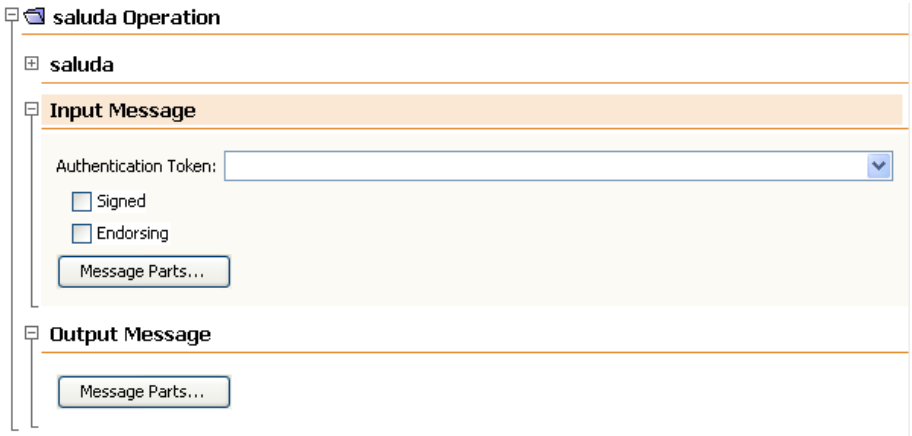
Seguridad a nivel de mensaje en Metro

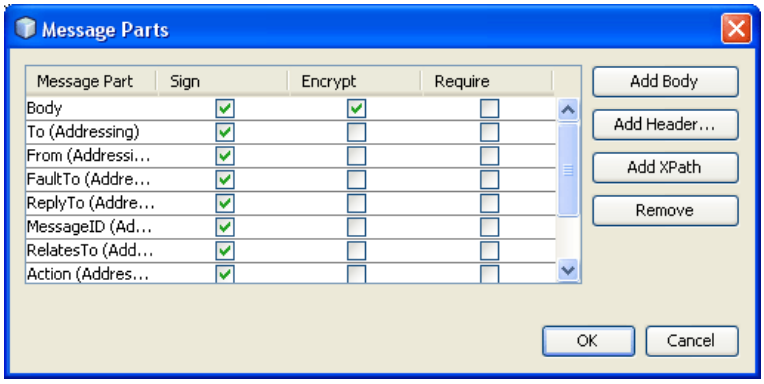
Índice

En la sección anterior vimos los diferentes mecanismos de seguridad a nivel de transporte que podemos configurar con Netbeans. Vamos a pasar ahora a ver los mecanismos de seguridad a nivel de mensaje. Cuando seleccionemos uno de estos últimos podremos configurar qué partes concretas del mensaje queremos que sean cifradas y firmadas. Esto lo haremos en la parte inferior de la ventana de edición de los atributos del servicio, en la que podemos especificar la configuración para cada mensaje concreto utilizado en el servicio:



Seguridad en las operaciones.

Pulsando sobre el botón *Message Parts ...* podremos configurar qué partes del mensaje queremos cifrar y cuales queremos firmar. Aquellas que sólo estén firmadas podrán ser vistas por cualquiera, pero no alteradas (se protege su integridad), mientras que las que estén cifradas tampoco podrán ser leídas sin permiso (se protege su confidencialidad). Como es evidente, está opción no está disponible cuando se utiliza seguridad a nivel de transporte.



Partes del mensaje.

A continuación veremos con mayor detalle cómo utilizar cada uno de los principales mecanismos de seguridad a nivel de mensajes.

1. Seguridad a nivel de mensaje con clave asimétrica

El primer mecanismo que veremos es el que nos proporciona confidencialidad e integridad mediante clave asimétrica.

Vamos a crear un nuevo servicio de nombre `ServicioMutual` en un nuevo proyecto web. Como mecanismo de seguridad seleccionamos *Mutual Certificates Security* y dejamos los valores por defecto.

```
public class ServicioMensajeMutual {
    @Resource
    private WebServiceContext context;

    @WebMethod(operationName = "consulta")
    public String consulta() {
      return "Accediendo con clave asimetrica " +
                context.getUserPrincipal().getName();
    }
}
```

Como vemos en el código, podemos obtener los datos del certificado utilizado por el cliente mediante el método `getUserPrincipal()`, con lo cual dicho certificado, además de proteger el mensaje de petición, nos puede servir para autentificar al cliente.

En este caso deberemos configurar *Keystore* y *Truststore* tanto en el cliente como en el servicio. Ambos deben confiar en el certificado utilizado por el otro extremo.

El WSDL obtenido será como el siguiente:

```
<definitions xmlns="http://...">
  <message name="consulta"/>
  <message name="consultaResponse"/>
  <portType name="ServicioMutual">
    <operation name="consulta">
      <input message="tns:consulta"/>
      <output message="tns:consultaResponse"/>
    </operation>
  </portType>
  <binding name="ServicioMutualPortBinding"
              type="tns:ServicioMutual">
    <wsp:PolicyReference URI="#ServicioMutualPortBindingPolicy"/>
    <operation name="consulta">
      <input>
        <wsp:PolicyReference URI=
                "#ServicioMutualPortBinding_consulta_Input_Policy"/>
      </input>
      <output>
        <wsp:PolicyReference URI=
                "#ServicioMutualPortBinding_consulta_Output_Policy"/>
      </output>
    </operation>
  </binding>
  <service name="ServicioMutualService">
    <port name="ServicioMutualPort"
```

```
                binding="tns:ServicioMutualPortBinding"/>
</service>
<wsp:Policy wsu:Id="ServicioMutualPortBindingPolicy">
  <wsp:ExactlyOne>
    <wsp:All>
      <wsam:Addressing wsp:Optional="false"/>
      <sp:AsymmetricBinding>
        <wsp:Policy>
          <sp:InitiatorToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken=
                     ".../IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:InitiatorToken>
          <sp:RecipientToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken=
                     ".../IncludeToken/Never">
                <wsp:Policy>
                  <sp:WssX509V3Token10/>
                  <sp:RequireIssuerSerialReference/>
                </wsp:Policy>
              </sp:X509Token>
            </wsp:Policy>
          </sp:RecipientToken>
          <sp:Layout>
            <wsp:Policy>
              <sp:Strict/>
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp/>
          <sp:OnlySignEntireHeadersAndBody/>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic128/>
            </wsp:Policy>
          </sp:AlgorithmSuite>
        </wsp:Policy>
      </sp:AsymmetricBinding>
      <sp:Wss10>
        <wsp:Policy>
          <sp:MustSupportRefIssuerSerial/>
        </wsp:Policy>
      </sp:Wss10>
      <sc:KeyStore wspp:visibility="private"
                   location=".../keystore.jks"
                   type="JKS" storepass="changeit"
                   alias="xws-security-server"/>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
<wsp:Policy wsu:Id=
        "ServicioMutualPortBinding_consulta_Input_Policy">
  <wsp:ExactlyOne>
    <wsp:All>
```

```
        <sp:EncryptedParts>
          <sp:Body/>
        </sp:EncryptedParts>
        <sp:SignedParts>
          <sp:Body/>
          <sp:Header Name="To" Namespace="http://..."/>
          <sp:Header Name="From" Namespace="http://..."/>
          <sp:Header Name="FaultTo" Namespace="http://..."/>
          <sp:Header Name="ReplyTo" Namespace="http://..."/>
          <sp:Header Name="MessageID" Namespace="http://..."/>
          <sp:Header Name="RelatesTo" Namespace="http://..."/>
          <sp:Header Name="Action" Namespace="http://..."/>
          <sp:Header Name="AckRequested" Namespace="http://..."/>
          <sp:Header Name="SequenceAcknowledgement"
                     Namespace="http://..."/>
          <sp:Header Name="Sequence" Namespace="http://..."/>
          <sp:Header Name="CreateSequence" Namespace="http://..."/>
        </sp:SignedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy
wsu:Id="ServicioMutualPortBinding_consulta_Output_Policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:EncryptedParts>
          <sp:Body/>
        </sp:EncryptedParts>
        <sp:SignedParts>
          <sp:Body/>
          <sp:Header Name="To" Namespace="http://..."/>
          <sp:Header Name="From" Namespace="http://..."/>
          <sp:Header Name="FaultTo" Namespace="http://..."/>
          <sp:Header Name="ReplyTo" Namespace="http://..."/>
          <sp:Header Name="MessageID" Namespace="http://..."/>
          <sp:Header Name="RelatesTo" Namespace="http://..."/>
          <sp:Header Name="Action" Namespace="http://..."/>
          <sp:Header Name="AckRequested" Namespace="http://..."/>
          <sp:Header Name="SequenceAcknowledgement"
                     Namespace="http://..."/>
          <sp:Header Name="Sequence" Namespace="http://..."/>
          <sp:Header Name="CreateSequence" Namespace="http://..."/>
        </sp:SignedParts>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
</definitions>
```

Podemos observar que para la protección de los mensajes se utilizan dos certificados, uno del cliente al servidor (`InitiatorToken`), que se incluye en los mensajes de petición, y otro del servidor al cliente (`RecipientToken`), que no se incluye en el mensaje de respuesta, sólo se utiliza para cifrarlo y firmarlo. Debemos destacar también la configuración de las partes del mensaje que deben ser cifradas y firmadas.

Respecto al cliente, en este caso no especificaremos la dirección segura, ya que la seguridad no va a nivel de transporte, sino dentro del mensaje XML. Crearemos la referencia al servicio, y una vez hecho esto activaremos la casilla *Use development*

defaults en su configuración para utilizar los certificados por defecto.

> **Nota**
>
> Podemos crear el cliente tanto en un proyecto web como en un proyecto Java, pero si lo hacemos en uno del segundo tipo deberemos especificar manualmente la ruta del *Keystore* y el *Truststore* en la ventana de edición de atributos del servicio, ya que si marcamos *Use development defaults* no funcionará correctamente.

Al invocar el servicio podemos observar los mensajes SOAP utilizados:

```
<S:Envelope xmlns:S="http://...">
<S:Header>
  <To xmlns="http://..." wsu:Id="_5005">
    http://localhost:8080/ServicioMensaje/ServicioMutualService
  </To>
  <Action xmlns="http://..." wsu:Id="_5004">
    http://.../ServicioMutual/consultaRequest
  </Action>
  <ReplyTo xmlns="http://..." wsu:Id="_5003">
    <Address>
      http://www.w3.org/2005/08/addressing/anonymous
    </Address>
  </ReplyTo>
  <MessageID xmlns="http://..." wsu:Id="_5002">
    uuid:354aef29-6462-7a39-85ce-45ae6f7ee65a0<
  /MessageID>
  <wsse:Security S:mustUnderstand="1">
    <wsu:Timestamp xmlns:ns18="http://..." wsu:Id="_3">
      <wsu:Created>2010-05-23T18:00:08Z</wsu:Created>
      <wsu:Expires>2010-05-23T18:05:08Z</wsu:Expires>
    </wsu:Timestamp>
    <wsse:BinarySecurityToken xmlns:ns18="http://..."
      ValueType="http://...#X509v3"
      EncodingType="http://...#Base64Binary"
      wsu:Id="uuid_b677ed4f-9c99-44f6-bbad-0978edb92b40">
        MIIDDzCCAnigAwIBAgIBAzANBgkqhkiG9w0BAQQFADBOMQswC
        QYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEMMAoGA1
        UEChMDU1VOMQwwCgYDVQQLEwNKV1MxDjAMBgNVBAMTBVNVTkN
        BMB4XDTA3MDMxMjEwMjQ0MFoXDTE3MDMwOTEwMjQ0MFowbzEL
        MAkGA1UEBhMCQVUxEzARBgNVBAgTClNvbWUtU3RhdGUxITAfB
        gNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEMMAoGA1
        UECxMDU1VOMRowGAYDVQQDExF4d3NzZWN1cml0eWNsaWVudDC
        BnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvYxVZKIzVdGM
        SBkW4bYnV80MV/RgQKV1bf/DoMTX8laMO45P6rlEarxQiOYrg
        zuYp+snzz2XM0S6o3JGQtXQuzDwcwPkH55bHFwHgtOMzxG4SQ
        653a5Dzh04nsmJvxvbncNH/XNaWfHaC0JHBEfNCMwRebYocxY
        M92pq/G5OGyECAwEAAaOB2zCB2DAJBgNVHRMEAjAAMCwGCWCG
        SAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY
        2F0ZTAdBgNVHQ4EFgQU/mItfvuFdS7A0GCysE71TFRxP2cwfg
        YDVR0jBHcwdYAUZ7plxs6VyOOOTSFyojDV0/YYjJWhUqRQME4
        xCzAJBgNVBAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMQww
        CgYDVQQKEwNTVU4xDDAKBgNVBAsTA0pXUzEOMAwGA1UEAxMFU
        1VOQ0GCCQDbHkJaq6KijjANBgkqhkiG9w0BAQQFAAOBgQBEnR
        dcQeMyCYqOHw2jbPOPUlvu07bZe7sI3ly/Qz+4mkrFctqMSup
        ghQtLv9dZcqDOUFLCGMse7+l5MG00VawzsoVe242iXzJB111e
        PzhhppIPOHXXtflj/JD2U4Qz75C/dfdd5AAZbqGSFtZh7pyE8
```

```
        Ot1vOq7R48/bHuvTsEVUQ==
    </wsse:BinarySecurityToken>
    <xenc:EncryptedKey xmlns:ns18="http://..." Id="_5007">
      <xenc:EncryptionMethod Algorithm="...#rsa-oaep-mgf1p" />
      <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
                CN=SUNCA, OU=JWS, O=SUN, ST=Some-State, C=AU
              </ds:X509IssuerName>
              <ds:X509SerialNumber>2</ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>
          qLpnzKy7zN+BvmXKzjf3a9yEtSjCaVokncdMEgdDucSlN74c2
          zgAtwmM2ogLnawQeb8ivAdJUcJ7Tg2ycw9WpRLdWLgM+H5AMe
          Ov+uP5eOmbqyg7efU3dbceeRHryu7FlTzlcTjB7DKse+Br/WK
          4XB8/hpZqwWzU7NGhwXuKJAA=
        </xenc:CipherValue>
      </xenc:CipherData>
      <xenc:ReferenceList>
        <xenc:DataReference URI="#_5008" />
      </xenc:ReferenceList>
    </xenc:EncryptedKey>
    <ds:Signature xmlns:ns18="http://..." Id="_1">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsse S" />
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="http://...#rsa-sha1" />
        <ds:Reference URI="#_5002">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            VJ7xOBhR0+zNqQZ5nifkt256OEo=<
          /ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5003">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            bfaj3tu9jIeOXTrb3JWtYD+ZKaI=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5004">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
```

```
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://...#sha1" />
        <ds:DigestValue>
          uttcPe+iu2U8bUrV5nJXV7TkzdM=<
        /ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5005">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://...#sha1" />
        <ds:DigestValue>
          J1Y7KigJGj9VauXK+72979jeKm0=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5006">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://...#sha1" />
        <ds:DigestValue>
          43t9/SfIxwT3HdGSmGsj5KD1HPI=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_3">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces
                    PrefixList="wsu wsse S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://...#sha1" />
        <ds:DigestValue>
          Hjt5KqWuPkRvjG8lDvK39UUqNyE=
        </ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      kjGN6PdD9WJ5FN9EkHCOPW8m2cU96I+UsH8vHsjGZt+eOXWAR
      INwiCVhKIxpBIORpQF2qbEuxyNEe9I2Md/KFBepytlSuHEqgm
      0IOHtzq9NyBvLoZi9bCGpqITH3VMcOYotNOyGLaBP8ZxJpFyo
      HW5TXaa8JhsUN8/yHhoLKu/8=
    </ds:SignatureValue>
    <ds:KeyInfo>
      <wsse:SecurityTokenReference>
        <wsse:Reference
               URI="#uuid_b677ed4f-9c99-44f6-bbad-0978edb92b40"
               ValueType="http://...#X509v3" />
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
 </wsse:Security>
</S:Header>
```

```
<S:Body wsu:Id="_5006">
  <xenc:EncryptedData xmlns:ns18="http://..." Id="_5008"
        Type="http://...#Content">
    <xenc:EncryptionMethod Algorithm="http://...#aes128-cbc" />
    <xenc:CipherData>
      <xenc:CipherValue>
        r6LQcfvjYdOzCrgVgFar7poLAuC7PrS3L3bCIW3kJT6V8ench
        grxRyBbAW3/SPRz7fHl+F4ztuYVQJNCMEJEXc+7kbN+Alsx33
        E7g3tYHXJnIij1dg4JFiN5Hd0HEGZVkJbSfNAMboSECeRocug
        +rw==
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

Para poder entender mejor el contenido del mensaje, a continuación mostramos una tabla con los números de referencia a las diferentes partes del mensaje:

Identificador	Parte
_1	Firma
_3	Timestamp
_5002	MessageID
_5003	ReplyTo
_5004	Action
_5005	To
_5006	Body
_5007	Clave de cifrado
_5008	Contenido de body
uuid_b677ed4f-9c99-44f6-bbad-0978edb9	Certificado cliente adjunto

Podemos observar que el certificado digital del cliente se adjunta al mensaje como un *token* binario sin cifrar (sólo va codificado en base64). Todas las partes que habíamos indicado que debían ser firmadas (Body, To, Action, ReplyTo, MessageID), además del *timestamp*, tienen una referencia dentro del bloque `Signature` y son firmadas utilizando el certificado adjunto.

La clave de cifrado hace referencia al certificado `xws-security-server` (con serial 2), no incluido en el mensaje. En las referencias a los elementos cifrados con dicha clave, encontramos únicamente el contenido del *body*.

```
<S:Envelope xmlns:S="http://...">
<S:Header>
  ...
  <wsse:Security S:mustUnderstand="1">
    <wsu:Timestamp xmlns:ns18="http://..." wsu:Id="_3">
```

```
      <wsu:Created>2010-05-23T18:00:08Z</wsu:Created>
      <wsu:Expires>2010-05-23T18:05:08Z</wsu:Expires>
    </wsu:Timestamp>
    <xenc:EncryptedKey xmlns:ns18="http://..." Id="_5007">
      <xenc:EncryptionMethod Algorithm="...#rsa-oaep-mgf1p" />
      <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
                CN=SUNCA, OU=JWS, O=SUN, ST=Some-State, C=AU
              </ds:X509IssuerName>
              <ds:X509SerialNumber>3</ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>
          DnxD0Fu2xNcNk8au998ylCRAkOPY+KFudhsSs+QNF5dWbFD4S
          fvjCzHB3iJeQX3tkurJL2bPGq281Hls6FbditXDXBIk/4o5dQ
          41meZyG+lYFXxCW+Cuh8tuGWeplYXvMOkx0T1hATB9HZGJ5pY
          +Fg4H4DK5zlaG6B3qQdfcxmQ=
        </xenc:CipherValue>
      </xenc:CipherData>
      <xenc:ReferenceList>
        <xenc:DataReference URI="#_5008" />
      </xenc:ReferenceList>
    </xenc:EncryptedKey>
    <ds:Signature xmlns:ns18="http://..." Id="_1">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsse S" />
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="http://...#rsa-sha1" />
        <ds:Reference URI="#_5002">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            2rnnF8g6/xFtlou99Yw7Mshc+VM=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5003">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            58qBSPkSlKEHfItEQno4nB2eQ7E=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5004">
          <ds:Transforms>
```

```
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            1dDaYsdB4xzlVr/IbynlFIwf5Vw=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5005">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            Nd/8wVmBdLowQKMblBRYK+6xcjA=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5006">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            HF0FrQEUpM98NXkdncg+e6HJm7c=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_3">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces
                        PrefixList="wsu wsse S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            Hjt5KqWuPkRvjG8lDvK39UUqNyE=
          </ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
        LZ7ti/S7lj5Sgej8Mfy0JTWkf9idLYmt0K8y8//RdZTSyexii
        fKo4HVC2HeW3GVFOGlXX/aJkYhH1LGEfWUUB+LOa04OfyP4HB
        iuebmxzlK4d3vN6gUFUCEJeKMLpgaygGs67qu36aMygE96q36
        1ncdh8mY3YACNLpISz+GfRII=
      </ds:SignatureValue>
      <ds:KeyInfo>
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
                CN=SUNCA, OU=JWS, O=SUN, ST=Some-State, C=AU
              </ds:X509IssuerName>
              <ds:X509SerialNumber>2</ds:X509SerialNumber>
            </ds:X509IssuerSerial>
```

```
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wsse:Security>
</S:Header>
<S:Body wsu:Id="_5006">
  <xenc:EncryptedData xmlns:ns18="..." Id="_5008"
                      Type="...#Content">
    <xenc:EncryptionMethod Algorithm="http://...#aes128-cbc" />
    <xenc:CipherData>
      <xenc:CipherValue>
        9ipfQQOlCZAs13DuGqBIWrbczNZZdubh4Uy3lz3ccEiGm6mj8
        kTbi6echVZCKDH7SGK+XwBb8ocICTrrdOPFZ3VEInHgtfAAKA
        t9+Km4Y1eBPz9jiWZrpyjh+qphkm86CL/VDVeSiE+RKU+QFQe
        JQEe7G75yTKeXRUM5tqbvZD5zpRye4q/kOX1R6QTGiJnxD2+M
        ThielTK78FUzCfjKAdkF3rDxNuD1IZhZdKtYtm7JuYxpLwcg7
        TjCPpBOVKqZC96NXr7k8OfBT8BOmkzVf4Sqqc1sijnACAou47
        I6jikUAiT74P3FHz2Y+c1gBwQcXQQwP87C0t64WbLePJTPVQ=
        =
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

El mensaje de respuesta es similar al de petición, pero en este caso no se incluye ningún certificado con el mensaje. Ambos certificados son únicamente referenciados. La firma se realiza utilizando el certificado del servidor (`xws-security-server`, con serial 2), mientras que la clave de cifrado para el *body* proviene del certificado del cliente (`xws-security-client`, con serial 3).

2. Clave simétrica y autentificación mediante nombre de usuario

Podemos también utilizar autentificación mediante nombre de usuario y password con seguridad a nivel de mensaje. Para utilizar este tipo de seguridad deberemos seleccionar la opción *Username Authentication with Symmetric Key*. Vamos a crear un servicio de nombre `ServicioMensajeUsername` con dicho tipo de seguridad.

El cliente, al igual que en los casos anteriores, se puede crear tanto en un proyecto web como en un proyecto Java independiente. La protección del mensaje se realizará mediante clave simétrica, utilizando el certificado del servidor. Por lo tanto, deberemos especificar el *Keystore* en el servidor y el *Truststore* en el cliente.

La configuración de los usuarios se realiza tal como vimos en la sección anterior, en el caso de seguridad a nivel de transporte con autentificación mediante nombre de usuario. Podremos utilizar el *realm* por defecto de Glassfish o de la aplicación *enterprise*, o bien definir nuestro propio mecanismo de validación mediante *handlers* o *validators*. De la misma forma, en el cliente podremos realizar la autentificación de forma estática o dinámica (sólo en aplicaciones Java independientes).

En este caso el WSDL será el siguiente:

```
<definitions  xmlns="http://...">
  ...
  <wsp:Policy wsu:Id="ServicioMensajeUsernamePortBindingPolicy">
    <wsp:ExactlyOne>
      <wsp:All>
        <wsam:Addressing wsp:Optional="false"/>
        <sp:SymmetricBinding>
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token sp:IncludeToken=
                              ".../IncludeToken/Never">
                  <wsp:Policy>
                    <sp:WssX509V3Token10/>
                    <sp:RequireIssuerSerialReference/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict/>
              </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp/>
            <sp:OnlySignEntireHeadersAndBody/>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic128/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
          </wsp:Policy>
        </sp:SymmetricBinding>
        <sp:Wss11>
          <wsp:Policy>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:SignedEncryptedSupportingTokens>
          <wsp:Policy>
            <sp:UsernameToken sp:IncludeToken=
                              ".../IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssUsernameToken10/>
              </wsp:Policy>
            </sp:UsernameToken>
          </wsp:Policy>
        </sp:SignedEncryptedSupportingTokens>
        <sc:KeyStore wspp:visibility="private"
                     location=".../keystore.jks"
                     type="JKS" storepass="changeit"
                     alias="xws-security-server"/>
      </wsp:All>
    </wsp:ExactlyOne>
```

```
  </wsp:Policy>
  <wsp:Policy wsu:Id=
      "ServicioMensajeUsernamePortBinding_consulta_Input_Policy">
    ... (partes del mensaje de entrada) ...
  </wsp:Policy>
  <wsp:Policy wsu:Id=
      "ServicioMensajeUsernamePortBinding_consulta_Output_Policy">
    ... (partes del mensaje de salida) ...
  </wsp:Policy>
</definitions>
```

Observamos que en este caso se utiliza una clave simétrica generada a partir del certificado del servidor. En este caso sólo es necesario especificar un *token* para la protección de los mensajes, aunque podríamos haber especificado por separado un *token* para firmar y otro para cifrar.

Además del *token* de protección, se especifica un *token* adicional de soporte, en este caso de tipo *username*, que estará firmado y cifrado, y se incluirá siempre en los mensajes del cliente al servicio (`AlwaysToRecipent`).

A continuación mostramos los mensajes SOAP utilizados en la invocación de este servicio. El mensaje de la petición SOAP es:

```
<S:Envelope xmlns:S="http://...">
<S:Header>
...
<wsse:Security S:mustUnderstand="1">
  <wsu:Timestamp xmlns:ns19="http://..." wsu:Id="_3">
    <wsu:Created>2010-05-23T19:20:04Z</wsu:Created>
    <wsu:Expires>2010-05-23T19:25:04Z</wsu:Expires>
  </wsu:Timestamp>
  <xenc:EncryptedKey xmlns:ns19="http://..." Id="_5002">
    <xenc:EncryptionMethod Algorithm="...#rsa-oaep-mgf1p" />
    <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
      <wsse:SecurityTokenReference>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>
              CN=SUNCA, OU=JWS, O=SUN, ST=Some-State, C=AU
            </ds:X509IssuerName>
            <ds:X509SerialNumber>2</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
        </ds:X509Data>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        cJ9Y9zo7YnQZZWxJn7CVv4w+w83EqqhPhgO4lUDTF/VDh92GyhyC
        UcCzWPGxyQT8533unHVZAyCFDAr7EB+1pqxibVbOWXwBrSh6VfQB
        hbe2L3E6VKF8u3ttHoe5ZW31CZTIbl316nQgjOjkVrToPFM90Jez
        vavRLvYqZxJfHag=
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedKey>
  <xenc:ReferenceList xmlns:ns19="http://...">
    <xenc:DataReference URI="#_5008" />
    <xenc:DataReference URI="#_5009" />
```

```
  </xenc:ReferenceList>
  <xenc:EncryptedData xmlns:ns19="http://..." Id="_5009"
                      Type="...#Element">
    <xenc:EncryptionMethod Algorithm="...#aes128-cbc" />
    <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
      <wsse:SecurityTokenReference>
        <wsse:Reference URI="#_5002"
                        ValueType="http://...#EncryptedKey" />
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        R4YsNK1vHBPM42ETnn222yExp6Nr1qu/WFGNEl8tLnNbBb4rtVrh
        Uek5neUsUR/WcvaP8JQWSu4f6IZH8IUnoonJeSWGgNeEy9053EM1
        aZB8CJd7DvLy8GgdxmaEilP3no6i3jTwqYFoPtJRA//CxkxOiVug
        oCdBhKa5OvXs89QtqhBzMiF8tqpX476kf9EKU3t9uLUHETBr80kP
        qa1FzVUz3+w4LZvy8HUw5kb3lAMaDu+m6yUv0H1r9WJJbJRSZf74
        xspWE1gZE15OoXk82Ns4gScJtJwNa3YKfYbTrUNP/4nLlN8+Ihi6
        phitoXP/uZ34zOogz14lKvXbR1mxd40UOiCoFMCE4hRAJsUloNmm
        Eiot++ydIAfb1qw+MDB2zHhCQxoMSFgbHdf7Rjgr+PJ81WCm7Hn4
        2HuJT0DEyFK4Y/mfq9Ex4y0ple7n/nAHQIm/aZIDwScvE07m5BJJ
        Bo0edABoMX6S51tU+f8A+E5tQSLN9QZXqxYL3izy18pGpRUKraow
        5ml14GNW7lBwmp3WpneNZznDChLNzQ6hJdIt2HaBx9Vs23JwLTrP
        0i/6xJcEJ8zmF/2rP9sq0w8pepVh1NJfx/z25uMVapzciAQz3Yvp
        kY5oZckPOJlJi6n5
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
  <ds:Signature xmlns:ns19="http://..." Id="_1">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://...">
        <exc14n:InclusiveNamespaces PrefixList="wsse S" />
      </ds:CanonicalizationMethod>
      <ds:SignatureMethod Algorithm="...#hmac-sha1" />
      <ds:Reference URI="#_5003">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          pE4UXA2w8RSM1d1XmS+Ek5xinHQ=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5004">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          5Ab1ebo4/FraGgck/A8iDx1J9+I=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5005">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
```

```
          <exc14n:InclusiveNamespaces PrefixList="S" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="...#sha1" />
      <ds:DigestValue>
        VfeAGSW+zTgOT5D/JmzLBWmVPlM=
      </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_5006">
      <ds:Transforms>
        <ds:Transform Algorithm="http:/...">
          <exc14n:InclusiveNamespaces PrefixList="S" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="...#sha1" />
      <ds:DigestValue>
        ss8hoyoJzzXVHnrHV6xLXhFGydA=
      </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_5007">
      <ds:Transforms>
        <ds:Transform Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="S" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://...#sha1" />
      <ds:DigestValue>
        99CKXPmV+EAk0iuMs/zYlfgLhVE=
      </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#_3">
      <ds:Transforms>
        <ds:Transform Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsu wsse S" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://...#sha1" />
      <ds:DigestValue>
        U+ucDGRQ8NA16rxMWqeuF+gVj8g=
      </ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI=
                  "#uuid_f8b964eb-a74e-453d-9141-b9b082a8e8ca">
      <ds:Transforms>
        <ds:Transform Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsu wsse S" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="...#sha1" />
      <ds:DigestValue>
        a26JKFN1L1RZgyqVT/o5rWdHd3I=
      </ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    +bBujAT6fa61vvvztbmpcdKVsP4=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <wsse:SecurityTokenReference wsu:Id=
```

```
                "uuid_f1e1388d-533b-46b6-a108-8071c9ef71e7">
        <wsse:Reference URI="#_5002" ValueType="...#EncryptedKey"/>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
</S:Header>
<S:Body wsu:Id="_5007">
  <xenc:EncryptedData xmlns:ns19="http://s..." Id="_5008"
                      Type="...#Content">
    <xenc:EncryptionMethod Algorithm="...#aes128-cbc" />
    <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
      <wsse:SecurityTokenReference>
        <wsse:Reference URI="#_5002" ValueType="...#EncryptedKey"/>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        gf727dxKqy9VMKI1KqGvI9KXQ034/JKu7dkoVdXGprMnCLCjn0
        sdH98+2WuNC20A68CRWpNbpxuLPhFaGmp9HgGsCQ0aUBOzAtem
        v11z1aC2bVzYks6djxuH6mN9kWM+DOxaJ3uFjfBT0qFO18pv3A
        ==
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

Al igual que en el caso anterior, para facilitar el análisis del mensaje mostramos una tabla con los identificadores de cada parte del mensaje:

Identificador	Parte
_1	Firma
_3	Timestamp
_5002	Clave de cifrado
_5003	MessageID
_5004	ReplyTo
_5005	Action
_5006	To
_5007	Body
_5008	Contenido de body
_5009	Username token

En este caso la clave de cifrado utilizada es simétrica, obtenida a partir del certificado del servidor. Además, en las referencias de dicha clave podemos ver que no se utiliza únicamente para cifrar el *body*, sino que también ciframos el nombre de usuario y *password* con ella. El mismo certificado del servidor es el que se utiliza para firmar el

mensaje.

La respuesta SOAP será:

```
<S:Envelope xmlns:S="http://...">
<S:Header>
...
<wsse:Security S:mustUnderstand="1">
  <wsu:Timestamp xmlns:ns19="http://..." wsu:Id="_3">
    <wsu:Created>2010-05-23T19:20:05Z</wsu:Created>
    <wsu:Expires>2010-05-23T19:25:05Z</wsu:Expires>
  </wsu:Timestamp>
  <xenc:ReferenceList xmlns:ns19="http://..." >
    <xenc:DataReference URI="#_5007" />
  </xenc:ReferenceList>
  <ds:Signature xmlns:ns19="http://..." Id="_1">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://...">
        <exc14n:InclusiveNamespaces PrefixList="wsse S" />
      </ds:CanonicalizationMethod>
      <ds:SignatureMethod Algorithm="...#hmac-sha1" />
      <ds:Reference URI="#_5002">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          o6eUIKrRYD2O32Q3yWJ3g42fPV8=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5003">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          ADxMEggWbANO309HVnpH081Q+Hg=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5004">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          qAOp4yOgxgo6yh+MYDMtxAGv1DY=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5005">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
```

```
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          Nd/8wVmBdLowQKMblBRYK+6xcjA=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_5006">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          2Pl8qsA04TDbGSzjFf4UbnhgUno=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_3">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="wsu wsse S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://...#sha1" />
        <ds:DigestValue>
          UK949xG3qaQb5tqhUFSHfAZwbWo=
        </ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      cmEXxN18qmrn81H2RmxEyRwHfqA=
    </ds:SignatureValue>
    <ds:KeyInfo>
      <wsse:SecurityTokenReference>
        <wsse:KeyIdentifier ValueType="...#EncryptedKeySHA1"
                            EncodingType="...#Base64Binary">
          d7BpVKn2Tm6oly/Yx8SUmOfl6FA=
        </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
</S:Header>
<S:Body wsu:Id="_5006">
<xenc:EncryptedData xmlns:ns19="http://..." Id="_5007"
                    Type="http://...#Content">
  <xenc:EncryptionMethod Algorithm="http://...#aes128-cbc" />
  <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
    <wsse:SecurityTokenReference>
      <wsse:KeyIdentifier ValueType="http://...#EncryptedKeySHA1"
                          EncodingType="...#Base64Binary">
        d7BpVKn2Tm6oly/Yx8SUmOfl6FA=
      </wsse:KeyIdentifier>
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
  <xenc:CipherData>
    <xenc:CipherValue>
      RffDq+mrIkGgrZzjctW6sVvsGTVPEwTMzkvlt5Dx/qBrcpRbT+V
      op+BJfvm3skdhl6zcGCLiD+G6Z2K/CCvaxBHT7d+pZ8yq10Nye7
```

```
      dqxurQVdji4k7jrVCyboRDYzUSl3EejzRpYN0FoyrzsLGYf2H+X
      OfpmmzDimvnXUBxQmzYIlDTlXW4Vu3PklB4MrCs4xzBtz4tSoCQ
      2UKQ+3oBz1cwqLsmqsQLYg+V/1ZJGQQ=
    </xenc:CipherValue>
  </xenc:CipherData>
</xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

En el mensaje de respuesta, dentro del *body*, podemos ver como en este caso se especifica una referencia a la clave simétrica generada anteriormente por el certificado del servidor. Esta misma clave se utiliza también para la firma del mensaje.

3. Clave simétrica y autentificación mediante certificado digital

Vamos a ver ahora cómo utilizar seguridad a nivel de mensaje con clave simétrica, utilizando el certificado del servidor, y autentificación mediante el certificado del cliente.

Crearemos un nuevo servicio de nombre `ServicioMensajeCert` con el tipo de seguridad *Endorsing Certificate*. Deberemos configurar *Keystore* y *Truststore* tanto en el cliente como en el servidor. El certificado configurado en el servidor se utilizará para la protección de los mensajes, y el del cliente para autentificación. Cada extremo debe confiar en el certificados del otro.

En este caso el WSDL será el siguiente:

```
<definitions xmlns="http://...">
  ...
  <wsp:Policy wsu:Id="ServicioMensajeCertPortBindingPolicy">
    <wsp:ExactlyOne>
      <wsp:All>
        <wsam:Addressing wsp:Optional="false"/>
        <sp:SymmetricBinding>
          <wsp:Policy>
            <sp:ProtectionToken>
              <wsp:Policy>
                <sp:X509Token sp:IncludeToken=
                              ".../IncludeToken/Never">
                  <wsp:Policy>
                    <sp:WssX509V3Token10/>
                    <sp:RequireIssuerSerialReference/>
                  </wsp:Policy>
                </sp:X509Token>
              </wsp:Policy>
            </sp:ProtectionToken>
            <sp:Layout>
              <wsp:Policy>
                <sp:Lax/>
              </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp/>
            <sp:OnlySignEntireHeadersAndBody/>
            <sp:AlgorithmSuite>
              <wsp:Policy>
```

```
                <sp:Basic128/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
          </wsp:Policy>
        </sp:SymmetricBinding>
        <sp:Wss11>
          <wsp:Policy>
            <sp:MustSupportRefIssuerSerial/>
            <sp:MustSupportRefThumbprint/>
            <sp:MustSupportRefEncryptedKey/>
          </wsp:Policy>
        </sp:Wss11>
        <sp:EndorsingSupportingTokens>
          <wsp:Policy>
            <sp:X509Token sp:IncludeToken=
                          ".../IncludeToken/AlwaysToRecipient">
              <wsp:Policy>
                <sp:WssX509V3Token10/>
              </wsp:Policy>
            </sp:X509Token>
          </wsp:Policy>
        </sp:EndorsingSupportingTokens>
        <sc:KeyStore wspp:visibility="private"
                     location=".../keystore.jks"
                     type="JKS" storepass="changeit"
                     alias="xws-security-server"/>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id=
        "ServicioMensajeCertPortBinding_consulta_Input_Policy">
    ... (partes del mensaje de entrada) ...
  </wsp:Policy>
  <wsp:Policy wsu:Id=
        "ServicioMensajeCertPortBinding_consulta_Output_Policy">
    ... (partes del mensaje de salida) ...
  </wsp:Policy>
</definitions>
```

En este caso el WSDL es similar al anterior, con la diferencia de que el *token* de soporte es de tipo X509, en lugar de *username*. Además, en lugar de incluirse firmado y cifrado (`SignedEncrypted`), se incluye como *token* de respaldo (`Endorsing`). En este caso lo que se hará es utilizar este *token* de soporte para firmar la firma que se había obtenido mediante el *token* de protección.

Para ver esto de forma más clara, mostramos los mensajes SOAP utilizados a continuación. Comenzamos viendo la petición SOAP:

```
<S:Envelope xmlns:S="http://...">
<S:Header>
  <To xmlns="http://..." wsu:Id="_5006">
    http://.../ServicioMensaje/ServicioMensajeCertService
  </To>
  <Action xmlns="http://..." wsu:Id="_5005">
    http://...jtech.ua.es/ServicioMensajeCert/consultaRequest
  </Action>
  <ReplyTo xmlns="http://..." wsu:Id="_5004">
```

```
  <Address>http://...</Address>
</ReplyTo>
<MessageID xmlns="http://..." wsu:Id="_5003">
  uuid:21a5babb-9795-43d5-8cd6-32559a586fdb
</MessageID>
<wsse:Security S:mustUnderstand="1">
  <wsu:Timestamp xmlns:ns19="http://..." wsu:Id="_3">
    <wsu:Created>2010-05-23T19:24:21Z</wsu:Created>
    <wsu:Expires>2010-05-23T19:29:21Z</wsu:Expires>
  </wsu:Timestamp>
  <wsse:BinarySecurityToken xmlns:ns19="http://..."
        ValueType="http://..#X509v3"
        EncodingType="http://...#Base64Binary"
        wsu:Id="uuid_fa1f8f1a-6f4e-44d3-a037-7ec26f79adce">
    MIIDDzCCAnigAwIBAgIBAzANBgkqhkiG9w0BAQQFADBOM
    QswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZT
    EMMAoGA1UEChMDU1VOMQwwCgYDVQQLEwNKV1MxDjAMBgN
    VBAMTBVNVTkNBMB4XDTA3MDMxMjEwMjQ0MFoXDTE3MDMw
    OTEwMjQ0MFowbzELMAkGA1UEBhMCQVUxEzARBgNVBAgTC
    lNvbWUtU3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZG
    dpdHMgUHR5IEx0ZDEMMAoGA1UECxMDU1VOMRowGAYDVQQ
    DExF4d3NzZWN1cml0eWNsaWVudDCBnzANBgkqhkiG9w0B
    AQEFAAOBjQAwgYkCgYEAvYxVZKIzVdGMSBkW4bYnV80MV
    /RgQKV1bf/DoMTX8laMO45P6rlEarxQiOYrgzuYp+snzz
    2XM0S6o3JGQtXQuzDwcwPkH55bHFwHgtOMzxG4SQ653a5
    Dzh04nsmJvxvbncNH/XNaWfHaC0JHBEfNCMwRebYocxYM
    92pq/G5OGyECAwEAAaOB2zCB2DAJBgNVHRMEAjAAMCwGC
    WCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZX
    J0aWZpY2F0ZTAdBgNVHQ4EFgQU/mItfvuFdS7A0GCysE7
    1TFRxP2cwfgYDVR0jBHcwdYAUZ7plxs6VyOOOTSFyojDV
    0/YYjJWhUqRQME4xCzAJBgNVBAYTAkFVMRMwEQYDVQQIE
    wpTb21lLVN0YXRlMQwwCgYDVQQKEwNTVU4xDDAKBgNVBA
    sTA0pXUzEOMAwGA1UEAxMFU1VOQ0GCCQDbHkJaq6KijjA
    NBgkqhkiG9w0BAQQFAAOBgQBEnRdcQeMyCYqOHw2jbPOP
    Ulvu07bZe7sI3ly/Qz+4mkrFctqMSupghQtLv9dZcqDOU
    FLCGMse7+l5MG00VawzsoVe242iXzJB111ePzhhppIPOH
    XXtflj/JD2U4Qz75C/dfdd5AAZbqGSFtZh7pyE8Ot1vOq
    7R48/bHuvTsEVUQ==
  </wsse:BinarySecurityToken>
  <xenc:EncryptedKey xmlns:ns19="http://..." Id="_5002">
    <xenc:EncryptionMethod Algorithm="...#rsa-oaep-mgf1p"/>
      <ds:KeyInfo xmlns:xsi="http://..."
                  xsi:type="KeyInfoType">
        <wsse:SecurityTokenReference>
          <ds:X509Data>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>
                CN=SUNCA, OU=JWS, O=SUN, ST=Some-State, C=AU
              </ds:X509IssuerName>
              <ds:X509SerialNumber>
                2
              </ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        ZIbU04pW+0mzdrLeGC78ad+DzKGjofbIhukr924Jt
```

```
          NYzPg7gxLupVKPEYB0DGiedp+J5hDB6Q0yRbWKket
          kjZ3XoMJWuDvnk/JMUtlWLwibqA6tq4gfub2jmQKf
          sTY48jTLJLziNXc5UIjBj5QPlC4VWz2ZSc1Uf5bSl
          axFPjCQ=
        </xenc:CipherValue>
      </xenc:CipherData>
    </xenc:EncryptedKey>
    <xenc:ReferenceList xmlns:ns19="http://...">
      <xenc:DataReference URI="#_5008" />
    </xenc:ReferenceList>
    <ds:Signature xmlns:ns19="http://..." Id="_1">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsse S" />
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="...#hmac-sha1" />
        <ds:Reference URI="#_5003">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="...#sha1" />
          <ds:DigestValue>
            T0rfUv5gcSx9eZMTXxDa2xv+rMM=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5004">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="...#sha1" />
          <ds:DigestValue>
            5Ab1ebo4/FraGgck/A8iDx1J9+I=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5005">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="...#sha1" />
          <ds:DigestValue>
            jPtewJP1NvFyk7uaIJOi0hdDouQ=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5006">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="...#sha1" />
          <ds:DigestValue>
            nWiBqPMwYLCiyR4jQEnbXa44/MM=
          </ds:DigestValue>
```

```
      </ds:Reference>
      <ds:Reference URI="#_5007">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="S" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          dcuZ/1UF8eGNr9xozOlvJOhAHjg=
        </ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_3">
        <ds:Transforms>
          <ds:Transform Algorithm="http://...">
            <exc14n:InclusiveNamespaces PrefixList="wsu wsse S"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="...#sha1" />
        <ds:DigestValue>
          Grqal7NeOXnoSwl5karT8OxVVPU=
        </ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
  <ds:SignatureValue>
    oZWc+in3Z+fJT6Tfk1xEgA2tHcw=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <wsse:SecurityTokenReference
          wsu:Id="uuid_6d8b66f5-41bc-4864-b1b3-82748ba54942">
      <wsse:Reference URI="#_5002"
                     ValueType="http://...#EncryptedKey" />
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
</ds:Signature>
<ds:Signature xmlns:ns19="http://..." Id="_4">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://...">
      <exc14n:InclusiveNamespaces PrefixList="wsse S" />
    </ds:CanonicalizationMethod>
    <ds:SignatureMethod Algorithm="http://...#rsa-sha1" />
    <ds:Reference URI="#_1">
      <ds:Transforms>
        <ds:Transform Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsu wsse S" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://...#sha1" />
      <ds:DigestValue>
        MKpa+9VKUBcNYQg0DJnaGDTb2aA=
      </ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    udNJppNXruii7yt1wWmWG6+fjpxr9/h99qeX1eQdRFniP
    +c3bw0QJFNDpcyY9l9oGzdLNQWwu7T4HVs3ij7hMfoN0a
    M9nm0YtIzxwzIGjebUrII1Bc/8ZWipm9kt+AfesWeDjgn
    By+7yj6My9FHKJLJeAeIl06xGzMNJ4ZMBaD4=
  </ds:SignatureValue>
```

```
    <ds:KeyInfo>
      <wsse:SecurityTokenReference>
        <wsse:Reference
                  URI="#uuid_fa1f8f1a-6f4e-44d3-a037-7ec26f79adce"
                  ValueType="http://#X509v3" />
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
</S:Header>
<S:Body wsu:Id="_5007">
  <xenc:EncryptedData xmlns:ns19="http://..." Id="_5008"
                      Type="...#Content">
    <xenc:EncryptionMethod Algorithm="...#aes128-cbc" />
    <ds:KeyInfo xmlns:xsi="http://..." xsi:type="KeyInfoType">
      <wsse:SecurityTokenReference>
        <wsse:Reference URI="#_5002" ValueType="...#EncryptedKey"/>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        /XXPmN5H81ZbFg/5RZqRI3euKkKsqGJ+Chqob+wkYEV
        9WOz94vDU+2KEvCSymTM8NSMB7BoXiBUtP6E7cveScp
        NS475iL7OAhx6nKjiERXDW/Dk+I0s7JtYhyPMM7+T9
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

En este caso las partes del mensaje tienen las siguientes referencias:

Identificador	Parte
_1	Firma
_3	Timestamp
_4	Firma de respaldo
_5002	Clave de cifrado
_5003	MessageID
_5004	ReplyTo
_5005	Action
_5006	To
_5007	Body
_5008	Contenido de body
uuid_fa1f8f1a-6f4e-44d3-a037-7ec26f79	Certificado cliente adjunto

Podemos ver que el certificado del servidor (`xws-security-server`, con serial 2) se utiliza tanto para firmar como para cifrar el mensaje, al igual que ocurría en el caso

anterior. Sin embargo, vemos que hay una segunda firma, con identificador `_4`, que se encarga de firmar la primera (con identificador `_1`) utilizando para ello el certificado del cliente adjunto.

A continuación se muestra el mensaje de respuesta SOAP:

```
<S:Envelope xmlns:S="http://...">
<S:Header>
  <To xmlns="http://..." wsu:Id="_5005">
    http://www.w3.org/2005/08/addressing/anonymous
  </To>
  <Action xmlns="http://..." wsu:Id="_5003">
    http://...jtech.ua.es/ServicioMensajeCert/consultaResponse
  </Action>
  <MessageID xmlns="http://..." wsu:Id="_5002">
    uuid:135963b0-5c3f-450c-a901-103c4d813858
  </MessageID>
  <RelatesTo xmlns="http://..." wsu:Id="_5004">
    uuid:21a5babb-9795-43d5-8cd6-32559a586fdb
  </RelatesTo>
  <wsse:Security S:mustUnderstand="1">
    <wsu:Timestamp xmlns:ns19="http://..." wsu:Id="_3">
      <wsu:Created>2010-05-23T19:24:22Z</wsu:Created>
      <wsu:Expires>2010-05-23T19:29:22Z</wsu:Expires>
    </wsu:Timestamp>
    <xenc:ReferenceList xmlns:ns19="http://...">
      <xenc:DataReference URI="#_5007" />
    </xenc:ReferenceList>
    <ds:Signature xmlns:ns19="http://..." Id="_1">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://...">
          <exc14n:InclusiveNamespaces PrefixList="wsse S" />
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="...#hmac-sha1" />
        <ds:Reference URI="#_5002">
          <ds:Transforms>
            <ds:Transform Algorithm="...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="...#sha1" />
          <ds:DigestValue>
            /ZVkkcTGg7NugoBLeAPgBdhf1ZU=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5003">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            U1KPNX4K1YP3P8FH5dNqvvCe53M=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5004">
          <ds:Transforms>
```

```
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            ZsT4RMdzHP8yj+dDHwNZC8Ra9mQ=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5005">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            Nd/8wVmBdLowQKMblBRYK+6xcjA=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_5006">
          <ds:Transforms>
            <ds:Transform Algorithm="http://...">
              <exc14n:InclusiveNamespaces PrefixList="S" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            qlHYcDqttN+uqylqJJmb9f0q16k=
          </ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_3">
          <ds:Transforms>
            <ds:Transform Algorithm="http://w...">
              <exc14n:InclusiveNamespaces PrefixList="wsu wsse S"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://...#sha1" />
          <ds:DigestValue>
            rNDSWvzABVW5gTOJm8agaIsuP9c=
          </ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
    <ds:SignatureValue>
      M6u55+sCKK22D53VxAZr+HUD9z4=
    </ds:SignatureValue>
    <ds:KeyInfo>
      <wsse:SecurityTokenReference>
        <wsse:KeyIdentifier ValueType="...#EncryptedKeySHA1"
                            EncodingType="...#Base64Binary">
          rp71Yj5lyUkHB0jvGPL4YA/2amc=
        </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
</S:Header>
<S:Body wsu:Id="_5006">
  <xenc:EncryptedData xmlns:ns19="http://..." Id="_5007"
```

```
                      Type="...#Content">
    <xenc:EncryptionMethod Algorithm="...#aes128-cbc" />
    <ds:KeyInfo xmlns:xsi="http://.." xsi:type="KeyInfoType">
      <wsse:SecurityTokenReference>
        <wsse:KeyIdentifier ValueType="...#EncryptedKeySHA1"
                            EncodingType="...#Base64Binary">
          rp71Yj5lyUkHB0jvGPL4YA/2amc=
        </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        j+I8vMacRSrdKZ5Frzj8yjw2vHjh7UQ97GcQ9LfUclfv/U2
        MoDXTNhDgu4+7JZh9NC10cWapoW86b/Zq9yZLYsXJwmmaAh
        SU1sHkp+YZKSjbUNNRBbRrW15+ST72u/UdbteGgz+gY0ODC
        rvXUF6VumGw8XlTqy1JM6aUjPkKMyhgORwwSBE6Y+sOe7Dn
        9++o22SKlvqce+RRZEN7GvnN5DOMnjKWE+V/lQFofIqYVrV
        aBgGcWgscdT5m19mqURnFNRYZLwjPLY7cjTW+HzqYb9B42l
        RVtKUAlIZcgsz68By8OInISsrUwfUBEGITODVe
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

El mensaje de respuesta en este caso es igual que en el anterior, ya que utilizamos cifrado mediante clave simétrica utilizando el certificado del servidor, y en este mensaje no se adjunta ningún token de autentificación.

4. Entorno SSO

Para finalizar, vamos a ver un ejemplo de cómo podríamos crear un entorno que implemente *Single Sign-On (SSO)* mediante el uso de servicios STS y *tokens* SAML.

En primer lugar deberemos crear un servicio STS que nos proporcione *tokens* de seguridad. Crearemos este servicio mediante la opción *File* > *New* > *Web Services* > *Secure Token Service (STS)*. Vamos a llamar a este servicio `ProveedorSTS`.

Nota

Al crear el servicio STS veremos que tiene errores de compilación. Esto se debe a un *bug* de NetBeans 6.8. Para solucionarlo deberemos añadir la librería Metro 2.0 al proyecto (como hicimos al crear un servicio con *tokens* SAML SV sobre SSL en la sesión anterior), sin que dicha librería se empaquete con nuestra aplicación al desplegarla. Esto debe producir que los errores de compilación desaparezcan.

Ahora tendremos que indicar el mecanismo de seguridad utilizado para acceder a este proveedor de identidades. Podemos utilizar *Username Authentication with Symmetric Key* (es la forma en la que el cliente accederá al proveedor para obtener su *token* de acceso a otros servicios). Este mecanismo seguramente estará seleccionado ya por defecto. A continuación pulsaremos sobre el botón *Configure...* junto al mecanismo de seguridad

seleccionado, y nos fijaremos en el *Algorithm Suite* utilizado, ya que deberá coincidir con el que se utilice posteriormente en el servicio (por defecto tendrá seleccionado *Basic 128 bit*).

En la misma pantalla de edición de atributos del servicio, nos aseguraremos de que está marcada la casilla *Act as Secure Token Service (STS)*. Pulsando el botón *Configure...* junto a dicha casilla podremos configurar las propiedades del servicio STS, como el nombre que queremos dar al emisor de *tokens*. En *Keystore...* seleccionaremos el par de claves con alias `wssip`.

Lamentablemente, en la versión 6.8 de NetBeans la creación de este tipo de servicios está plagada de *bugs*, como el que hemos corregido anteriormente añadiendo las librerías de Metro 2.0. A continuación mostramos otras correcciones que deberemos hacer para tener nuestro servicio funcionando:

- Si estamos en una aplicación Java EE 6 Web, veremos que en el código del servicio se ha añadido una anotación `@Stateless` que es innecesaria. Deberemos eliminarla.
- En el fichero WSDL del servicio (`ProvedorSTSService.wsdl` en nuestro caso), en la sección `tc:STSConfiguration` de la política de seguridad, hay un campo `tc:Contract` cuyo valor contiene una errata, ya que aparece como `WSTRustContractImpl` cuando debería ser `WSTrustContractImpl` (la `r` debe ser minúscula). Realizaremos esta modificación y grabaremos el fichero.
- Por último, NetBeans no despliega correctamente estos servicios en GlassFish. Deberemos desplegarlo manualmente. Para ello nos aseguramos de que se recompilen y empaqueten los últimos cambios realizados, pulsando sobre *Clean and Build* y copiaremos el fichero WAR de la carpeta `dist` del proyecto en el directorio `autodeploy` de nuestro dominio de GlassFish.

Con esto el servicio STS debe haber quedado correctamente desplegado, y deberemos poder ser capaces de consultar su documento WSDL en la siguiente dirección:

```
http://localhost:8080/ProveedorSTS/ProveedorSTSService?wsdl
```

A continuación vamos a crear el servicio al que accederemos medianto los *tokens* proporcionados por el STS. Para ello creamos un nuevos servicio igual que hemos hecho anteriormente, al que llamaremos `ServicioSTS`, y como mecanismo de seguridad seleccionamos *STS Issued Token*. Entramos en *Configure...* y seleccionamos el mismo *Algorithm Suite* que utilizamos en el proveedor STS (*Basic 128 bit*), y longitud de clave (*Key Size*) de 128 bits. Dejaremos marcada la casilla *Use development defaults*.

Ahora, para finalizar, deberemos crear el cliente. Vamos a crearlo en una aplicación web a la que llamaremos *ClienteSTS*. En primer lugar crearemos una referencia al servicio `ServicioSTS`, que es el servicio al que queremos acceder, al igual que lo hemos hecho en casos anteriores. Entraremos en la ventana de edición de atributos del cliente que acabamos de crear, e indicaremos en *Keystore...* que el alias del certificado del cliente será `xws-security-client`, y en *Truststore...* indicaremos que el del servicio es `xws-security-server`. Veremos además abajo una sección *Secure Token Service*, en la

que deberemos configurar la forma en la que se obtendrán los *tokens* de seguridad para acceder a dicho servicio. El único campo que deberemos completar aquí es *Endpoint*, en el que introduciremos la URL del servicio STS:

```
http://localhost:8080/ProveedorSTS/ProveedorSTSService
```

Para que el cliente sea capaz de obtener los *tokens* de seguridad a partir de dicho servicio, deberemos añadir una referencia a él. Crearemos un nuevo cliente para `ProveedorSTS` dentro del mismo proyecto. Una vez hecho esto, deberemos entrar en la ventana de edición de atributos para dicho cliente, y en *Truststore...* especificamos el alias `wssip` (recordemos que es el certificado que seleccionamos al crear el proveedor STS). Introducimos también el nombre y password con el que acceder al servicio (por defecto un usuario del *realm* `file`).

Con esto podemos probar ya nuestro servicio. Si observamos los mensajes que se intercambian, veremos que primero accedemos al servicio STS (`ProveedorSTS`) para obtener un *token* de seguridad, y tras esto nos conectaremos al servicio (`ServicioSTS`) para invocar una de sus operaciones.

5. Ejercicios

5.1. Gestión de multas con seguridad a nivel de mensaje

Como ejercicio proponemos la implementación del servicio para la consulta de multas especificado en la sesión anterior, esta vez utilizando seguridad a nivel de mensaje. ¿Qué tipo de mecanismo de seguridad deberemos utilizar en este caso?