- **Based on recommendations made in analysis presented in Geneva in April**

Applying digital signature

Choice of technology – ESSI:

- **corporate Commission signature infrastructure, with support for:**
  - signing documents (XAdES, PAdES)
  - validation (incoming signed document
  - extension – timestamp, digital certificate inclusion
  - long-time archiving (re-signing, but not for physical storage of signed docs)
  - security aspects (HSM…)
  - Support EU official list of CA / CSP

Overview



- Signed SPSCertificate message
- Signed SPSCertificate message forwarded
- Signature validated
- Certificate data validated, stored
- SPSAcknowledgement created, signed
- SPSAcknowledgement returned

Actual steps in the prototype

Prepare the document for signature

- **Without XMLGate envelope**
- **With TRACES credentials**

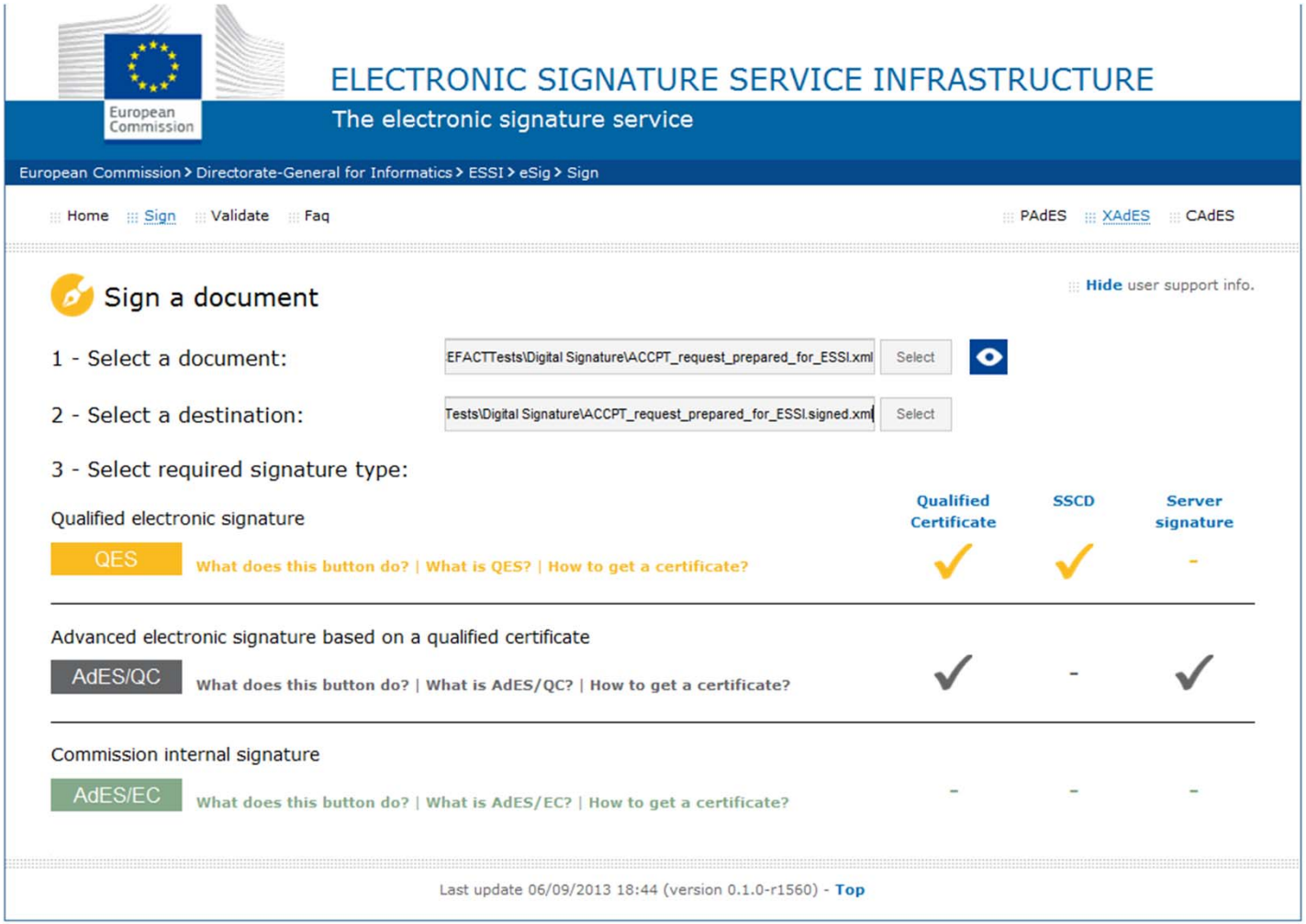
Sign the data

- **Upload to ESSI**
- **Sign it (using ESSI built-in test certificate)**

Put signed message in XMLGate envelope

Send it to XMLGate

European Commission



Signed certificate ready to send

Enveloping Signature

SPSCertificate enveloped in the Signature

```
<soap:Body>
   <sas:callServices>
      <dgs:SubmitSignedCertificateRequest xmlns:dgs="urn:protocol.schema.wsdl.uncefact.traces.sanco.cec
         <ds:Signature Id="Signature_1381398931876">
            <ds:SignedInfo Id="Signature_1381398931876-SignedInfo">
               <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
               <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
               <ds:Reference URI="#Doc_1381398931876-1" Id="Signature_1381398931876-Reference-0">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                  <ds:DigestValue>P6TyZo19j1PtDnORYmMymsdb7Tt6q2Q6adp/ai/SdwzD3CiWGuy5W8ov0SyAf3k5h0Fc+
               </ds:Reference>
               <ds:Reference URI="#Signature_1381398931876_SignedProperties" Type="http://uri.etsi.org/
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                  <ds:DigestValue>iQp8pLu7xAcLwW+SxpnGfgJQ5dcrSaxURN1A2z8OSE772tseJXG2bUzHmGwuAgZX1I7jJ
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue Id="Signature_1381398931876_Value">L/Zy/+bLFDgERrMC/5OFarV4l0UMH/x79XPF2
            <ds:KeyInfo>
               <ds:X509Data>
                  <ds:X509Certificate>MIIF0DCCBLigAwIBAgIEOrZQizANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJCI
                  <ds:X509Certificate>MIIFjjCCBHagAwIBAgIUIBhwLg4/l5vcFjA30Du20n1cSyIwDQYJKoZIhvcNAQEFB
                  <ds:X509Certificate>MIIGijCCBHKgAwIBAgIUS1qCiGUEuPo4cOB9rL1yVIX1AxIwDQYJKoZIhvcNAQEFB
               </ds:X509Data>
            </ds:KeyInfo>
            <ds:Object Id="Doc_1381398931876-1">
               <urn:ImportCertificateRequest xmlns:urn1="urn:un:unece:uncefact:data:standard:SPSCertifi
                  <urn:TRACESAuthInfo>
                     <urn:Username>CCA.NZ@traces-cbt.net</urn:Username>
                     <urn:Password>Q0NBLk5a</urn:Password>
                  </urn:TRACESAuthInfo>
                  <rsm:SPSCertificate xmlns:rsm="urn:un:unece:uncefact:data:standard:SPSCertificate:5"
                     <rsm:SPSExchangedDocument>
                        <ram:Name languageID="en">Animal and Public Health Certificate&lt;sup>1&lt;/sup
                        <ram:Name languageID="de">Tiergesundheits- und Genusstauglichkeitsbescheinigung
                        <ram:ID>DGS/131010/T01</ram:ID>
                        <ram:TypeCode>852</ram:TypeCode>
                        <ram:StatusCode>39</ram:StatusCode>
                        <ram:IssueDateTime>2013-01-29T22:38:11Z</ram:IssueDateTime>
                        <ram:IssuerSPSParty>
                           <ram:Name languageID="en">NEW ZEALAND FOOD SAFETY AUTHORITY</ram:Name>
                           <ram:RoleCode>PQ</ram:RoleCode>
                        </ram:IssuerSPSParty>
```

Signed acknowledgement message

Enveloping Signature

SPSAcknowledgement enveloped in the Signature

Corrupt or manipulated data or signature

Enveloping Signature

SPSAcknowledgement enveloped in the Signature, indicating error


```
<ds:Signature Id="Signature_1381405426596" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo Id="Signature_1381405426596-SignedInfo">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
    <ds:Reference URI="#Doc_1381405426596-1" Id="Signature_1381405426596-Reference-0">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
      <ds:DigestValue>sqUVkPDsUTMI3JOK0qPTgrUnw23WmEGCngSBz729kkSwe2zTZGbOw4DX+6Pt7k5e02wIGLGbtA
    </ds:Reference>
    <ds:Reference URI="#Signature_1381405426596_SignedProperties" Type="http://uri.etsi.org/01903
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
      <ds:DigestValue>WrWumEYBcbIj431paKgrAQKn9eVQkPZYMwBzcFE/EdyBcXKPZG879sxhSkes4IOB1p0D8sOURk
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue Id="Signature_1381405426596_Value">XoQvzHE1RkenrRtgkrR5Mj4wnexTebCC7AUh8WAVm1
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>MIIF0DCCBLigAwIBAgIEOrZQizANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJCTTEZMB
      <ds:X509Certificate>MIIFjjCCBHagAwIBAgIUIBhwLg4/l5vcFjA30Du20n1cSyIwDQYJKoZIhvcNAQEFBQAwfz
      <ds:X509Certificate>MIIGijCCBHKgAwIBAgIUS1qCiGUEuPo4cOB9rL1yVIX1AxIwDQYJKoZIhvcNAQEFBQAwgZ
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:Object Id="Doc_1381405426596-1">
    <urn:ImportCertificateResult xmlns:urn="urn:protocol.schema.wsdl.uncefact.traces.sanco.cec.eu"
      <urn1:SPSAcknowledgement xmlns:urn1="urn:un:unece:uncefact:data:standard:SPSAcknowledgement
        <urn1:SPSAcknowledgementDocument>
          <urn2:IssueDateTime >2013-10-10T11:43:46.547Z</urn2:IssueDateTime>
          <urn2:StatusCode>17</urn2:StatusCode>
          <urn2:ReasonInformation>1002: Signature error</urn2:ReasonInformation>
        </urn1:SPSAcknowledgementDocument>
      </urn1:SPSAcknowledgement>
    </urn:ImportCertificateResult>
  </ds:Object>
  <ds:Object>
    <xades:QualifyingProperties Target="#Signature_1381405426596" xmlns:xades="http://uri.etsi.org
      <xades:SignedProperties Id="Signature_1381405426596_SignedProperties">
        <xades:SignedSignatureProperties>
          <xades:SigningTime>2013-10-10T11:43:46.597Z</xades:SigningTime>
          <xades:SigningCertificate>
            <xades:Cert>
              <xades:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                <ds:DigestValue>XyG+jdS7pQX9rNM+Dhq0LyIfmF9HoTqc0KWErRp4AaqqYaqQSDswUgu5jHV
              </xades:CertDigest>
              <xades:IssuerSerial>
                <ds:X509IssuerName>CN=QuoVadis EU Issuing Certification Authority G2,OU=Issu
                <ds:X509SerialNumber>430192745889505299029505060922684438153620947730</ds:X
              </xades:IssuerSerial>
            </xades:Cert>
          </xades:SigningCertificate>
        </xades:SignedSignatureProperties>
```

Summary

The key mechanisms are in place and work

For a Production deployment some steps are needed:

- **Agreement on CA / CSP of SPSCertificate issuing authority, agree on equivalence criteria**
- **Adapt ESSI for this additional CA / CSP**
- **Develop archival facility**
- **Agreement on details (timestamping, audit logging…) may depend on bilateral agreements**

WS-security not considered at this moment