Servicios Web Seguros

Sesión 6: Seguridad a nivel de mensaje. Firma digital

Puntos a tratar

- Firma digital en el WSDL
- Password Callback Handler
- Propiedades de seguridad
- Firma en los mensajes SOAP

Firma digital

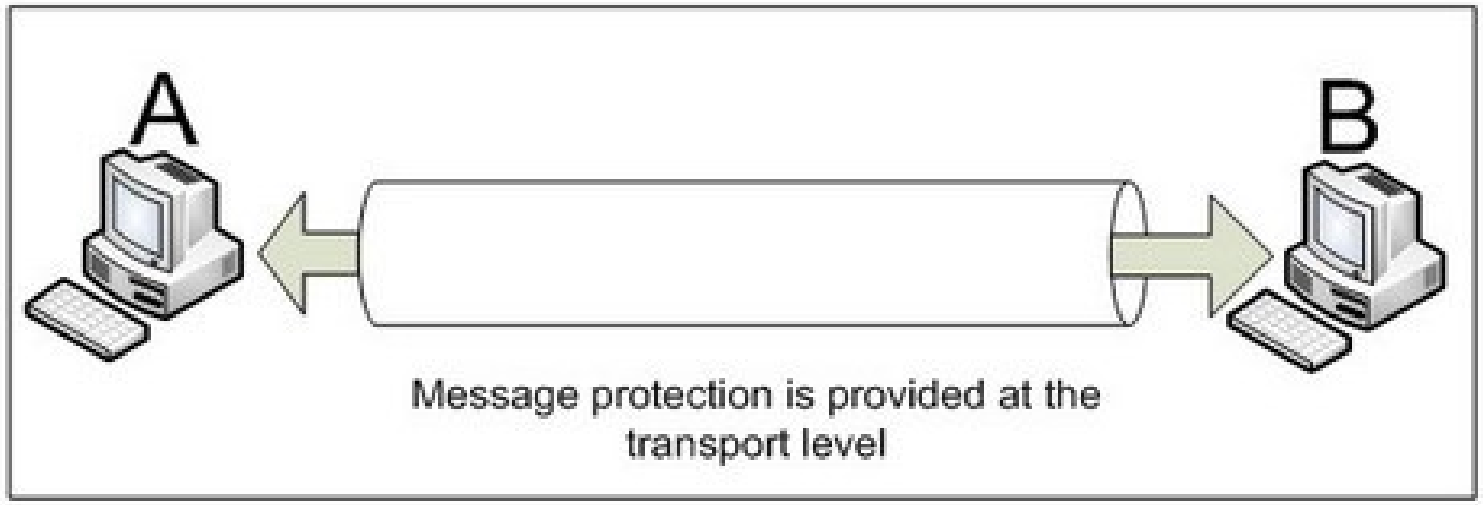
- Añadir política de seguridad al WSDL
- <wsp:PolicyReference URI="#p1" wsdl:required="true"/>
- <wsp:Policy wsu:Id="p1">
  <sp:AsymmetricBinding>

  </sp:AsymmetricBinding>
  </wsp:Policy>

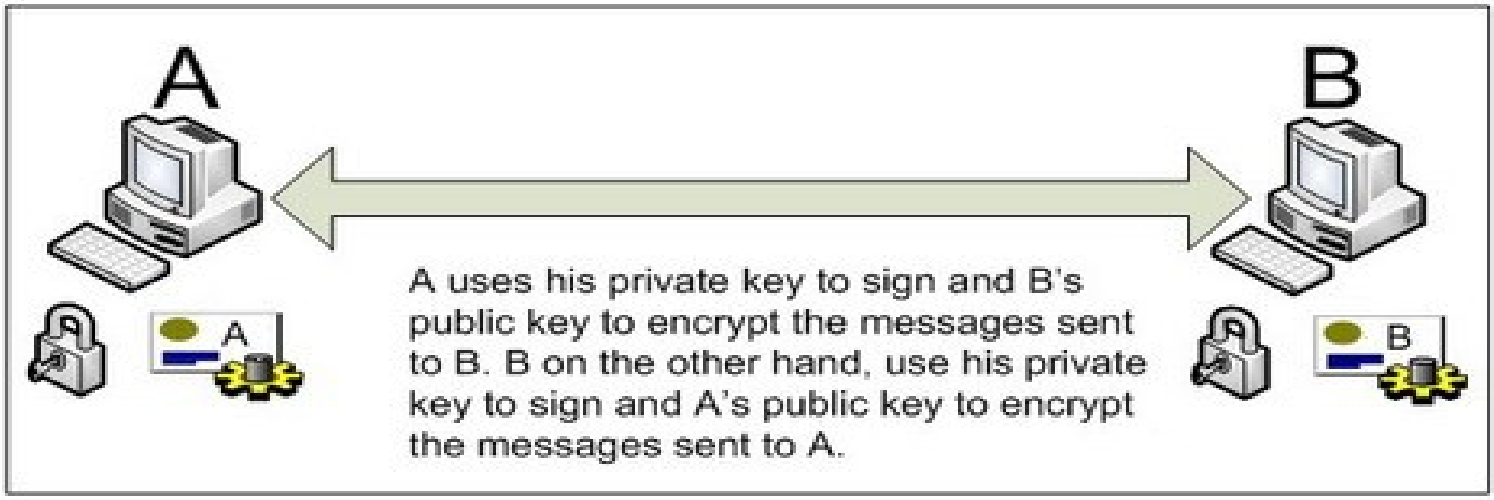
Binding

- Transport binding
- Asymmetric binding
- Symmetric binding

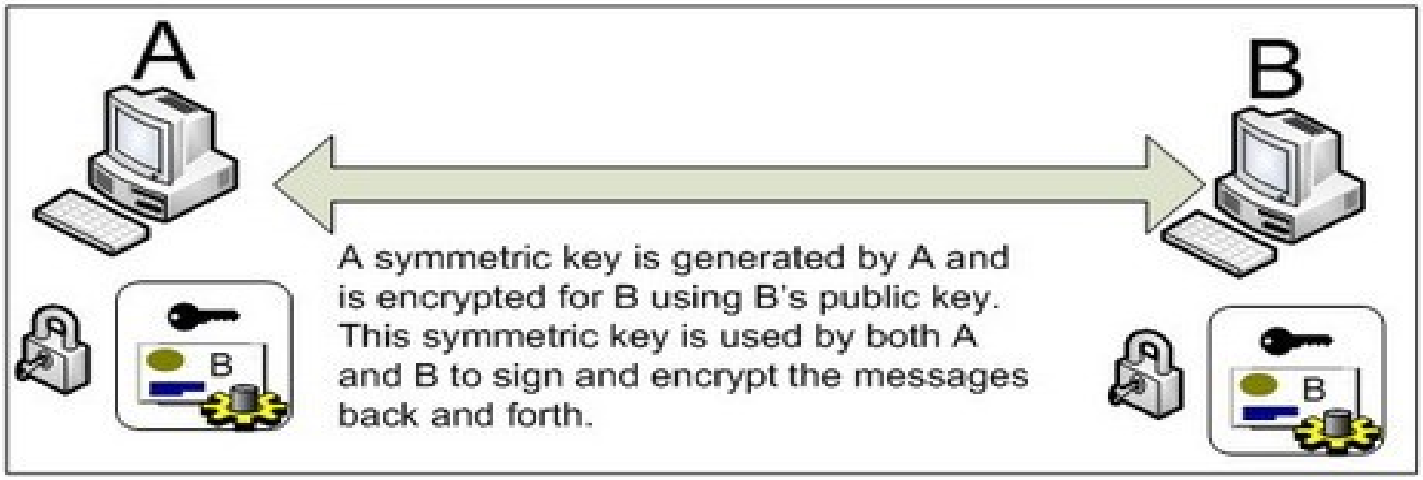
Transport binding



Asymmetric binding



Symmetric binding



Política del binding

- Tokens de seguridad y Algoritmos

```
<sp:AsymmetricBinding>
  <wsp:Policy>
    <sp:InitiatorToken>

    </sp:InitiatorToken>
    <sp:RecipientToken>

    </sp:RecipientToken>
    <sp:AlgorithmSuite>

    </sp:AlgorithmSuite>
  </wsp:Policy>
</sp:AsymmetricBinding>
```

Tokens de seguridad

```
<sp:InitiatorToken>
  <wsp:Policy>
        <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/
                ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient">
          <wsp:Policy>
                <sp:WssX509V3Token10 />
          </wsp:Policy>
        </sp:X509Token>
  </wsp:Policy>
</sp:InitiatorToken>
```

Otras preferencias de seguridad

- <sp:Wss10>: Opciones de WSS SOAP Message Security 1.0
  - <sp:MustSupportRefEmbeddedToken />
  - <sp:MustSupportRefIssuerSerial />
- <sp:SignedParts>
  - <sp:Body /> : firmar el contenido del cuerpo del mensaje

Password callback handler

- Manejador de contraseñas
  - Se ejecutará cada vez que se requiera una contraseña para abrir un almacén, para un certificado o para otro tipo de autentificación
- Map<String, Object> properties = ((BindingProvider)port).getRequestContext();
- properties.put(SecurityConstants.CALLBACK_HANDLER, new CallbackHandler(){ … });

Password callback handler

```
new CallbackHandler() {

            @Override
            public void handle(Callback[] callbacks) throws IOException,
                            UnsupportedCallbackException {
                    for(Callback cb : callbacks){
                            WSPasswordCallback pcb = (WSPasswordCallback)cb;
                                if(pcb.getIdentifier().equals("cliente1")){
                                    pcb.setPassword("cliente1-pass");
                            }
                    }
            }
     }
```

Otras propiedades

- Otras propiedades configurables desde el código cliente o servidor:
  - properties.put(SecurityConstants.SIGNATURE_USERNAME, "cliente1");
  - properties.put(SecurityConstants.SIGNATURE_PROPERTIES, "crypto.properties");
  - properties.put(BindingProvider.ENDPOINT_ADDRESS_PROPERTY, "http://localhost:1234/Seguro");

Otras propiedades

- Archivo crypto.properties:
  - org.apache.ws.security.crypto.provider=
    org.apache.ws.security.components.crypto.Merlin
  - org.apache.ws.security.crypto.merlin.keystore.type=JKS
  - org.apache.ws.security.crypto.merlin.file=/home/servicios/claves/cliente.ks
  - org.apache.ws.security.crypto.merlin.keystore.password=cliente1-ks-pass

Mensaje SOAP firmado

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/
...
    </wsse:Security>
  </soap:Header>
  <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/
   oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Id-7182746">
    <ns2:saluda xmlns:ns2="http://jtech.ua.es/Seguro/">
      <nombre>Boyan</nombre>
      <apellido>Bonev</apellido>
    </ns2:saluda>
  </soap:Body>
</soap:Envelope>
```

Mensaje SOAP firmado

- Security
  - BinarySecurityToken ← el certificado
  - Signature Id=”Signature-1”
    - SignedInfo (referencias e información del algoritmo)
    - SignatureValue ← la firma
    - KeyInfo (información de políticas de seguridad)

Certificado en SOAP

```
<wsse:BinarySecurityToken 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"
  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#X509v3"
    wsu:Id="CertId-897C23E154C65197...
                                                    ...
                                                    ...
                                                    ...
...rZSJE3b16AceZPJbXnKsORMBstU=</wsse:BinarySecurityToken>
```

Firma en SOAP

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  Id="Signature-1">
   <ds:SignedInfo>
      ...
   </ds:SignedInfo>

<ds:SignatureValue>IC7YAzDpY93JCUGLI3HD79R+Exn9LBpEecq2wTTzFRA
      /ztCiZkSrdOPVG7t5cRAVCMN+czXspfhl124p/6rXvazqcX42Vv7VwycyZzNa6
      OifZlJOypUqgh7++sJjrIW46gD2HnZT+/YjKZSIDttBJ331iv+AlZyBbZZQmaq
      1XP4=</ds:SignatureValue>
      <ds:KeyInfo Id="KeyId-897C23E154C65197B31274025550735 2">
        ...
      </ds:KeyInfo>
   </ds:Signature>
</wsse:Security>
```

¿Preguntas...?