Signed SOAP Messages

Signed SOAP Messages

- Signed SOAP Messages
  - Introduction
  - Purpose
  - SOAP Digital Signature Extension - SOAP-DSIG
  - Examples of Digitally Signed SOAP Message
    - Example 1
    - Example 2

Introduction

This page presents a brief concept of digitally signing SOAP messages.

Purpose

Digital signatures, in the form of public-private key pairs, provide means for:

- *authentication* of the message sender (proving that the sender is whom when claims to be);
- *authorization* (certifying that the sender has the proper clearances to perform the queries or methods intended);
- verifying *integrity* of the signed data, by utilizing hashes;
- *encryption*, if needed.

SOAP Digital Signature Extension - SOAP-DSIG

The Digital Signature Extension (SOAP-DSIG) specifies a XML document structure that denotes the original signed message and the digital signature data. This XML structure contains specifications for the algorithms, public key, message digest, and digital certificate.

Examples of Digitally Signed SOAP Message

Example 1

Extracted from http://publib.boulder.ibm.com/infocenter/cicsts/v3r1/index.jsp?topic=/com.ibm.cics.ts31.doc/dfhws/wsSecurity/dfhws_soapmsg_signed.htm.

The header contains elements such as `ds:DigestValue`, where the message digest, generated with `ds:DigestMethod Algorithm`, is displayed (in this case, *sha1*). The `ds:Reference URI` shows the content being signed. The element `ds:SignatureValue` contains the digital signature, and `wsse:BinarySecurityToken` has information about the X.509 certificate, including the public key, encoded in base64Binary.

```
<?xml version="1.0" encoding="UTF8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header>
 <wsse:Security xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" SOAP-ENV:mustUnderstand="1">
 <wsse:BinarySecurityToken  1
              EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0
#Base64Binary"
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509"
              wsu:Id="x509cert00">MIIChDCCAe2gAwIBAgIBADANBgkqhkiG9w0BAQUFADAwMQswCQYDVQQGEwJHQjEMMAoGA1UEChMD
                                  SUJNMRMwEQYDVQQDEwpXaWxsIFlhdGVzMB4XDTA2MDEzMTAwMDAwMFoXDTA3MDEzMTIzNTk1OVow
                                  MDELMAkGA1UEBhMCR0IxDDAKBgNVBAoTA0lCTTETMBEGA1UEAxMKV2lsbCBZYXRlczCBnzANBgkq
                                  hkiG9w0BAQEFAAOBjQAwgYkCgYEArsRj/n+3RN75+jaxuOMBWSHvZCB0egv8qu2UwLWEeiogePsR
                                  6Ku4SuHbBwJtWNr0xBTAAS9lEa70yhVdppxOnJBOCiERg7S0HUdP7a8JXPFzA+BqV63JqRgJyxN6
                                  msfTAvEMR07LIXmZAte62nwcFrvCKNPCFIJ5mkaJ9v1p7jkCAwEAAaOBrTCBqjA/BglghkgBhvhC
                                  AQ0EMhMwR2VuZXJhdGVkIGJ5IHRoZSBTZWN1cml0eSBTZXJ2ZXIgZm9yIHovT1MgKFJBQ0YpMDgG
                                  ZQVRFU0BVSy5JQk0uQ09ggdJQk0uQ09NhgtXV1cuSUJNLkNPTYcECRRlBjAO
 </wsse:BinarySecurityToken>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
                 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
                 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    <c14n:InclusiveNamespaces xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds wsu xenc SOAP-
ENV "/>
   </ds:CanonicalizationMethod>
   <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
   <ds:Reference URI="#TheBody">
    <ds:Transforms>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
       <c14n:InclusiveNamespaces xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsu SOAP-ENV "
/>
     </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/> 2
    <ds:DigestValue>QORZEA+gpafluShspHxhrjaFlXE=</ds:DigestValue> 3
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>drDH0XESiyN6YJm27mfK1ZMG4Q4IsZqQ9N9V6kEnw2lk7aM3if77XNFnyKS4deglbC3ga11kkaFJ 4
                     p4jLOmYRqqycDPpqPm+UEu7mzfHRQGe7H0EnFqZpikNqZK5FF6fvYlv2JgTDPwrOSYXmhzwegUDT
                     lTVjOvuUgXYrFyaO3pw=</ds:SignatureValue>
   <ds:KeyInfo>
    <wsse:SecurityTokenReference>
      <wsse:Reference URI="#x509cert00"
                      ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0
#X509"/> 5
    </wsse:SecurityTokenReference>
   </ds:KeyInfo>
  </ds:Signature>
 </wsse:Security>
</SOAP-ENV:Header>
<SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="TheBody">
 <getVersion xmlns="http://msgsec.wssecfvt.ws.ibm.com"/>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Example 2

Extracted from http://searchsoa.techtarget.com/news/article/0,289142,sid26_gci872858,00.html.

Below is an example of a SOAP in RCP-style, not signed. The method `testMethod` is invoked; the SOAP service is located at `http: //localhost: 8080/LogTestService`.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <SOAP-ENV:Body>
      <ns1:testMethod xmlns:ns1="http://localhost:8080/LogTestService"/>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The same document is now signed using a X.509 certificate and public key. We can note the elements `ds:DigestValue`, representing the digest of the original message above. The element `ds:SignatureValue` brings the digital signature of the digest, and `ds:KeyInfo` presents the X.509 certificate and public key. The server must use these data to verify the signature.

```
<SOAP-ENV:Envelope SOAP-ENV:actor="some-uri" SOAP-ENV:mustUnderstand="1" xmlns:SOAP-ENV="http://
schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12" xmlns:xsd="http:/
/www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP-ENV:Header>
    <SOAP-SEC:Signature>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>

          <ds:Reference URI="#Body">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>
              2jmj7l5rSw0yVb/vWAYkK/YBwk=
            </ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
          Xwu8MRCOvJGRhjZcfgOqq9sXM/hsAzAmS/SbyVnAy7x0JwrMiqc4sg==
        </ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              MIIC9jCCArQCBDruqiowCwYHKoZIzjgEAwUAMGExCzAJBgNVBAYTAkRFMR0wGwYDVQQKExRVbml2
              ZXJzaXR5IG9mIFNpZWdlbjEQMA4GA1UECxMHRklxMk5VRTEhMB8GA1UEAxMYQ2hyaXN0aWFulEdl
              dWVyLVBvbGxtYW5uMB4XDTAxMDUwMTEyMjA1OFoXDTA2MTAyMjEyMjA1OFowYTELMAkGA1UEBhMC
              REUxHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgU2llZ2VuMRAwDgYDVQQLEwdGQjEyTlVFMSEwHwYD
              VQQDExhDaHJpc3RpYW4gR2V1ZXltUG9sbG1hbm4wggG3MIIBLAYHKoZIzjgEATCCAR8CgYEA/X9T
              gR11EilS30qcLuzk5/YRt1I870QAwx4/gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv
              8mZgt2uZUKWkn5/oBHsQlsJPu6nX/rfGG/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HX
              Ku/ylgMZndFIAccCFQCXYFCPFSMLzLKSuYKi64QL8Fgc9QKBgQD34aCF1ps93su8q1w2uFe5eZSv
              u/o66oL5V0wLPQeCZ1FZV4661FIP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64e
              K7OmdZFuo38L+iE1YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAAC
              gYASWfn+G1k/nWntj9jX7Nk5JKaiLZ9BLR16eJJxqff33THLfdGs98Xmh2oRWZVh9PMV8oTP3hpR
              cRipjZUZVElqsBlOGTVLCg4H5TJ81JWOiprh+mkhClNqUr8l5Hu7FBSvQB6inryeva7j0aKNilvK
              8vfHTiUZpnyNRhkveBlM0jALBgcqhkjOOAQDBQADLwAwLAIUPDd/UmB9GeHqvGjny30Bvjt0AkUC
              FA9ab72kKuB5geYGeckbBrcgPnZk
            </ds:X509Certificate>
          </ds:X509Data>
          <ds:KeyValue>
            <ds:DSAKeyValue>
              <ds:P>
                /X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuA
                HTRv8mZgt2uZUKWkn5/oBHsQlsJPu6nX/rfGG/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOu
                K2HXKu/ylgMZndFIAcc=
              </ds:P>

              <ds:Q>
                I2BQjxUjC8yykrmCouuEC/BYHPU=
              </ds:Q>

              <ds:G>
                9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCBgLRJFnEj6EwoFhO3
                zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKL
                Zl6Ae1UlZAFMO/7PSSo=
              </ds:G>

              <ds:Y>
                Eln5/ntZP51p7Y/Y1+zZOSSmoi2fQS0deniScan3990xy33RrPfF5odqEVmVYfTzFfKEz94aUXEY
                qY2VGVRCKrAZThk1SwoOB+UyfNSVjoqa4fppIQpTalK/JeR7uxQUr0Aeop68nr2u49GijYiLyvL3
                x04lGaZ8jUYZL3gZTNl=
              </ds:Y>
            </ds:DSAKeyValue>
          </ds:KeyValue>
        </ds:KeyInfo>
      </ds:Signature>
    </SOAP-SEC:Signature>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <ns1:testMethod xmlns:ns1="http://localhost:8080/LogTestService"/>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```