Seguridad en entornos SOA

Agenda

- Descripción SOA
- Desafíos de Seguridad
- TLS vs MLS
- Estándares relacionados con WS
  - WS-Security
  - XML Signature
  - XML Encryption
  - WS-*
  - SAML
  - XACML
- Ingeniería de Seguridad

Descripción SOA

- Un tipo especifico de sistema distribuido que permite exponer y consumir funcionalidades, como un conjunto de servicios
- Un servicio es una funcionalidad concreta que puede ser descubierta en la red y que describe tanto lo que puede hacer como el modo de interactuar con ella.
- Para interaccionar usa protocolos y formatos de datos estándar

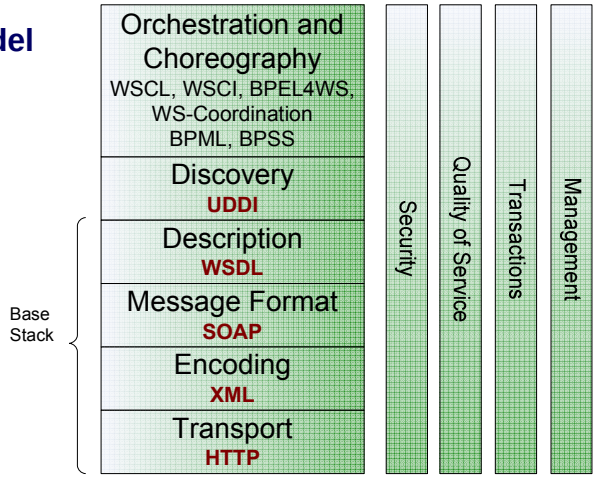
Servicios WEB

- Conjunto de aplicaciones o tecnologías con capacidad para interoperar en la Web
- Proporcionan mecanismos de comunicación estándares entre diferentes aplicaciones, que interactúan entre sí para presentar información dinámica al usuario

- Los WS se han convertido en el estandarte de SOA, ya que permiten implementar la base tecnológica establecida

Servicios WEB y SOA

- **Construcción del ecosistema de servicios Web**

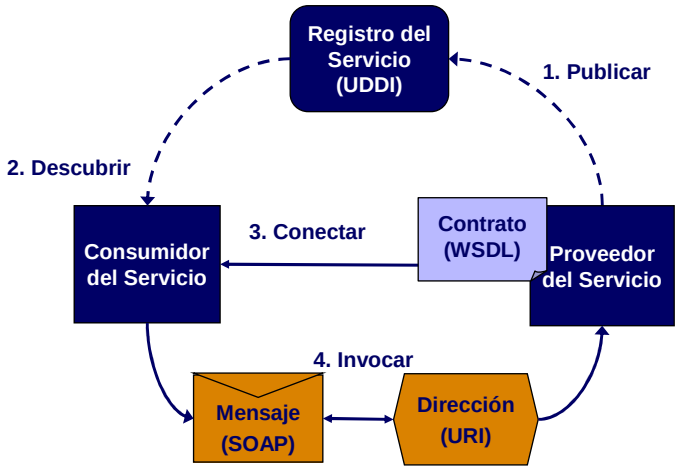


Adapted from "XML and Web Services Unleashed", SAMS Publishing

Fuente: SEI (Software Engineering Institute)

Servicios WEB y SOA

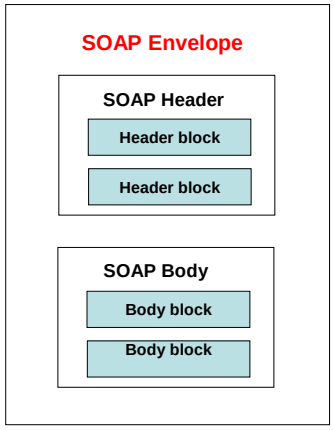
- **Ciclo de vida**



Mensajes SOAP

SOAP: Simple Object Access Protocol

- **Estructura del mensaje SOAP**



Sobre SOAP (*Envelope*)

Envelope es el elemento raíz del mensaje SOAP:

```
<SOAP-ENV: Envelope
xmlsns:SOAP-ENV="http://WWW.w3.org/2001/12/soap-envelope">
```

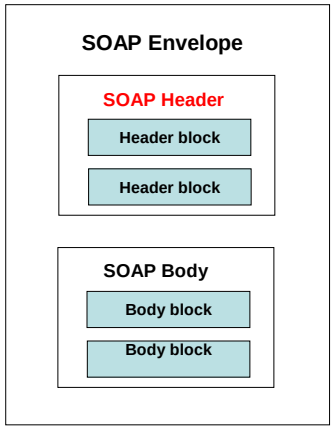
La función de esta etiqueta es definir los namespaces que van a ser utilizados. Ejemplos típicos:

1) xmlns:SOAP-ENV
2) xmlns:xsi (XML instaces)
3) xmlns:xsd (XML Schema)

Mensajes SOAP

SOAP: Simple Object Access Protocol

- **Estructura del mensaje SOAP**



Cabecera SOAP *(Header)*

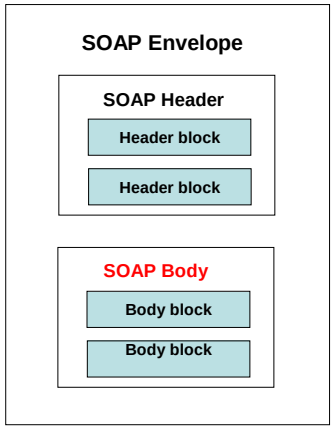
La cabecera contiene información específica de la aplicación (información de pagos, routing, etc…).

```
<SOAP-ENV:Header>
<SOAP-SEC:Signature xmlns:SOAP-
SEC="http://schemas.xmlsoap.org/soap/security/2000-12" SOAP-
ENV:actor="some-URI" SOAP-ENV:mustUnderstand="1"> <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2000/CR-
xml-c14n-20001026"> </ds:CanonicalizationMethod>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<ds:SignatureValue>MC0CFFrVLtRlk=...</ds:SignatureValue>
</ds:Signature> </SOAP-SEC:Signature> </SOAP-ENV:Header>
```

Mensajes SOAP

SOAP: Simple Object Access Protocol

- **Estructura del mensaje SOAP**



Cuerpo SOAP (*Body*)

El cuerpo SOAP es la principal carga útil del mensaje. El cuerpo contiene la información que debe ser procesada por el destinatario final.

```
<SOAP-ENV: Envelope
...
<SOAP-ENV:Body>
<m:GetStock xmlns:m=www.esi.es/OrderStock>
                <ProductId>12x898ff</ProductId>
</m:GetStock>
</SOAP-ENV:Body>
</SOAP-ENV: Envelope>
```

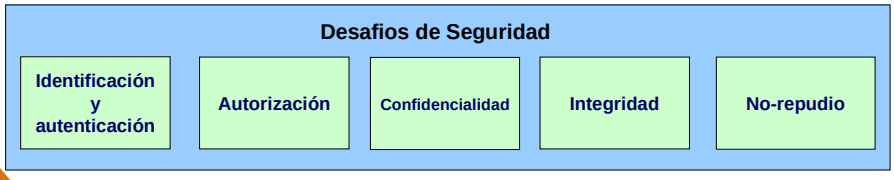


Soy
vulnerable

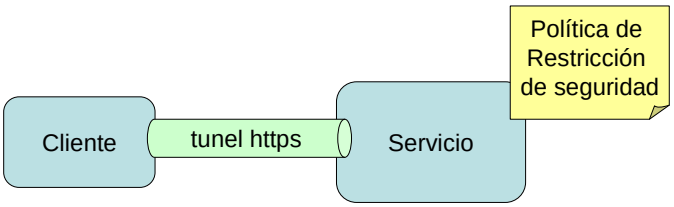

MAI → SEPT.
MAY → SEPT.

Desafios de seguridad

- **Retos de seguridad en Servicios Web:**
  - **Identificación y autenticación:** Garantizar la identidad de quien realiza la transacción (procesos, dispositivos, personas)
  - **Autorización:** Permiso para acceder a un recurso: puede ser concedido directa o indirectamente por una aplicación o un administrador
  - **Integridad:** Garantizar que la información intercambiada no es manipulada durante el trayecto
  - **No-repudio:** Garantizar que no se pueda rebatir la procedencia (la propiedad) de la información
  - **Confidencialidad:** Proteger la información privada de acceso no autorizados

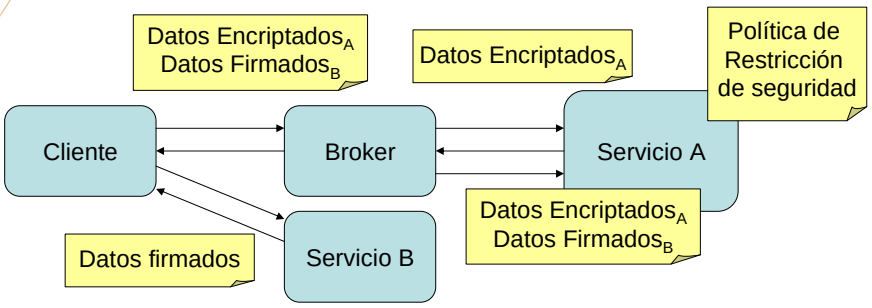


Seguridad a nivel de transporte



- **Autenticación:** básica, digest o autenticación de cliente
- **Autorización:** control de acceso basado en roles
- **Confidencialidad:** SSL
- **Integridad:** SSL
- **No repudio:** No está soportado

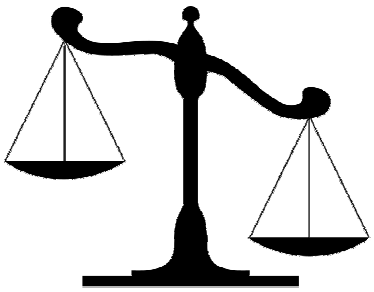
Seguridad a nivel de mensaje



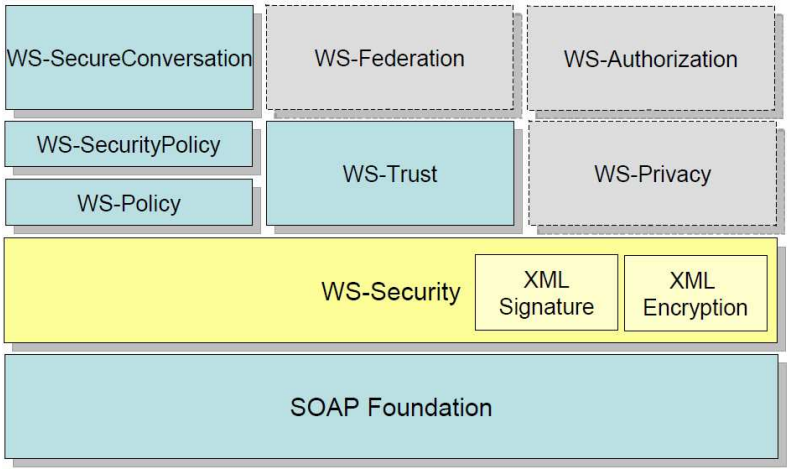
- **Autenticación:** SAML, WS-Tokens, XML Signature
- **Autorización:** J2EE security, SAML Assertions
- **Confidencialidad:** XML Encryption
- **Integridad:** XML Signature
- **No repudio:** XML Signature

Comparativa

- **Soporte para diferentes protocolos**
- **Seguridad extremo a extremo cuando los mensajes son procesados por intermediarios**
- **Posibilidad de firmar y/o encriptar partes del mensaje**



Estándares relacionados con WS



Fuente: http://www.ibm.com/developerworks/library/ws-secroad/

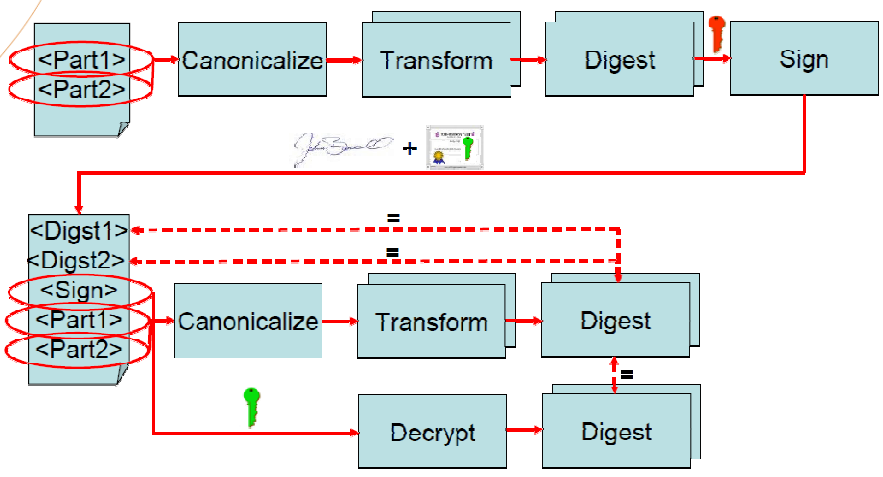
WS-Security

- OASIS SOAP Message Security 1.1 Standard, Feb. 2006
- Objetivos
  - Establecer un sistema de seguridad para el intercambio de mensajes SOAP
  - Integrar múltiples soluciones de seguridad (formatos de tokens, técnicas de encriptación, etc.)
- Motivación
  - Establecer un conjunto de extensiones SOAP para la autenticación de mensajes, la integridad, confidencialidad, tokens de seguridad, etc.
- Tecnologías
  - XML Signature
  - XML Encryption

XML Signature & Encryption

- XML_Sig: Recomendación W3C, 12 de Febrero 2002
  - Objetivos
    - Asegurar la integridad de los mensajes
    - Autenticación de las fuentes de datos
    - No-repudio
- XML_Enc: Recomendación W3C, 10 de Diciembre 2002
  - Objetivos
    - Confidencialidad
    - Asegurar la seguridad extremo a extremo

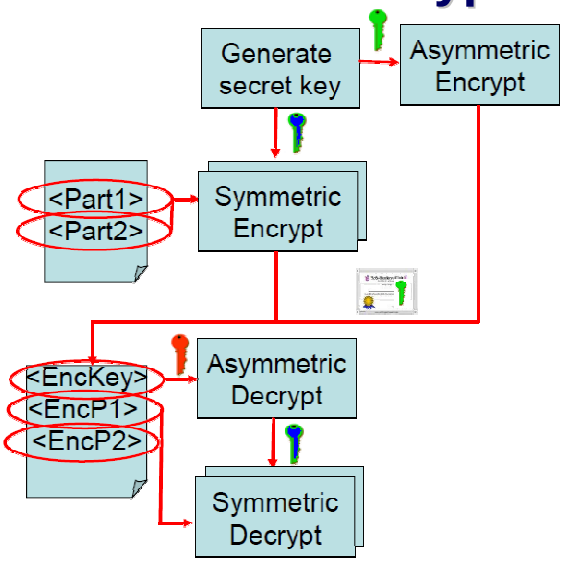
XML Signature



Ej. 1: XML Signature

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-26460367">
    <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="#Id-26936546">
      <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>hSTR6/8GUorQk9z0cpvG3RahGC4=</ds:DigestValue>
     </ds:Reference>
     <ds:Reference URI="#Timestamp-21905217">
      <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>pm0JZfzS0/dsehn0Y7QH6lHQoZY=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
     EV1Xz+KPgPM/SvpB/G2muZVtVRcfHT+bzAmNS3PxBWq/aXsVhCRdcja6uc/ZDfU3yWzFx+x2xVfK
     5+I14pgSuZkQrFOokEjZo+LdqrNpdkIfjB/BO46fCEiwTU76jk6G7Zyfuoi3J8RjYc5Txzj730Se
     CKEzj7iWhi0c/rOGhtk=
    </ds:SignatureValue>
    <ds:KeyInfo Id="KeyId-18055655">
     <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd" wsu:Id="STRId-24417480">
      <wsse:Reference URI="#CertId-148082" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-x509-token-profile-1.0#X509v1" />
     </wsse:SecurityTokenReference>
    </ds:KeyInfo>
</ds:Signature>
```


XML Encryption



Ej. 1: XML Encryption

```
<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
    wssecurity-utility-1.0.xsd" wsu:Id="Id-14247087">
  <xenc:EncryptedData Id="EncDataId-14247087"
    Type="http://www.w3.org/2001/04/xmlenc#Content">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-
    cbc" />
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-
    open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
    <wsse:Reference URI="#EncKeyId-urn:uuid:2EFC2B478B5DB54F2712670975399482" />
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>
        IydqtueDrqu3AfNVObVIi5OX4jtpvITD0iDIFt9EEB3hc1Sw3WpJpA30RqPTyrNXtvsXX/keu65r
    O2dhxSH99eUkJIt17YjnVMYyGx+vFjM+bIGNRLa4alUOK9y/cNMQUU+HAMjx8vZLbIfwewsyuBK5
    AP3FTQqiIolXaX6yXtCL017PngJmvw2K8zlTAt/aQZIz0pdzuU9H5NoOX+JWKZy9eHEBztHdaXXJ
    SbcMcYj9i+MlKCDJHx46/gSdYAf9L4ZQq/Xj4+kxCnRgIriSVzQzbhCXIIxkrtSoetGoWhayyMyW
    5O0QJmOI93D9XQf5vRdeLxwv6TboorjsYS02dPFdd4PGE31tE9irf9QlDhNHmT6O4El6FRE3EV8b
    VYifmMbm75FYyxkeStUqoU+EGlBuJYhuJUMd0Yu4vba9nHcNF2bXEz9NobNXqBTkDrgAIBq3NseP
    l7w=
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</soapenv:Body>
```


Ej. 1: XML Encryption (key info)

```
<xenc:EncryptedKey Id="EncKeyId-
    urn:uuid:2EFC2B478B5DB54F2712670975399482">
      <xenc:EncryptionMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <wsse:SecurityTokenReference>
          <wsse:KeyIdentifier 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/oasis-wss-
    soap-message-security-
    1.1#ThumbprintSHA1">CJ+I51M5honzWpG12gKyLwsXErk=</wsse:KeyIden
    tifier>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>
    VyihDq2ApXI/2s9MLpGf90dVrGRwdmBwb9P6wBH58xG7yY2z5gfdPQpYiWvR
    C4MSeP6p+w4xgsj0fs2bLiGwefWLtds2WRNeDv3vdOtiMUZndX88GipFhz73Bv
    6uRJo9GPOOo7JkwVZEev9N5sLp0Xd099PRgnGM8isOnziUKYU=
    </xenc:CipherValue>
      </xenc:CipherData>
      <xenc:ReferenceList>
        <xenc:DataReference URI="#EncDataId-14247087" />
      </xenc:ReferenceList>
    </xenc:EncryptedKey>
```

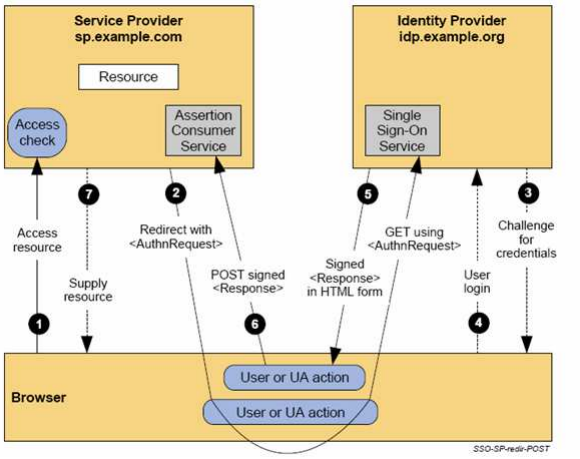
WS-Policy

- **WS-Policy**
  - Definir los mecanismos necesarios para permitir especificar la información relativa al dominio de aplicación.
    - Modelo de políticas (XSD) + Algebra
- **WS-SecurityPolicy**
  - Definir un subconjunto de patrones (*assertions*) que representan formas comunes de securizar mensajes
- **WS-SecureConversation**
  - Definir cómo se establecen contextos de seguridad
    - Gestión de las claves

SAML

- Security Assertion Markup language OASIS TC (Technical Commitee) SAML V2.0 Standard, March 2005
- **Objetivos**
  - Intercambio de información de autenticación y autorización entre dominios independiente de protocolo y plataforma
  - Extender el uso de federación de entidades (Single Sign On) mas allá de las intranets
- **Motivación**
  - Integrar nuevas características de seguridad sin el desarrollo de líneas y líneas de código => código reutilizable + servicios genéricos
  - Integración cross-domain de las soluciones Web
- **Tecnologías (opcionales)**
  - Seguridad a nivel de transporte
    - SSL 3.0 or TLS 1.0
  - Seguridad a nivel de mensaje
    - XML Signature and XML Encryption

SAML



SAML

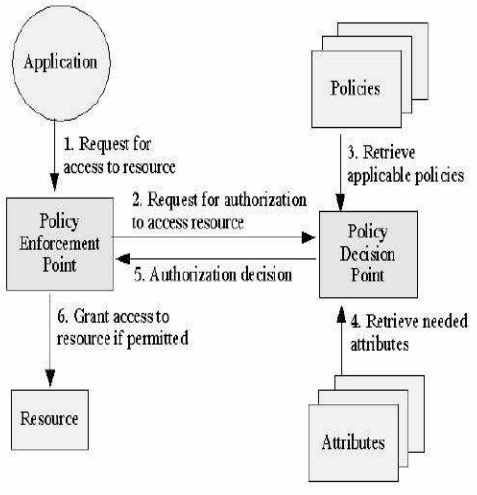
- Disección de SAML
  - SAML Profiles
  - SAML Bindings
  - SAML Protocols
  - SAML Assertions

XACML

- eXtensible Access Control Markup language OASIS XACML V2.0 Standard, Febreruary 2005
- **Objetivos**
  - Intercambio de información de autorización entre dominios
  - Establecer mecanismos de autorización complejos
- **Motivación**
  - Integrar nuevas características de seguridad sin el desarrollo de líneas y líneas de código => código reutilizable + servicios genéricos
  - Integración cross-domain de las soluciones Web

XACML

- Componentes
  - Policy Enforcement Point
  - Policy Decision Point
  - Policy Administration Point
  - Policy Information Point



Authorization inside Fedora

XACML

Request Schema

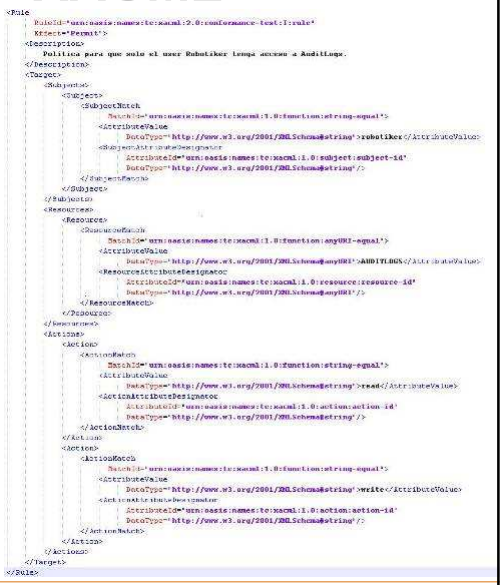
Request
- Subject
- Resource
- Action

Policy Schema

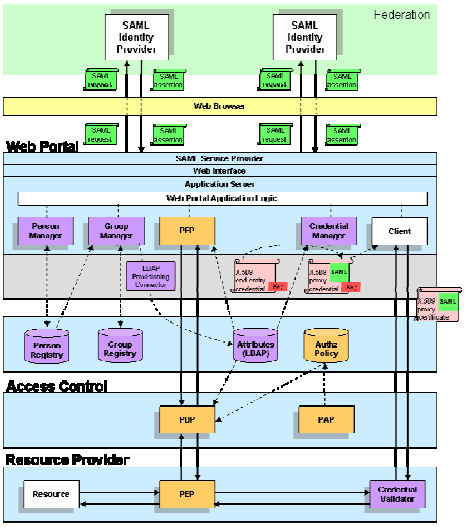
PolicySet (Combining Alg)
- Policy (Combining Alg)
  - Rule (Effect)
  - Subject
  - Resource
  - Action
  - Condition
  - Obligation

Response Schema

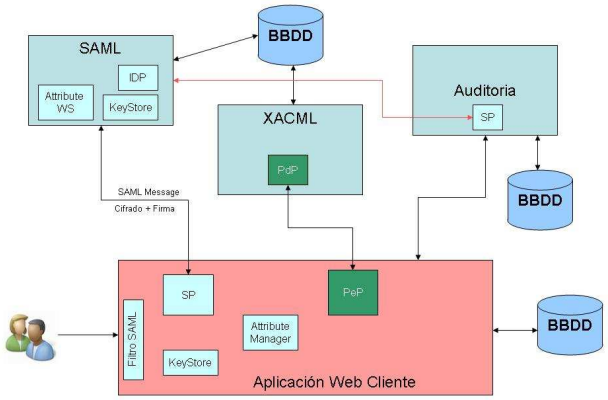
Response
- Decision



XACML + SAML



REALTH Demo
XACML + SAML



Reference Implementations

- Web-Services Security
  - Eclipse + Axis2 + Rampart
    - Eclipse IDE -- http://www.eclipse.org/webtools/
    - Axis2 : Web Services Engine -- http://ws.apache.org/axis2/
    - Rampart : WS Securtiy Engine -- http://ws.apache.org/axis2/modules/rampart/1_3/security-module.html
  - Netbeans + Glawfish
    - NetBeans -- http://netbeans.org/features/index.html
    - Glassfish -- https://glassfish.dev.java.net/
- SAML
  - JBOSS -- http://www.jboss.org/picketlink
- XACML
  - Sun Java XAMCL implementation -- http://sunxacml.sourceforge.net
  - HERAS SF -- http://www.herasaf.org/index.php
  - JBOSS -- http://www.jboss.org/jbosssecurity/downloads/JBoss%20XACML/

Ingenieria de Seguridad

- ¿Porque la seguridad lógica no es suficiente?
  - Algunas vulnerabilidades se manifiestan a si mismas solo en producción donde los sistemas interconectados intercambian datos de todo tipo.
  - La opinión publica de la empresa puede verse muy afectada con estos bugs en producción
  - La eslabón mas débil de la cadena determina la resitencia de toda la cadena
- "Two pieces of code put together, one with a limited spec for strong data typing, and the other with weak handling of output, result in a new set of behaviors that fail to meet specification, though each unit of code individually meets it's own specification". – Arian Evans
- Las vulnerabilidades se presentan mas evidentemente en entornos no controlados
  - Cloud computing
  - Web Services

Ingenieria de Seguridad

- Inspección del Código Fuente
  - Static
    - PC Lint & Flexelint - Gimpel -- http://www.gimpel.com/html/products.htm
    - Prevent - Coverity -- http://www.coverity.com/products/coverity-prevent.html
  - Dynamic
    - Valgrind – http://valgrind.org
    - Purify IBM http://www.ibm.com/software/awdtools/purify
  - Profiling
    - Oprofile -- http://oprofile.sourceforge.net/
    - VTune – INTEL -- http://software.intel.com/en-us/intel-vtune/
- Post Devolopment analysis
  - Test Framework
    - Check -- http://check.sourceforge.net/
    - JUnit -- http://www.junit.org/
  - Coverage
    - Gcov -- http://gcc.gnu.org/onlinedocs/gcc/Gcov.html
    - EMMA -- http://emma.sourceforge.net/

Conclusiones

Desafío	Estándares relacionados	
AUTENTICACIÓN	SAML, WS-Security (Tokens)	WS-Policy WS-SecurityPolicy
AUTORIZACIÓN	XACML	
CONFIDENCIALIDAD	XML Encryption	
INTEGRIDAD	XML Signature	
NO-REPUDIO	XML Signature	

Bibliografía

1. **OASIS Web Services WG:** http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
2. **XACML specification:** http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
3. **W3C XML Encryption WG:** http://www.w3.org/Encryption/2001/
4. **W3C XML Signature WG:** http://www.w3.org/Signature/
5. **Online Community for SAML OASIS Standard:** http://saml.xml.org/
6. **Security Challenges, Threats and Countermeasures Version 1.0:** http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf


Ibai Iturricha
R&D Projects
Ibai.Iturricha@esi.es
Borja Urkizu
R&D Projects
Borja.Urkizu@esi.es
Parque Tecnológico, # 204
E-48170 Zamudio
Bizkaia (Spain)
Tel.: +34 94 420 95 19
Fax: +34 94 420 94 20
www.esi.es
ESI
European
Software
Institute
tecnalia