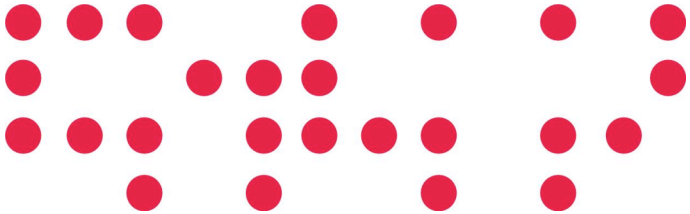
Protegiendo nuestros servicios webs
WS-SEC

Cándido Rodríguez
candido.rodriguez@rediris.es



¿Qué es WS-SEC?

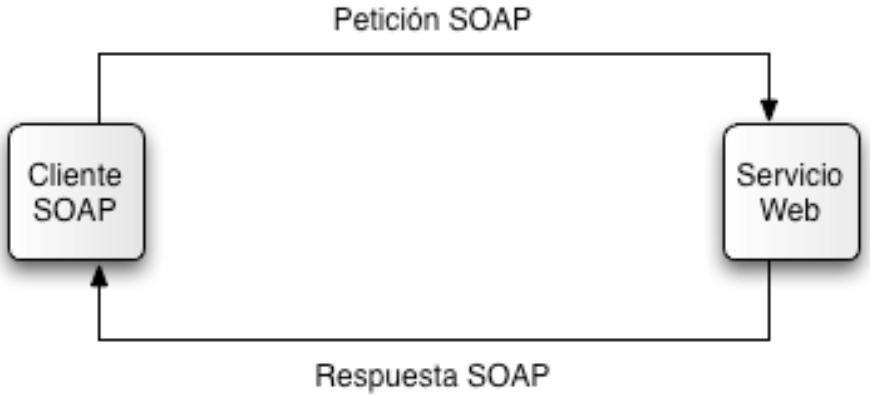
- La especificación WS-SEC proporciona unas extensiones SOAP
  - Capa de seguridad sobre servicios web
- Soporta una gran variedad de modelos de seguridad
  - Diferentes tokens de seguridad
  - Múltiples dominios de confianza
  - Diferentes formatos de firmas digitales
  - Diferentes tecnologías de encriptación
- Permite
  - Enviar los tokens de seguridad en el mensaje
  - Integridad del mensaje
  - Confidencialidad del mensaje

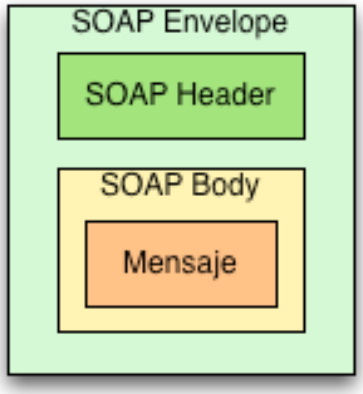
¿Qué es WS-SEC?

- Objetivos
  - Asegurar los intercambios de mensajes SOAP
- No pretende resolver
  - Crear contextos de seguridad
  - Proporcionar mecanismos de autenticación
  - Gestión de las claves
  - Publicación e intercambio de políticas de seguridad
  - En qué está basada la confianza
  - No repudiación

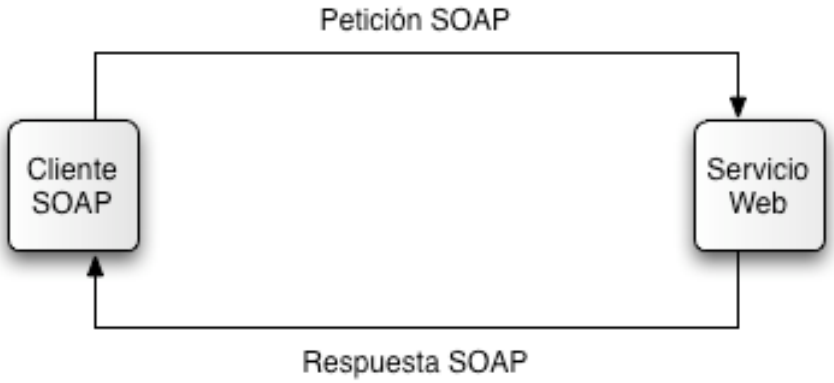
¿Cómo funciona WS-SEC?

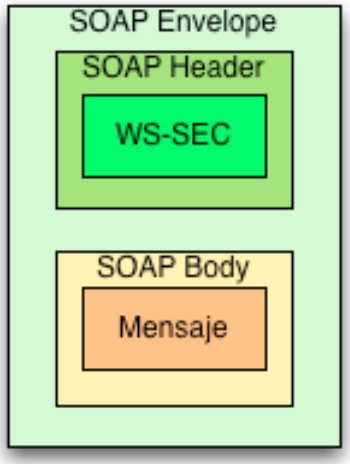
- Intercambio típico basado en servicios web





- Usando WS-SEC





¿Cómo funciona WS-SEC?

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

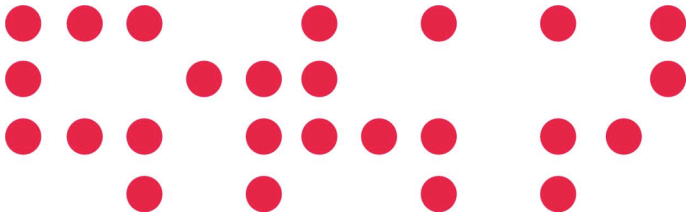
red.es

```
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Header>
      <wsse:Security
         xmlns:wsse="…"
         soapenv:actor="…" soapenv:mustUnderstand="1">
            .
            .
            .
       </wsse:Security>
   </soapenv:Header>
   <soapenv:Body>
      .
      .
      .
   </soapenv:Body>
</soapenv:Envelope>
```

¿Cómo funciona WS-SEC?

- El elemento <wsse:Security> contiene información relacionada con la seguridad del mensaje SOAP
  - Puede aparecer tantas veces como sea necesario
    - Su atributo actor/role indica quién debe ser el destinatario
  - Trabaja tanto con SOAP 1.1 como con SOAP 1.2

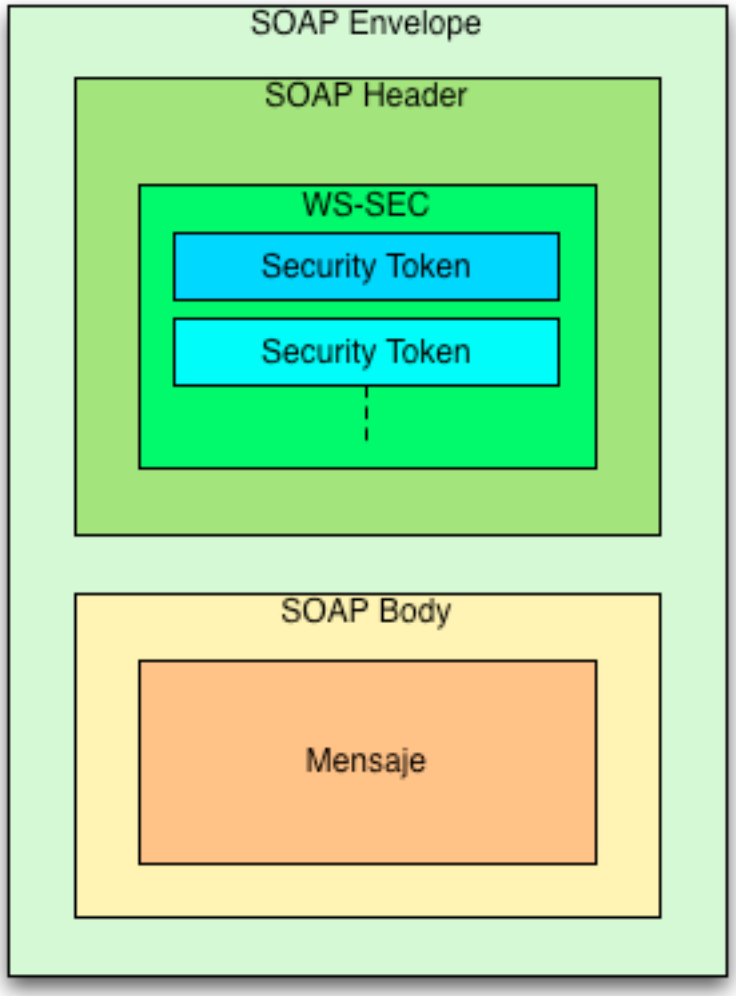
Índice



Tokens de seguridad

- Un token de seguridad es un conjunto de afirmaciones hecho por una entidad determinada
  - Ej: nombre, identidad, clave, privilegios, etc.
- Tipos de token de seguridad
  - Simples
    - Nombre del usuario
  - Tokens binarios
    - Usados en el perfil de certificados X.509
    - Usados en el perfil de Kerberos
  - Tokens basados en mensajes XML
    - Usados por el perfil de lenguajes de expresión de derechos (REL)
    - Usados por el perfil de aserciones SAML

Tokens de seguridad



Tokens de seguridad: User Name

- El elemento <wsse:UsernameToken> proporciona una vía para indicar el nombre del usuario

```
<wsse:UsernameToken>
  <wsse:Username>
    ...
  </wsse:username>
</wsse:UsernameToken>
```

Tokens de seguridad: binarios

- El elemento <wsse:BinarySecurityToken> es un formato de token que necesita una codificación especial para su inclusión
  - Generalmente mediante Base 64

```
<wsse:BinarySecurityToken
  EncodingType="#Base64Binary"
  ValueType="…">
    …
</wsse:BinarySecurityToken>
```

  - Cada uno de los perfiles basados en tokens binarios especifican cómo están definidos y cómo se debe trabajar con ellos

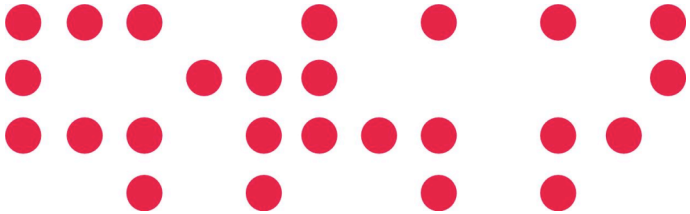
Tokens de seguridad: mensajes XML

- Puede ser cualquier elemento de un mensaje XML
  - Sólo se podrán usar los definidos por el perfil
    - Error en caso contrario

```
<saml:Assertion …>
    …
</saml:Assertion>
```

Índice

1. **Introducción a WS-SEC**
2. **Tokens de seguridad**
3. **Perfiles**
4. **Mejorando la seguridad**
   1. **Encriptación**
   2. **Marcas de tiempo**
5. **Ejemplos**



Perfiles

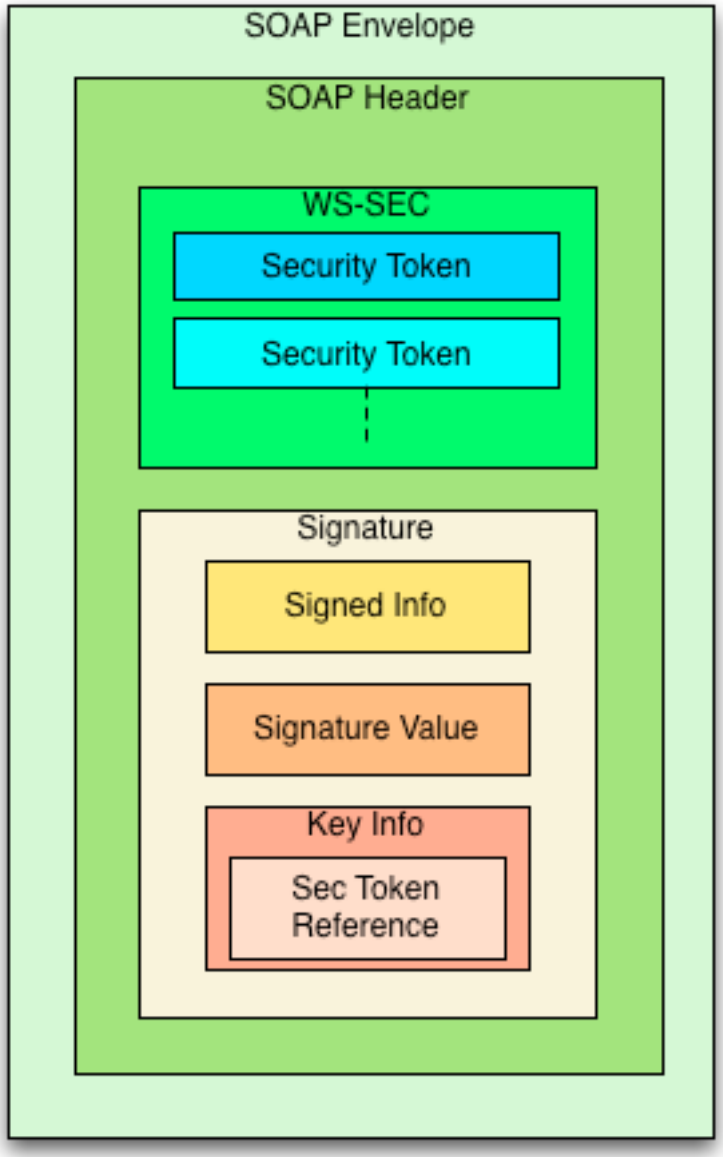
- Nos indican como integrar nuestros entornos de confianza con WS-SEC
- Se definen en la especicación WS-SEC:
  - Perfil de tokens basados en certificados X.509
  - Perfil de tokens basados en aserciones SAML
  - Perfil de tokens de Nombre de usuario
  - Perfil de tokens de Kerberos
  - Perfil de tokens de lenguajes de expresión de derechos (REL)

Perfil de certificados X.509

- El perfil X.509 especifica como integrar un framework de autenticación basado en certificados X.509
  - Información del usuario contenido en tokens
  - Creación de firma digitales
- Tipos de tokens binarios:
  - Un certificado X.509
    - `ValueType="#X509v3"`
  - Una lista ordenada de certificados X.509 en un *PKIPath*
    - `ValueType="#X509PKIPathv1"`
  - Un conjunto de certificados X.509 y CRLs
    - `ValueType="#PKCS7"`

- No siempre se incluye un token con el certificado
  - Uso de referencias a un token
    - A través del *Key Identifier* del usuario
    - Incluyendo información del Emisor y del Número de Serie

Perfil de certificados X.509



- Firma digital
  - En `<ds:SignedInfo>` hay una lista con los elementos del mensaje SOAP con su *digest*
  - En `<ds:SignatureValue>` está el valor de la firma digital de `<ds:Signature>`
  - En `<ds:KeyInfo>` tenemos la referencia al token utilizado para los *digests* y las firmas

Perfil de tokens SAML

- El perfil de tokens SAML nos especifica cómo utilizar aserciones SAML 1.1 ó 2.0 con WS-SEC

```
<wsse:Security
  xmlns:wsse="…"
  soapenv:actor="…" soapenv:mustUnderstand="1">
    <saml:Assertion …>
        …
    <saml:Assertion …>
</wsse:Security>
```

  - Las aserciones SAML pueden ser referenciadas como token de seguridad
- El contenido de la aserción SAML (su semántica) está bajo la especificación SAML 1.1 o 2

- Métodos de confirmación de los datos del usuario
  - *Holder-of-key*
    - El cliente SOAP actúa en nombre del usuario de la aserción SAML
      - Comprueba que el usuario está en posesión de las claves
      - Se añade información de dicho chequeo en la aserción
  - *Sender-vouches*
    - El cliente SOAP se responsabiliza de la identidad del usuario
      - Debe haber una plena confianza entre el cliente y el servicio web

Perfil de token Nombre de usuario

- Especifica como un cliente SOAP puede incluir información sobre el usuario
  - Nombre de usuario *[Obligatorio]*
  - Contraseña *[Recomendado]*
    - El valor en texto plano, un *hash* o usando S/KEY
    - Un *digest* del valor
  - Valor aleatorio *[Opcional]*
    - Generalmente en base 64
  - Fecha de creación *[Opcional]*
- Seguridad en el perfil (I/II)
  - Recomiendan rechazar cualquier token `<wsse:UsernameToken>` si no incluye
    - El valor aleatorio
    - La fecha de creación

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

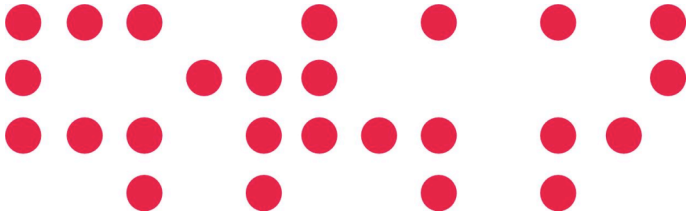
red.es

- Seguridad en el perfil (II/II)
  - Recomiendan rechazar cualquier token `<wsse:UsernameToken>` si su fecha de creación es antigua.
    - Rango es decisión del servicio web
  - Recomiendan almacenar en el lado del servidor el valor aleatorio durante la validez del token para verificar que no se vuelve a utilizar

```
<wsse:Security …>
  <wsse:UsernameToken …>
    <wsse:Username>…</wsse:Username>
    <wsse:Password type="…">…</wsse:Password>
    <wsse:Nonce EncodingType="…">…</wsse:Nonce>
    <wsu:Created>…</wsu:Created>
  </wsse:UsernameToken>
</wsse:Security>
```

Índice

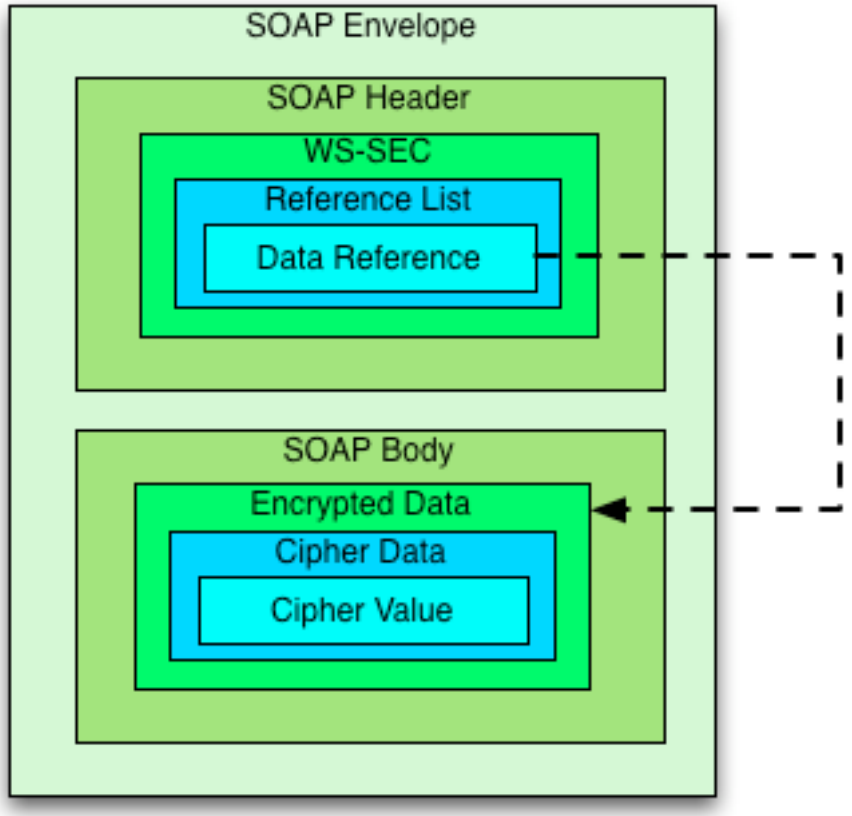
1. **Introducción a WS-SEC**
2. **Tokens de seguridad**
3. **Perfiles**
4. **Mejorando la seguridad**
   1. **Encriptación**
   2. **Marcas de tiempo**
5. **Ejemplos**



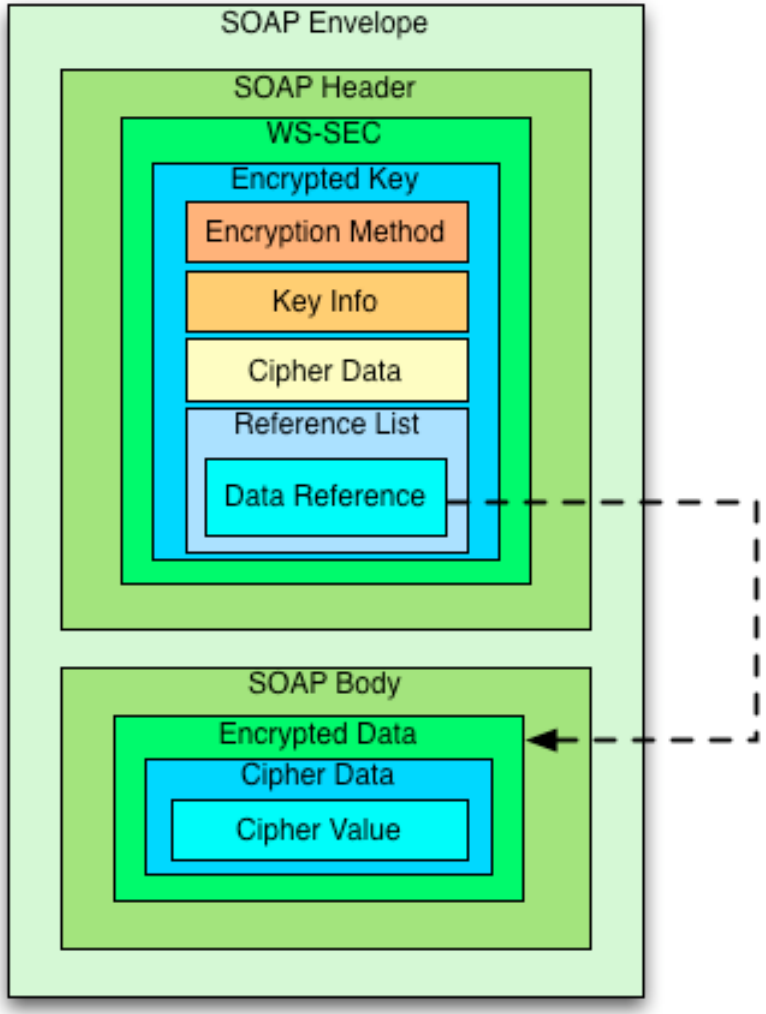
Encriptación

- WS-SEC permite encriptar
  - SOAP bodies
  - SOAP headers
  - Cualquier elemento que esté en alguno de ellos
- La encriptación se basa en
  - Una clave simétrica común previamente intercambiada entre cliente y servidor
  - Una clave simétrica enviada en el mensaje, encriptada con una clave simétrica o asimétrica común
- WS-SEC especifica como integrar su especificación con la estándar de encriptación XML

- Encriptación por clave simétrica compartida



- Encriptación por clave simétrica enviada en el mensaje

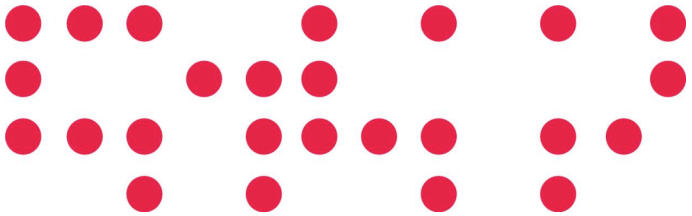


Marcas de tiempo

- WS-SEC nos permite indicar marcas de tiempo de una cabecera de seguridad
  - ¿Cuándo fue creado?
  - ¿Cuándo va a expirar?

```
<wsse:Security …>
  <wsu:Timestamp …>
    <wsu:Created>…</wsu:Created>
    <wsu:Expires>…</wsu:Expires>
  </wsu:Timestamp>
</wsse:Security>
```

Índice



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Edificio CICA, Campus Universitario
Avenida Reina Mercedes s/n
41012 Sevilla. España

Tel.: 95 505 66 00
Fax: 95 505 66
www.red.es