
# Seguridad en Web Services

Por: Jorge Mario Calvo L.

Junio/2010

# Objetivo

- Proveer una visión de los principales aspectos de seguridad de los Web Services y cuales alternativas y estándares existen para resolverlos
- Mostrar algunos ejemplos prácticos a través de un productos de Software Libre que implementa algunos de los estándares

# Plan de la Charla

- ¿Que es un Web Services?
- Aspectos de seguridad a resolver
- Niveles donde podemos resolver el problema
  - Transporte
  - Mensajería
  - Aplicación
- Otros Estándares relacionados con la seguriada en XML y Web Services

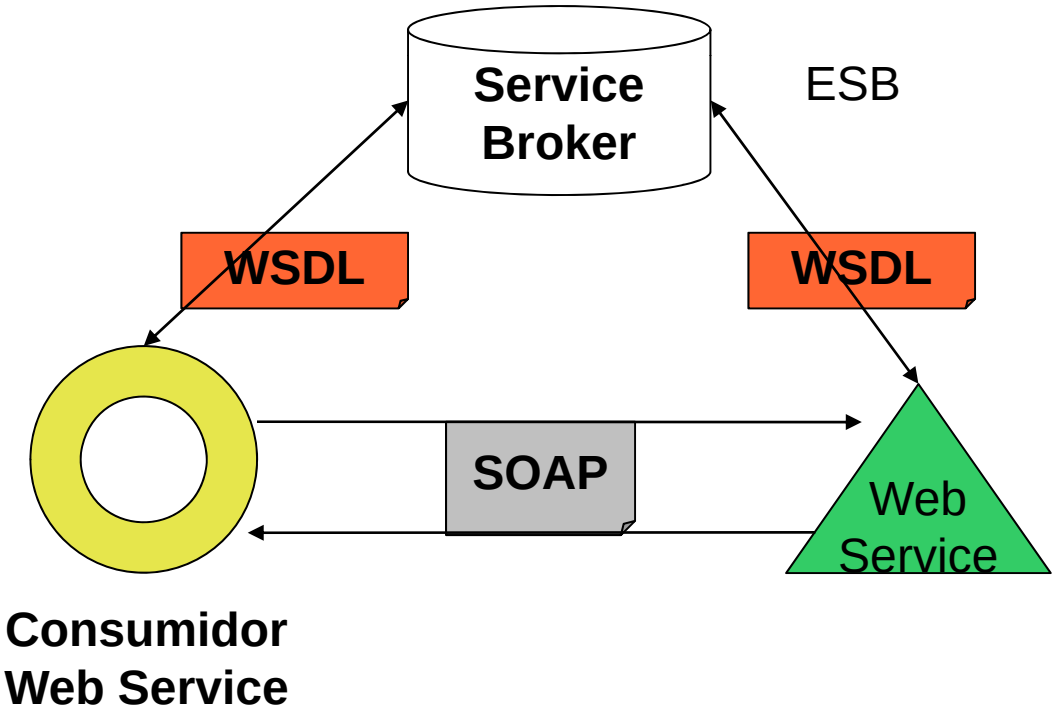
# ¿Que es un Web Services?

- A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. (www.w3c.org)

# ¿Que es un Web Services?

- Una de las posibles interfaces de mensajeria de un servicio, en una Arquitectura SOA
- Mensajeria basada en XML
  - SOAP
  - WSDL

# Operación de un Web Service



# Mensajería SOAP

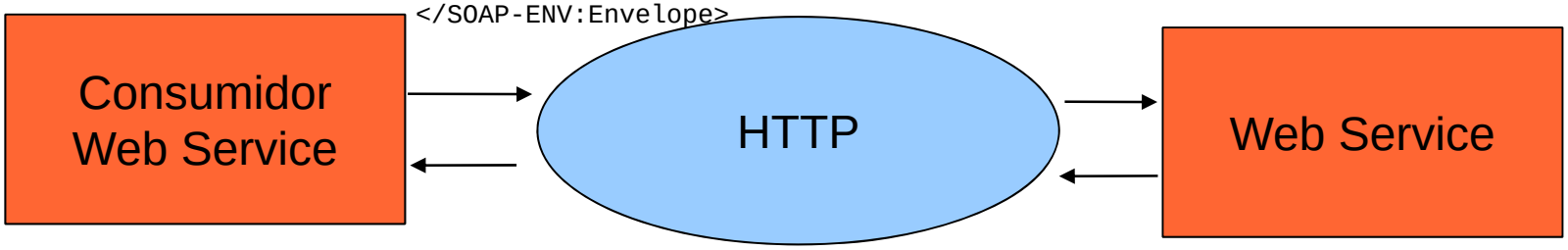
```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas....
  <SOAP-ENV:Body>
    <SOAP-ENV:getOrderStatus>
       <body>US-247860</body>
    </SOAP-ENV:getOrderStatus>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Request

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.....
  <SOAP-ENV:Body>
    <SOAP-ENV:getOrderStatusResponse>
        <body>Shipped</body>
    </SOAP-ENV:getOrderStatusResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Response

```
POST /temperApp/GetLocalTemperature HTTP/1.1
Host: www.ubiquando.com.co
Content-type: text/xml
Content-length: 543
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas....
  <SOAP-ENV:Body>
    <SOAP-ENV:getOrderStatus>
       <body>US-247860</body>
    </SOAP-ENV:getOrderStatus>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



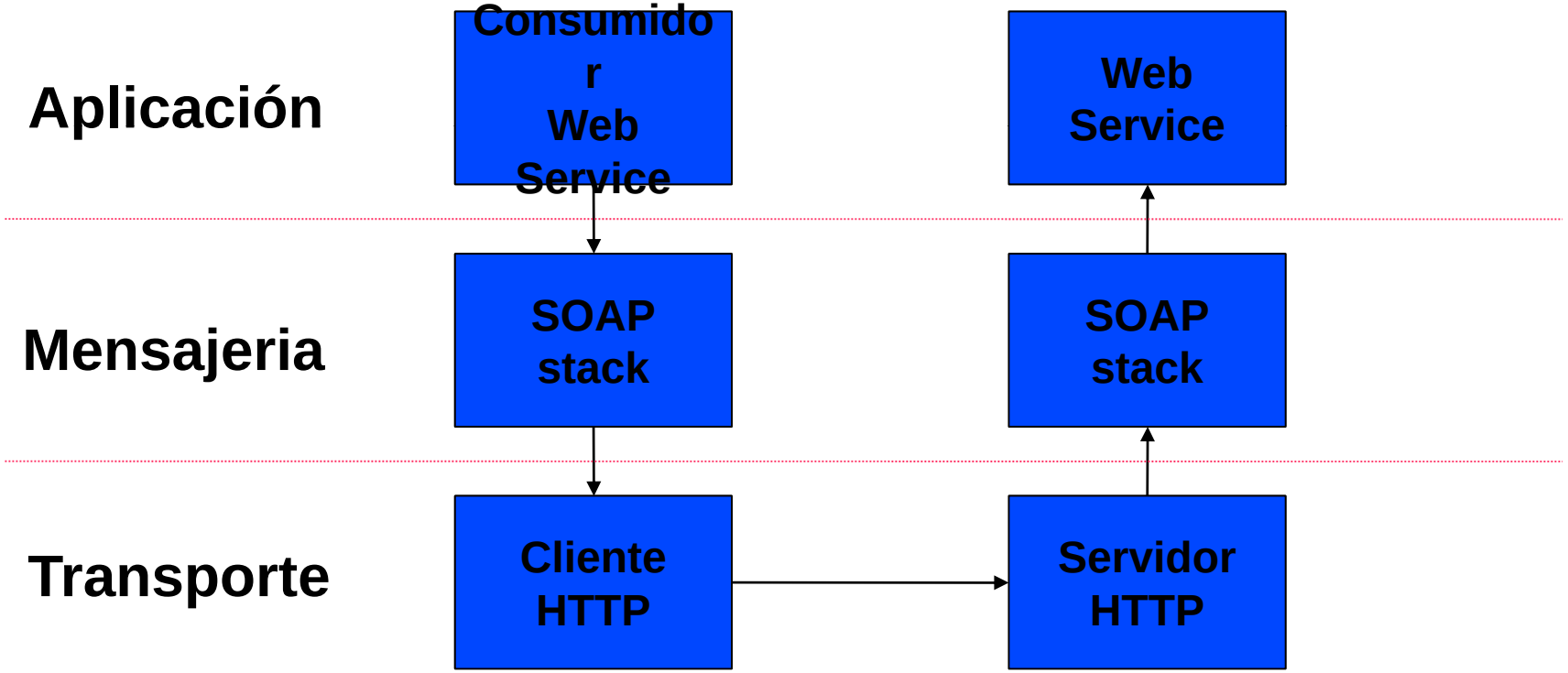

```
HTTP/1.1 200 OK
Content-type: text/xml
Content-length: 145
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.....
  <SOAP-ENV:Body>
    <SOAP-ENV:getOrderStatusResponse>
        <body>Shipped</body>
    </SOAP-ENV:getOrderStatusResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

# Mostrar un Web Service simple

# Aspectos de Seguridad

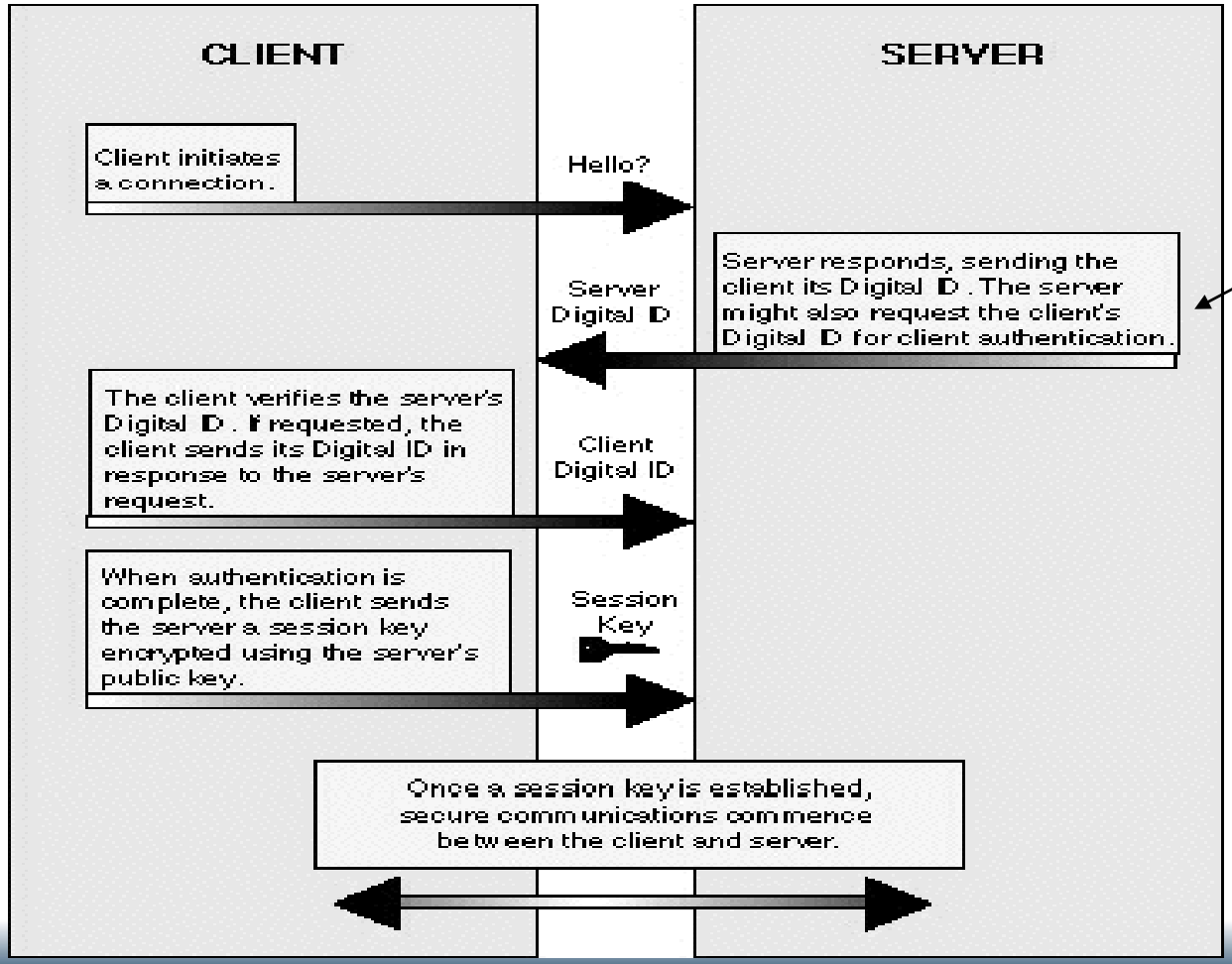
- Autenticación-Identidad
  - ¿Quién lo consume?
- Autorización-Control de Acceso
  - ¿Qué esta autorizado a hacer el consumidor?
- Confidencialidad
- Integridad

# Nivel donde lo podemos resolver



Browser

Servidor Web




CA

Verisign,
Certicamara
firma el Digital ID
del servidor Web

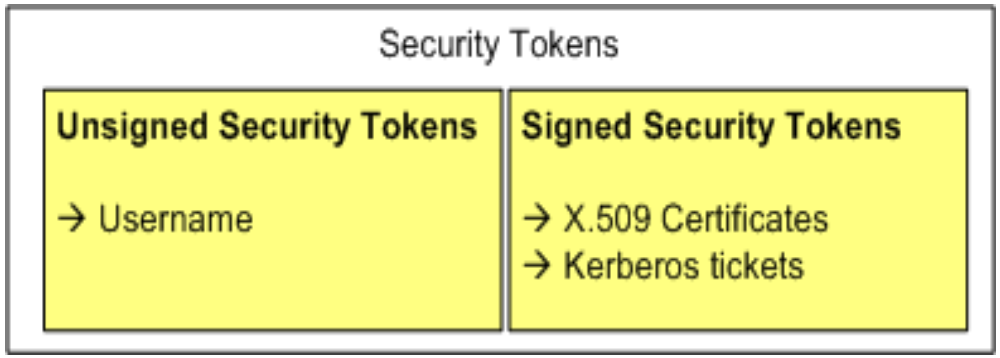
# A nivel de Transporte

- Utilizando SSL y su sucesor TLS (https)
  - Autenticación-Identidad
    - Certificado de servidor seguro y Cerrtificado de cliente
  - Autorización-Control de Acceso
    - No existe
  - Confidencialidad
    - Conexión encriptada de SSL
  - Integridad
    - Conexión encriptada de SSL

# A nivel de mensajería

- WSS: SOAP Message Security
  - Security Tokens: almacena la información para autenticación y autorización. Ejemplo: login/password o Certificados X.509
  - XML Encryption: almacena EncryptedKey element y ReferencedList que apuntan a las partes encriptadas del mensaje
  - XML Signatures

# WS-Security: Security Tokens




```
<Envelope>
 <Header>
  <Security>
   <UserNameToken>
    <UserName>administrador</UserName>
    <Password>1234</Password>
   </UserNameToken>
  </Security>
 </Header>
 <Body> .......
```

# WS-Security: XML Encryption

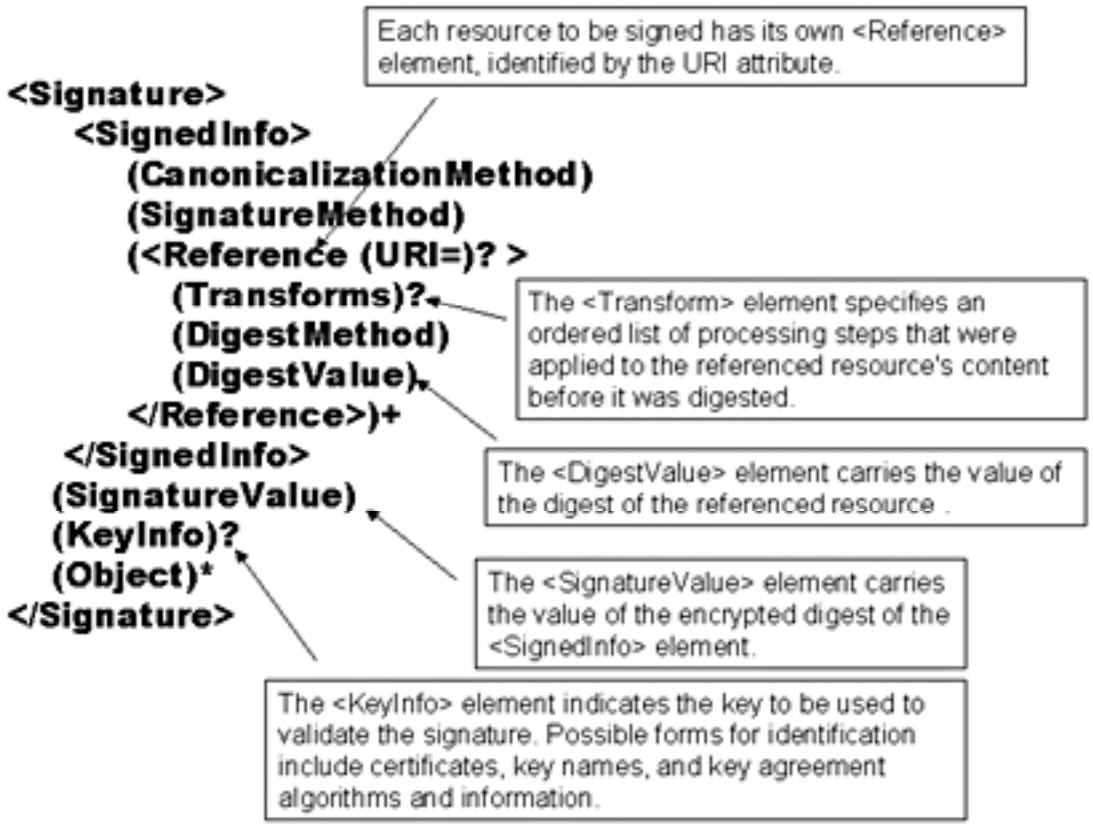
```
<Envelope>
    <Header>
        <Security>
            <ReferenceList>
                <DataReference URI="#bodyID"/>
            </ReferenceList>
        </Security>
    </Header>
    <Body>
        <EncryptedData Id="bodyID">
          <KeyInfo>
            <KeyName>CN=Hiroshi Maruyama, C=JP</KeyName>
          </KeyInfo>
          <CipherData>
            <CipherValue>...</CipherValue>
          </CipherData>
        </EncryptedData>
    </Body>
</Envelope>
```


# Mostrar el Web Service con el estandar WS-Security

# A nivel de aplicación

- XML Signatures y XML Encryption
  - Estándar para el uso de Digital Signatures en los mensajes XML y garantizar la autenticidad de los mensajes.
  - Adicionar autenticidad, integridad y no repudio a los mensajes XML
  - Permite firmar parte de los mensajes y no el documento completo

# XML Signatures



# A nivel de aplicación

- Generar campos adicionales y/o encriptar parámetros
- Amazon Web Service AWS

# Otros Estándares

- XML
  - XML Signatures y XML Encryption
- Web Services
  - WS-Security, WS-Trust, WS-Policy
- AAA
  - SAML

# WS-Policy

- Framework para expresar las limitaciones y los requisitos de los Web Services, utilizando aserciones o predicados.
- Estos predicados definen las características de seguridad que deben tener los mensajes SOAP.

# Ejemplo de WS-Policy

```
<wsp:Policy>
  <sp:SymmetricBinding>
     <wsp:Policy>
       <sp:ProtectionToken>
          <wsp:Policy>
                <sp:KerberosV5APREQToken sp:IncludeToken=".../IncludeToken/Once" />
          </wsp:Policy>
        </sp:ProtectionToken>
        <sp:SignBeforeEncrypting />
        <sp:EncryptSignature />
     </wsp:Policy>
```

# SAML

- Framework XML para representar información acerca de autenticidad, autorización y seguridad que pueda ser utilizada por las aplicaciones y/o intercambiada entre diferentes aplicaciones y plataformas.
- Utiliza predicados (statements)

# Usos de SAML

- Single sign-on (SSO)
- Identity federation
- Attribute services
- Securing web service messages
  - Handled by the OASIS WSS TC as the “SAML Token Profile of WS-Security”

# SAML Token Profile of WS-Security

- Definir el uso de tokens para SAML dentro de WSS: SOAP Message Security specification
- Cuando un Web Service recibe el SOAP Request con una referencia a un(os) predicado(s) SAML los selecciona y los procesa.

```
<S12:Envelope xmlns:S12="...">
  <S12:Header>
    <wsse:Security xmlns:wsse="...">
      <saml:Assertion xmlns:saml="..."
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer=”www.opensaml.org”
        MajorVersion="1"
        MinorVersion="1">
        <saml:AuthenticationStatement>
         <saml:Subject>
          <saml:NameIdentifier
            NameQualifier="www.example.com"
            Format=“urn:oasis:names:tc:SAML:1.1:nameidformat:
```

# Otros Temas

- La seguridad en el código del Web Service es algo por fuera de esta presentación