Firma Digital en SOA

Agenda

asdc
Argentina Software Development Center

- SOAP
- XML - Signature
- WS-Digital Signature
- Métodos de Canonicalización

•SOAP

asdc
Argentina Software Development Center

- Se creó como una forma de transporte en XML de un ordenador a otro a través de una serie de protocolos estándar de transporte.
HTTP es el más común de los protocolos de transportes y, por supuesto, es el más utilizado en la Web

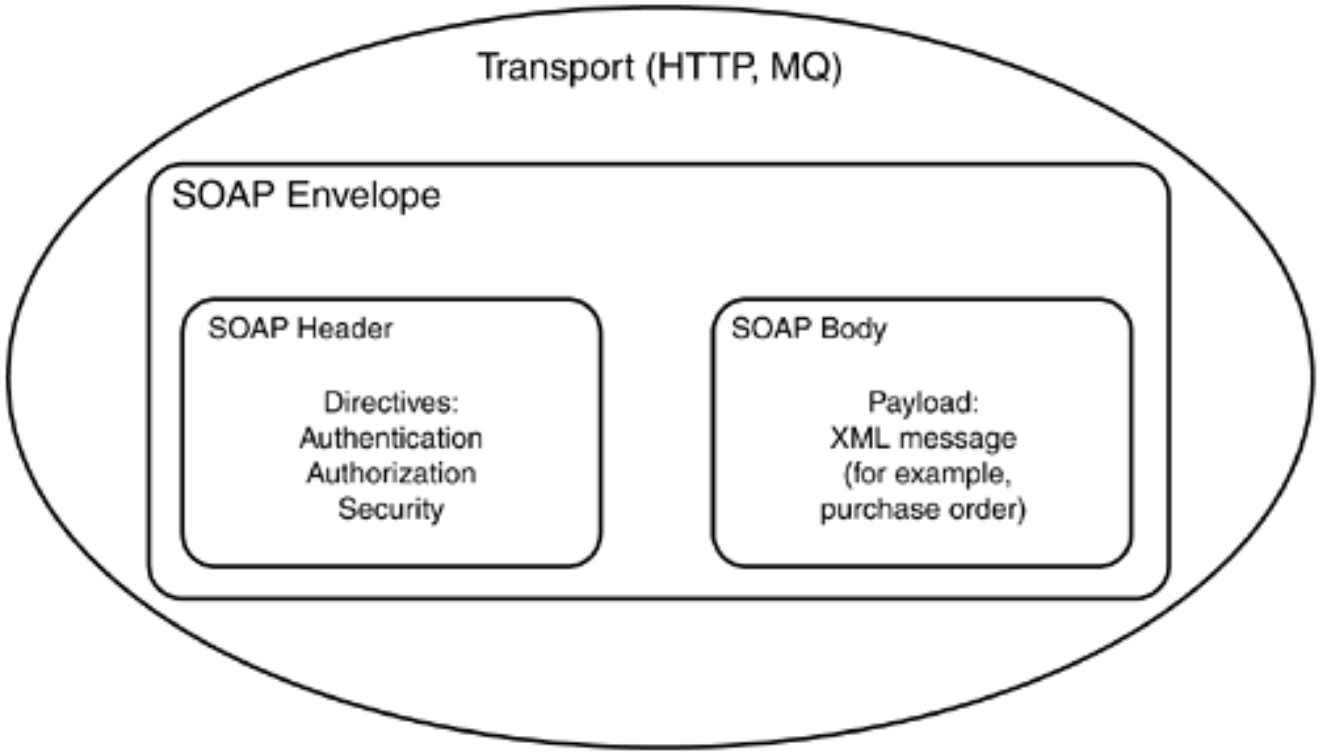
SOAP proporciona un mecanismo de forma simple, coherente y extensible mecanismo que permite que una aplicación pueda enviar un mensaje XML a otro.

SOAP es lo que hace posible integración de aplicaciones, porque después que XML define el contenido de un mensaje, es SOAP el qeu se encarga de mover los datos de un lugar a otro durante de la red

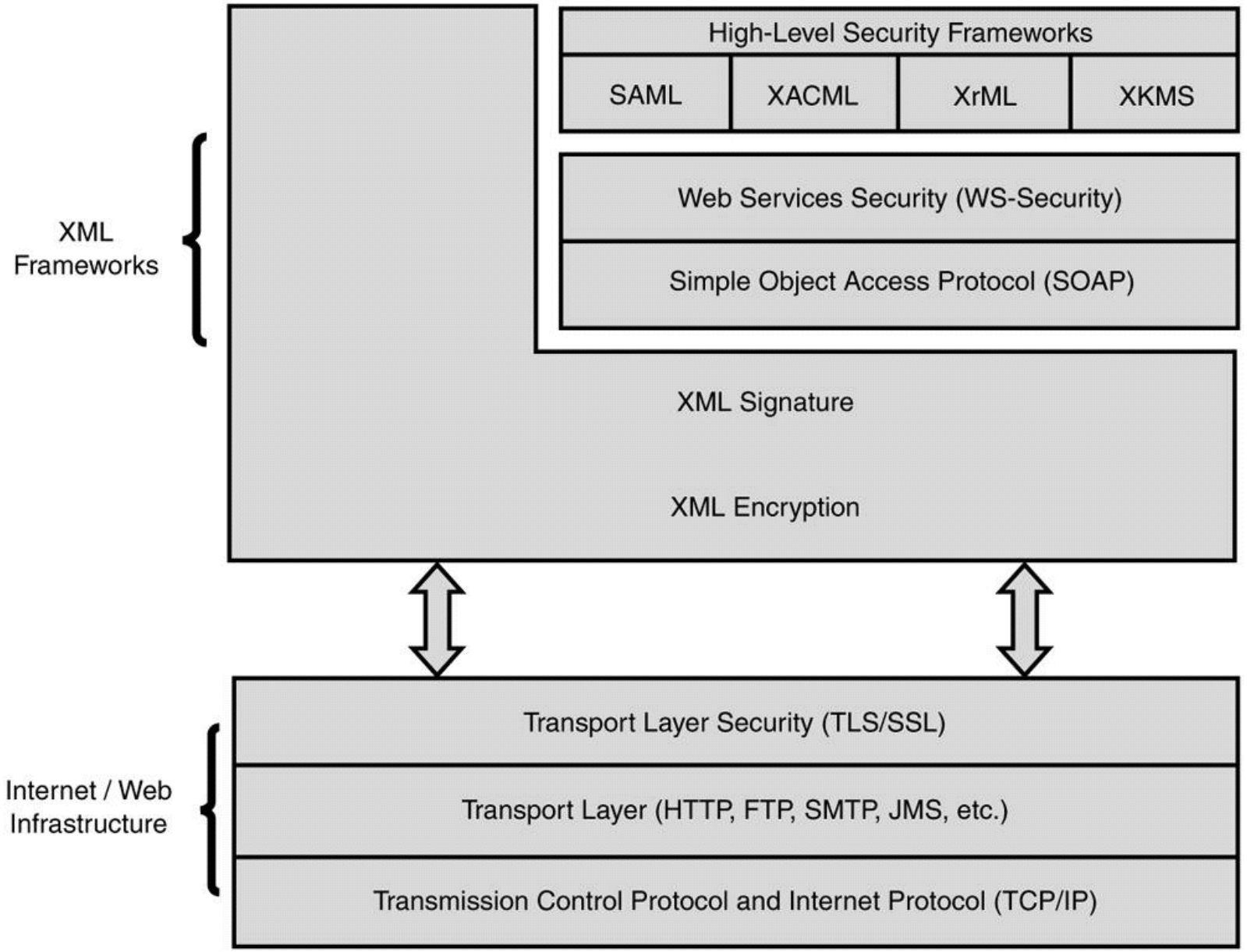
- El modelo SOAP permite una separación limpia entre la infraestructura de proceso y aplicación de proceso de mensajes.

•SOAP

asdc
Argentina Software Development Center



•SOAP


High-Level Security Frameworks
SAML
XACML
XrML
XKMS
Web Services Security (WS-Security)
Simple Object Access Protocol (SOAP)
XML Frameworks
XML Signature
XML Encryption
Transport Layer Security (TLS/SSL)
Transport Layer (HTTP, FTP, SMTP, JMS, etc.)
Transmission Control Protocol and Internet Protocol (TCP/IP)
Internet / Web Infrastructure

Tokens de Seguridad

La especificación WSS describe las reglas para procesar XML-Signature y XML-Encryption Estas reglas Deben ser seguidas cuando se utiliza cualquier token de seguridad.

1.)User Name Token

El elemento <wsse:UsernameToken> es introducido como una forma de provee un username.

Este token es opcionalmente incluido en el Header

```
<wsse:UsernameToken wsu:Id="...">
    <wsse:Username>...</wsse:Username>
</wsse:UsernameToken>
```

/wsse:UsernameToken

Este elemento se utiliza para representar una identidad declarada.

/wsse:UsernameToken/@wsu:Id

Un label para este token de seguridad. El wsu:Id permite un atributo modelo.

/wsse:UsernameToken/wsse:Username

Este elemento especifica la identidad declarada.

•SOAP

asdc
Argentina Software Development Center

El elemento <wsse:BinarySecurityToken> define dos atributos

1.) El ValueType Este atributo indica que los tokens de seguridad son por ejemplo ticket de Kerberos

2.) El EncodingType te avisa como los securiting tokens es encoded, por ejemplo, Base64Binary.

Tokens de Seguridad

2.) Binary Security Tokens

Para formato binario los tokens de seguridad que WS Security da son elementos del tipo <wsse:BinarySecurityToken> y <wsse:Security> en el Header

```
(001) <?xml version="1.0" encoding="utf-8"?>
(002) <S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..."
            xmlns:ds="...">
(003)   <S11:Header>
(004)      <wsse:Security
             xmlns:wsse="...">
(005)    <wsse:BinarySecurityToken ValueType="
http://fabrikam123#CustomToken "
     EncodingType="...#Base64Binary" wsu:Id=" MyID ">
(006)           FHUIORv...
(007)    </wsse:BinarySecurityToken>
(008)         <ds:Signature>
(009)            <ds:SignedInfo>
(010)               <ds:CanonicalizationMethod
                        Algorithm=
                          "http://www.w3.org/2001/10/xml-exc-c14n#"/>
(011)               <ds:SignatureMethod
```

Tokens de Securidad

3.) XML Tokens

En ciertos casos es deseable que tokens de seguridad sean incluidos en la <wsse:Security> del header y sean encriptados.

En ese caso el elemento <xenc:EncryptedData> Puede contener un security token en el header <wsse:Security>.

El standard define el uso de <xenc:EncryptedData> para encriptar
Los tokens de seguridad estan contenidos en el <wsse:Security>.

All <xenc:EncryptedData> Debería tener una clave de cifrado incorporados o debe ser referenciado por una clave de encripción separada.

•XML - Signature

•XML-Signature Syntax and Processing

•Recommendación del12 Febrero de 2002

•Este documento especifica la firma digital XML y reglas de procesamiento de la sintaxis. La Firmas en XML proporciona integridad, la autenticación de mensajes y / o servicios de autenticación de datos de cualquier tipo, ya sea situada en el XML, o en cualquier otro lugar.

•XML - Signature

asdc
Argentina Software Development Center

•Objetivos

- Asegurar que un mensaje no ha sido alterado o manipulado . (integritegridad)
- Protección contra los ataques que alteran un mensaje, sino mantener la integridad . (autenticación)
- Proporcionar un medio para que en la auditoría el mensaje no puedea ser repudiado . (autenticidad del firmante)

asdc
Argentina Software Development Center

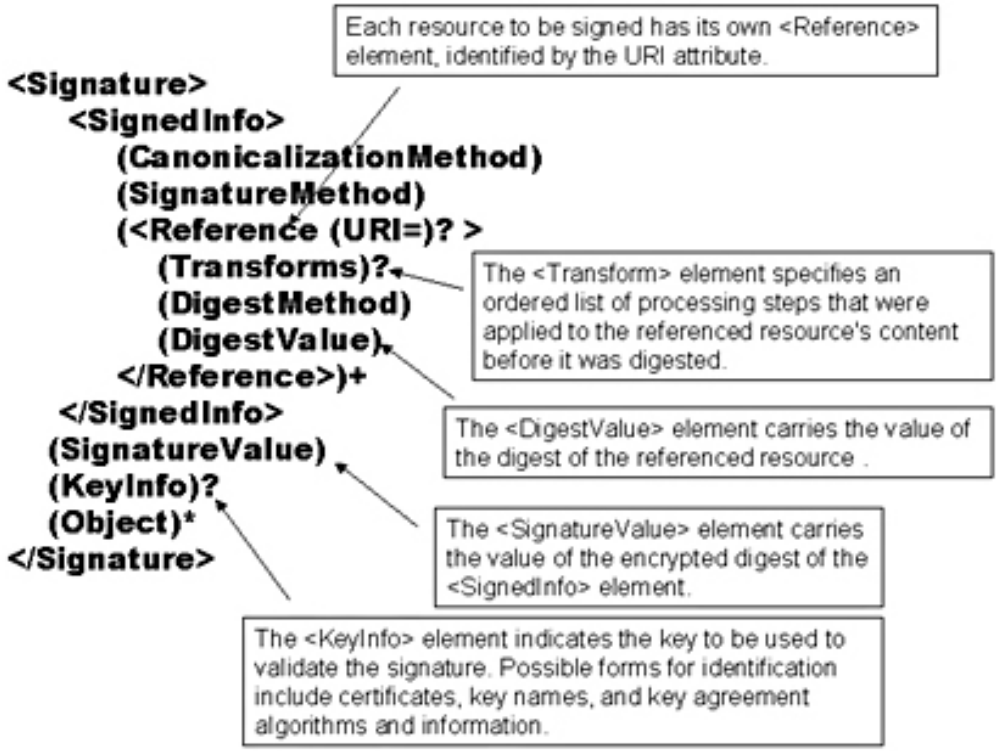
Structure

- <Signature>
- <SignedInfo>
- <CanonicalizationMethod/>
- <SignatureMethod/>
- (<Reference URI? >
- (<Transforms>)?
- <DigestMethod>
- <DigestValue>
- </Reference>)+
- </SignedInfo>
- <SignatureValue>
- (<KeyInfo>)?
- (<Object Id?>)*
- </Signature>

xmlns="http://www.w3.org/2000/09/xmldsig#"

•XML - Signature

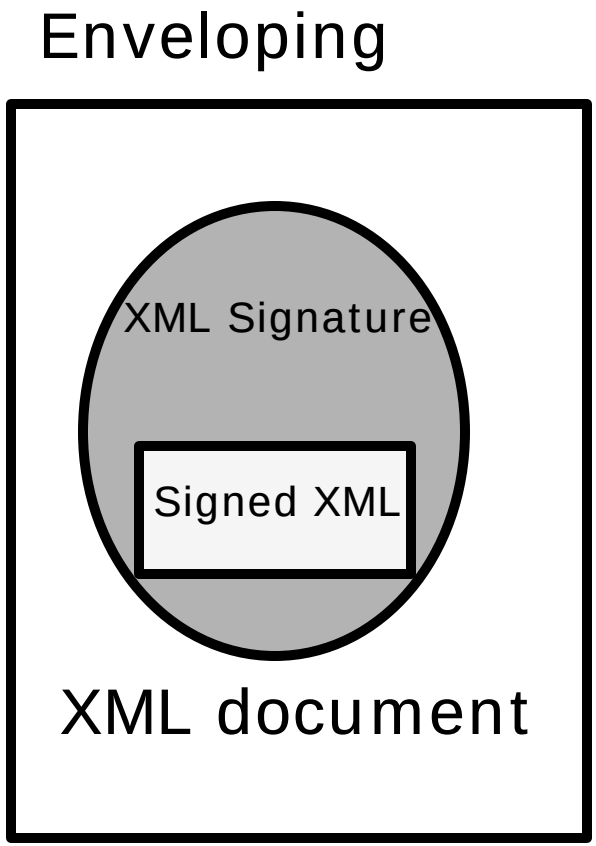
asdc
Argentina Software Development Center



asdc
Argentina Software Development Center

Types of Signatures

- Enveloping Signature
  - El dato vive dentro de la estructura XML signature
  - Bueno para la firma de datos que se están envasados en la carga útil del XML



asdc
Argentina Software Development Center

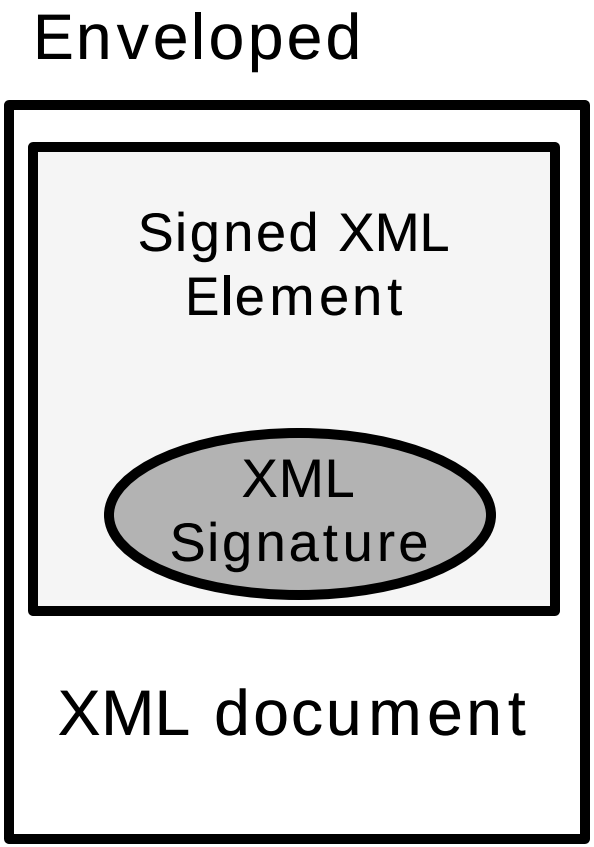
Enveloping Signature

```
<?xml version="1.0"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
                Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
    20010315"/>
    <SignatureMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
    sha1"/>
    <Reference URI="#myobj">
      <DigestMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>C2g9BLcGyGPCVKuF2byR1Ym+6pE=</DigestValue>
    </Reference>
  </SignedInfo>
   <SignatureValue>+R/XEOHDvR/jbmmpiuH4ZcRqC6c=</SignatureValue>
  <Object Id="myobj">Hello World!</Object>
</Signature>
```

asdc
Argentina Software Development Center

Types of Signatures

- Enveloped Signature
  - Los Datos viven fuera y contienen la estructura de XML siganture
  - Bueno para la firma de partes o la totalidad de un documento XML



Enveloped Signature

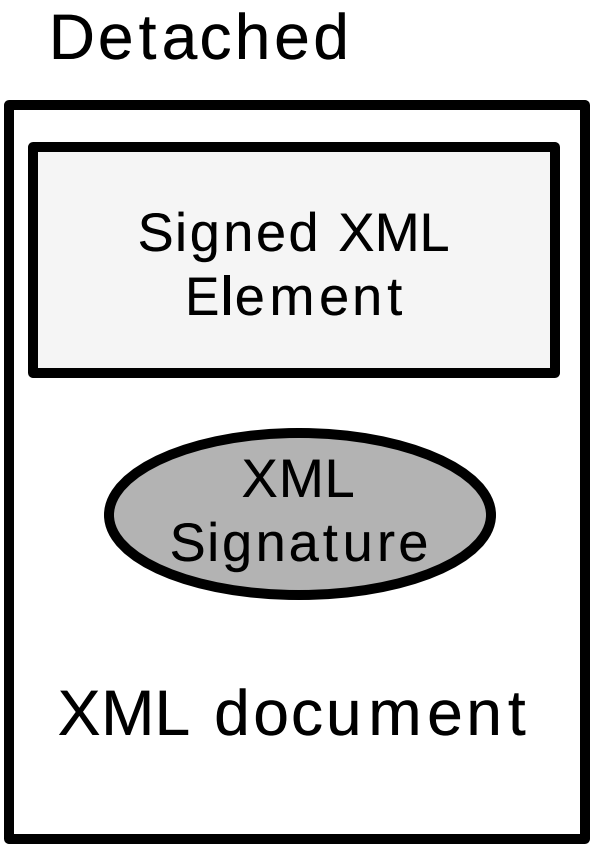
asdc
Argentina Software Development Center

- <?xml version="1.0"?>
- **<Envelope>**
- **<Data>content</Data>**
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
- <SignedInfo>
- <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
- <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
- **<Reference>**
- <Transforms>
- <Transform
- Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
- </Transforms>
- <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
- <DigestValue>MMMkB0ZPp82XrUvJMFqDIEuXy0o=</DigestValue>
- </Reference>
- </SignedInfo>
- <SignatureValue>mVPvfcVSXi9elKL+IcSCAzD4Jbk=</SignatureValue>
- </Signature>**</Envelope>**

asdc
Argentina Software Development Center

Types of Signatures

- Detached Signature
  - Los datos viven fuera y no contiene la estructura XML signature
  - Los datos pueden residir en un lugar remoto direccionable por URI



Ejemplo de Detached XML Signature

asdc
Argentina Software Development Center

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig# ">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="http://www.w3.org/TR/xml-stylesheet">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>60NvZvtdTB+7UnlLp/H24p7h4bs=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
  juS5RhJ884qoFR8flVXd/rbrSDVGn40CapgB7qeQiT+rr0NekEQ6BHhUA8dT3+BC
  TBUQI0dBjlml9lwzENXvS83zRECjzXbMRTUtVZiPZG2pqKPnL2YU3A9645UCjTXU
  +jgFumv7k78hieAGDzNci+PQ9KRmm//icT7JaYztgt4=
  </SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509IssuerSerial>
        <X509IssuerName>CN=Test RSA CA,O=Baltimore Technologies\, Ltd.,ST=Dublin,C=IE</X509IssuerName>
        <X509SerialNumber>970849928</X509SerialNumber>
      </X509IssuerSerial>
    </X509Data>
  </KeyInfo>
</Signature>
```

asdc
Argentina Software Development Center

Generación de firma paso a paso

- Para cada elemento
  - Aplicar las transformaciones necesarias
  - Calcular el hash para el output de la transformación
  - Guardar el hash en DigestValue
- Canonicalizar el elemento SignedInfo
- Calcular el hash del SignedInfo canonicalizado
- Firmar el hash de SignedInfo con mi clave privada y guardarlo en SignatureValue
- Agregar la información de la clave en KeyInfo
- recorger SignedInfo, SignatureValue, KeyInfo dentro de Signature

asdc
Argentina Software Development Center

Verificación de la firma Paso a Paso

- Canonicalizar el SignedInfo
- Realizar el hash de SignedInfo
- Verificar la firma en SignedInfo
  - Verificar el valor de la firma con la clave pública
  - Verificar la veracidad de la clave pública
- Para cada elemento de referencia que fue firmado
  - Aplicar las transformaciones necesarias
  - Calcualr el digesto de la salida de la trasforamción
  - Verificar si el hash que calculamos es igual al valor que setá en DigestValue

asdc
Argentina Software Development Center

XML Signature Algoritmos Cryptograficos

- Funciones de Hash
  - **SHA-1**, SHA-256, SHA-384, SHA-512, MD-5
- Métodos de firma asimétricos
  - **RSA with SHA-1**, SHA-256, SHA-384, SHA-512, MD-5
  - DSA with SHA-1, SHA-256, SHA-384, SHA-512, MD-5
- Methodos de firma simétricos
  - **HMAC with SHA-1**, SHA-256, SHA-384, SHA-512, MD-5

asdc
Argentina Software Development Center

XML Signature – Opciones de Key Info

- Clave Asimétrica
  - Key Name
  - Key Value
    - RSA
      - » Modulus, Exponent
    - DSA
      - » P,Q,Y,G
  - X509 Data
    - Certificado
    - Issuer/Serial
    - Subject Key Identifier
    - Subject Name
- Clave Simétrica
  - Key Name

•WS-Digital Signature

Cabecera de Seguridad

asdc
Argentina Software Development Center

El bloque de la cabecera <wsse:Security> provee un mecanismo para attachar información relacionada con seguridad

La especificación WS-Security define a <wsse:Security> com oun mecanismo para transmitir información de seguridad en un mensaje SOAP.

Este encabezado es, por diseño, extensible para soportar muchos tipos de información de seguridad

Por seguridad tokens de seguridad basados en XML, <wsse:Security> pueden ser agregados en el Header

```
<soap:Header>
    <wsse:Security>
      <wsu:Timestamp wsu:Id="T0"> .... </wsu:Timestamp>
      <wsse:BinarySecurityToken> .....
      </wsse:BinarySecurityToken>
      <xenc:EncryptedKey> .... </xenc:EncryptedKey>
      <ds:Signature> .... </ds:Signature>
    </wsse:Security>
  </soap:Header>
```

•WS-Digital Signature

asdc
Argentina Software Development Center

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#T0">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>LyLsF094hPi4wPU...</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#body">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>LyLsF094hPi4wPU...</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>Hp1ZkmFZ/2kQLXDJbchm5gK...</ds:SignatureValue>
  <ds:KeyInfo>
    <wsse:SecurityTokenReference>
      <wsse:Reference URI="#X509Token"/>
    </wsse:SecurityTokenReference>
  </ds:KeyInfo>
</ds:Signature>
```

asdc
Argentina Software Development Center

C14N – Espacio en blanco

- Insignificante espacio en blanco
- <a><b c="d">foo bar
- Es semanticamente equivalente a
- <a><b c="d"
- >foo bar</a
- >
- Relevante espacio en blanco
- <a><b c="d"> foo bar
-
- El proceso de Canonicalización normaliza los insignificantes espacios en blanco y conserva los relevantes espacios en blanco

asdc
Argentina Software Development Center

C14N – Prefijos del Namespace

- Los Prefijos son significantes
- <n1:a xmlns:n1="www.intel.com">foo bar</n1:a>
- No es lo mismo que
- <n2:a xmlns:n1="www.intel.com">foo bar</n2:a>
- Debido a que los prefijos pueden ser embebidos dentro de texto/atributo valor
- <n1:a xmlns:n1=www.intel.com language="n1:english">foo bar</n1:a>
- <n2:a xmlns:n2=www.intel.com language="n1:english">foo bar</n2:a>
- Canonicalización preserva el prefijo del namespace

asdc
Argentina Software Development Center

Tipos de Canonicalización

- Inclusive Canonicalization
  - Todos los nombres de los nodos en un ápice elemento se considera que tienen un efecto y aparecen en el nodo-conjunto
- Inclusive Canonicalization With Comments
  - Igual que el anterior, nodos comentados se incluyen en la salida
- Exclusive Canonicalization
  - El nodo de Namespace es considerado para tener un efecto y aparece en la salida donde el prefijo es visible en el nombre del elemento o en le nombre del atributo
  - Es el método más utilizado
- Exclusive Canonicalization With Inclusive List
  - Los namespace de los nodos son tratados como se especifica en Inclusive Canonicalization cuando el aparato esté especificado en la Inclusive List y como Exclusive Canonicalization

asdc
Argentina Software Development Center

C14N Input Rules

- Eliminar la declaración XML y de DTD
- Sustituir entity/character referencias con definiciones
- Convertir lineas rotas en x0A
- Eliminar secciones CDATA
- Normalizar attributo valor
  - Todas las líneas rotas son normalizadas
  - Comenzar con un valor vacío normalizado
  - Para cada caracter , entidad ref, char ref
    - Todos los caracteres referenciados son reemplazados
    - Reemplazar las entidades referenciadas y recurrentemente aplicar este paso
    - Por cada caracter espacio en blanco, tab horizontal, nueva línea, retorno de carro o espacio, añadir un carácter de espacio para el valor normalizado
  - Si el tipo de atributo no es CDATA, descartar los principales caracteres de espacio y los rezagados, y reemplaza cualquier secuencias internas del espacio con un único carácter de espacio

asdc
Argentina Software Development Center

Q&A

Tks

applause please