Seguridad en JEE

Sesión3: Identity Management con SAML

Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Identity Management (SSO)

- Motivación de la IM:
  - Proliferación de aplicaciones web al alcance de un **mismo** usuario:
    - Banca, líneas aéreas, seguros, hospitales…
  - El usuario se ve obligado a mantener diversas **identidades digitales**:
    - Esto limita el desarrollo del B2B ya que el usuario debe fichar **(sign-on)** en cadena.
    - Esto no es solo problemático para el usuario sino para los sistemas de gestión (muchas veces heterogéneos):
      - P.e. un cambio de password debería propagarse para mantener la consistencia.
  - Todo sería más fácil con una **identidad única**.

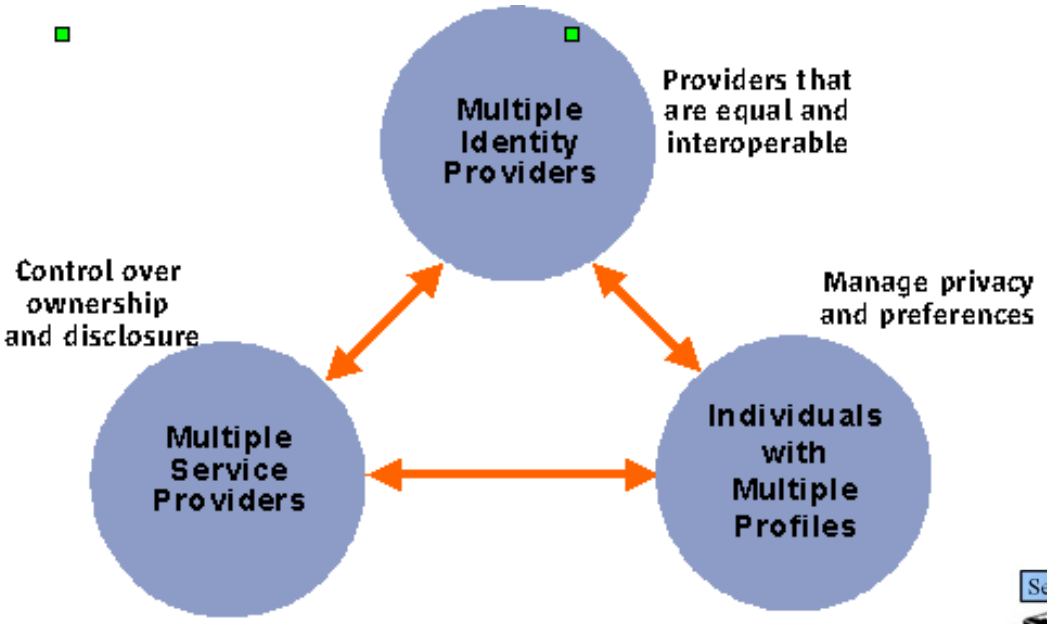
Identity Management (SSO)

- Conceptos clave:
  - Identidad de red (NI):

    Solución software que incorpora procesos de negocio en red y la tecnología necesaria para gestionar tanto el **ciclo de vida** de las identidades como las **relaciones** entre estas y las aplicaciones.
  - Identidad federada (FI):

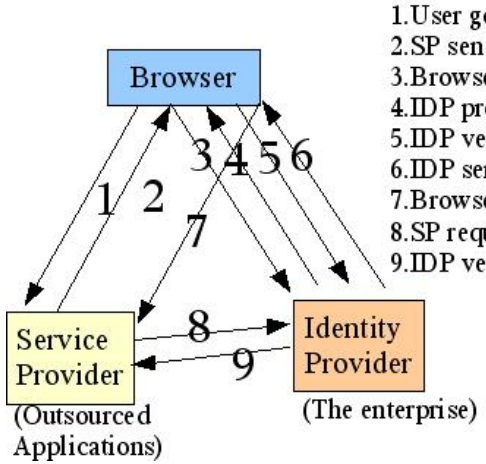
    Uso inter-dependiente de información de identidad entre compañías y aplicaciones o bien a través de diversas infraestructuras en Internet:
    - Extiende el concepto de identidad de red dentro de una compañía a múltiples empresas con infraestructuras de seguridad distintas.
    - Incluiría gestionar cómo las identidades aparecen, desaparecen o son revocadas por un **proveedor de identidad.**

Identity Management (SSO)

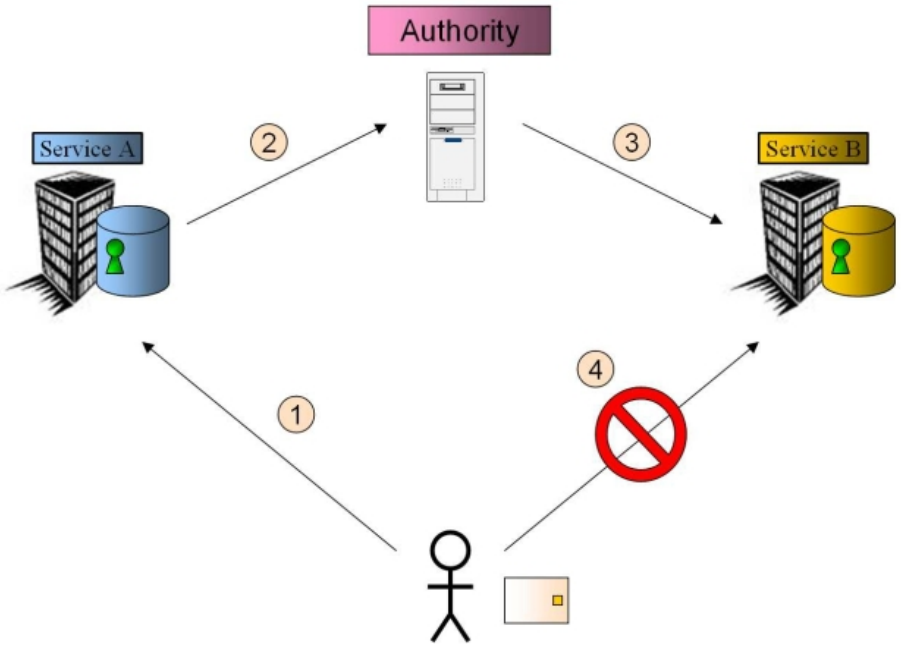


LIBERTY ALLIANCE PROJECT

Federated Identity using Liberty



1.User goes to SP
2.SP sends redirect to IDP
3.Browser redirects to IDP
4.IDP prompts for login
5.IDP verifies credentials
6.IDP sends redirect to SP
7.Browser redirects to SP
8.SP requests session verification
9.IDP verifies session



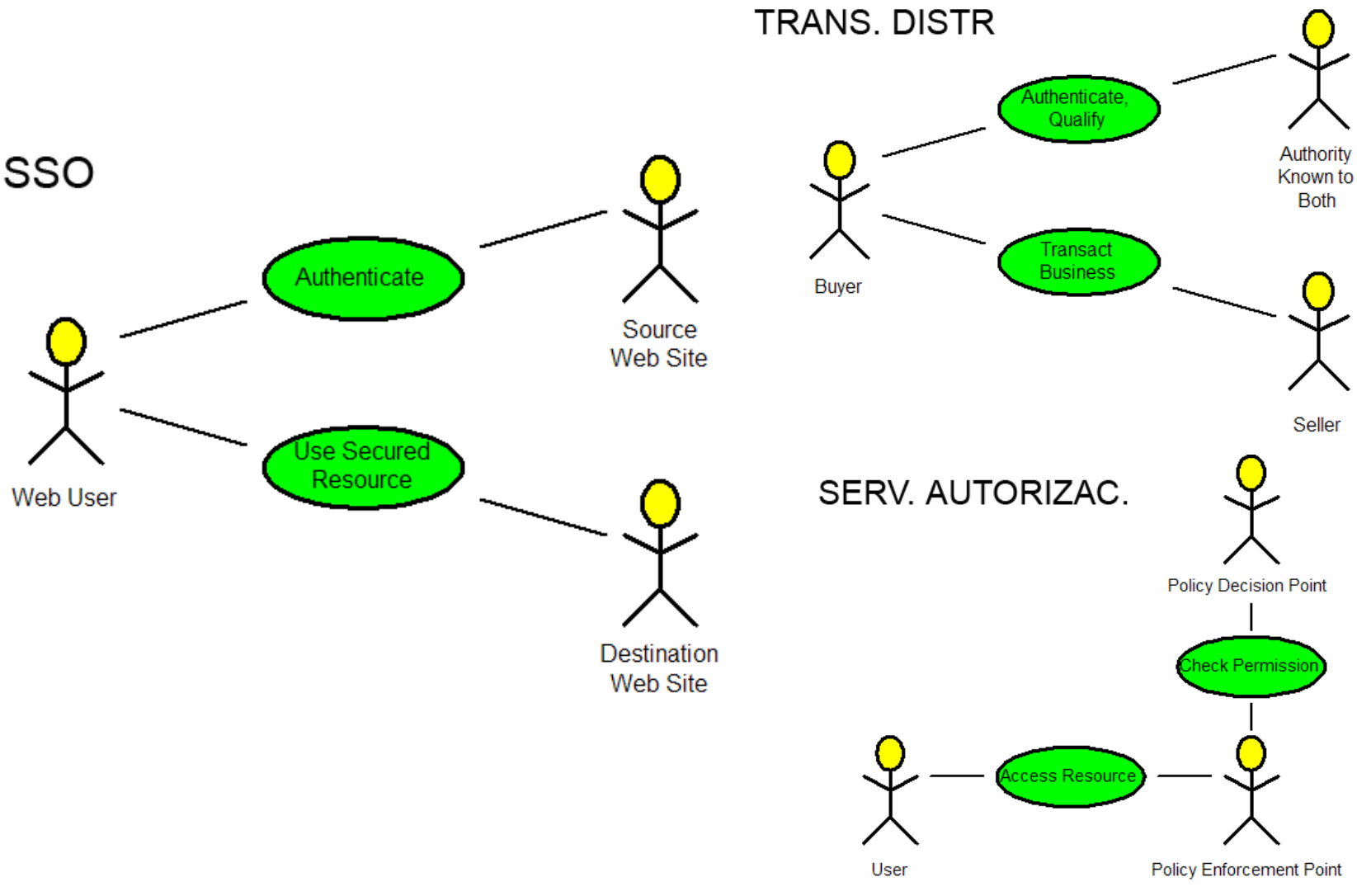
Identity Management (SSO)

- Conceptos clave:
  - Gestion de identidad (IM) = (manejar NI & FI)
    - **Administración** de las identidades.
    - **Mapeo** de estas a usuarios y grupos.
    - **Provisión** de cuentas en diferentes sistemas incluyendo usuarios y passwords.
    - Aplicación de **políticas de seguridad**
    - **Administración delegada** (local o distribuída).
    - Tracking (**auditing**) del ciclo de vida de la identidad.
    - **SSO:** Single-Sign-On
    - **Global** log-out.
  - **SAML:** Security Assertion Markup Language

Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Motivación de SAML: Escenarios



Motivación de SAML: Escenarios

- SSO:

  Un analista que ha hecho login en un sitio PepitoCO® tiene acceso directo a la información que hay en el sitio JuanitoCO® , ambos de la **misma compañía** CO

- Transacción distribuída:

  Los empleados de PepitoCO® pueden hacer pedidos directamente de OficinaOF si tienen suficiente presupuesto para el pedido.

- Servicio de autorización:

  Los empleados de PepitoCO® pueden hacer pedidos directamente de OficinaOF quien se encarga de pedir autorización.

Motivación de SSL: Escenarios

- ¿Qué necesitamos para implementarlos?:
  - **Formato XML estándar.** Solamente datos viajando por el cable. Se dispone de un amplio espectro de herramientas para manejar XML.
  - **Protocolo estándar de intercambio de mensajes**. Debe especificarse claramente como se pide y cómo se obtiene la información que uno necesita.
  - **Reglas de interoperatividad.** Sobre cómo se mueven los mensajes y los protocolos de transporte.
- SAML:

  Es un framework basado en XML para el intercambio de mensajes de seguridad.

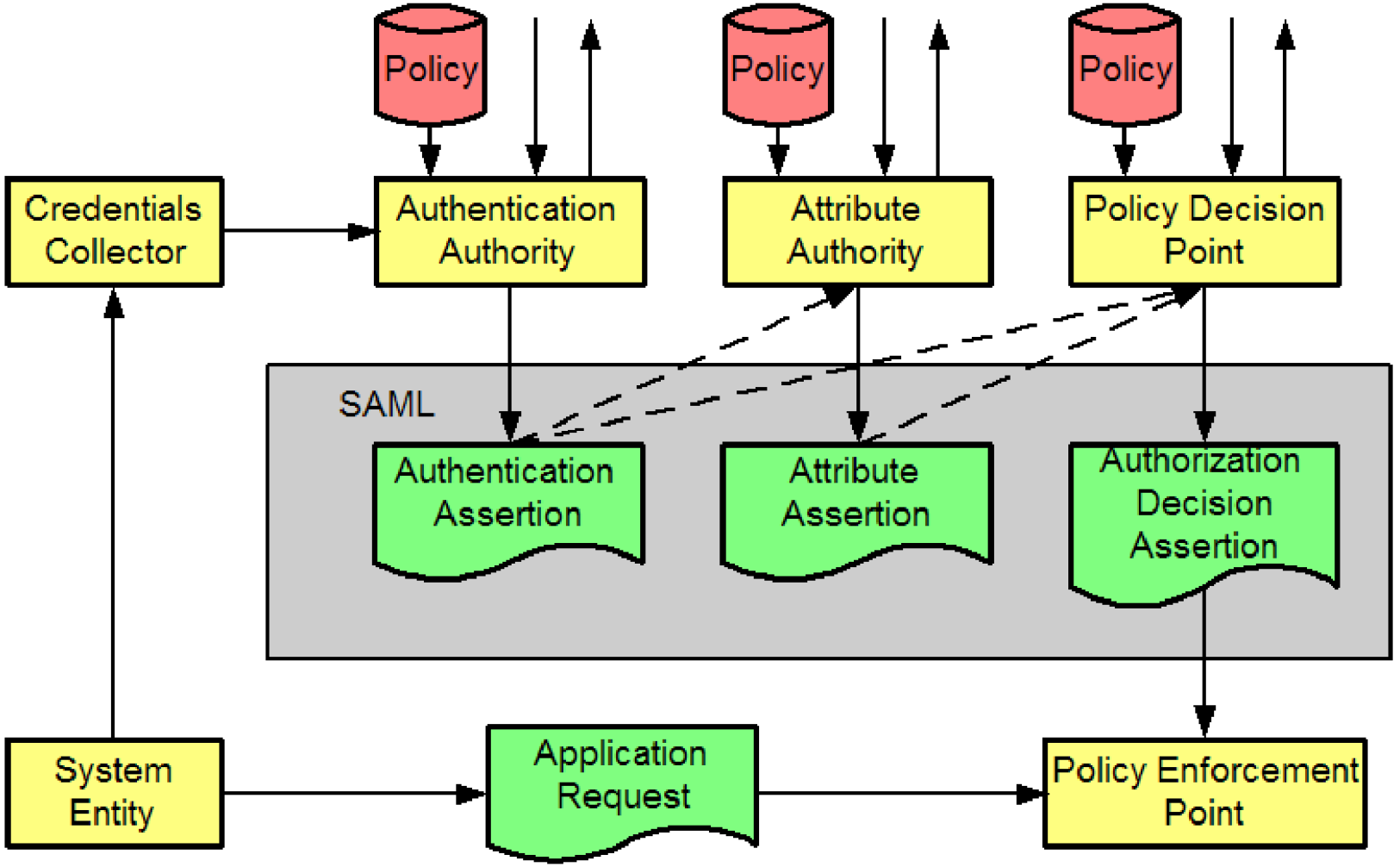
Motivación de SAML: Escenarios

- Características de SAML
  1. **Assertions.** Se basa en afirmaciones/asertos codificadas en XML.
  2. **Request-reply**. Usa un protocolo de intercambio de petición/respuestas
  3. Se basa en reglas para usar assertions con protocolos estándar y frameworks de mensajes también estándar.
- Especificaciones:
  - La primera especificación de SAML fue la 1.0 (Nov. 2002), pero el servidor BEA-Weblogic 9.2 implementa la 1.1 (Sept. 2003) dando soporte a la identidad de red.
  - La última especificación aprobada por OASIS es la 2.0 (Marzo 2005).

Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Arquitectura: Modelo conceptual SAML



Arquitectura: Modelo conceptual SAML

- Credential Collector:

  Objeto del sistema que recoge las credenciales del usuario para autentificarlas con las **Authentication Authority, Attribute Authority** y **Policy Decision Point** (PDP)

- Authentication Authority:

  Entidad del sistema que produce **asertos de autentificación**.

- Attribute Authority:

  Entidad del sistema que produce **asertos de atributo**.

- Session Authority:

  Entidad del sistema (p.e. un proveedor de identidad) que mantiene el estado de la sesión.

- Attribute Repository:

  Repositorio donde se almacenan los asertos de atributo

Arquitectura: Modelo conceptual SAML

- Policy Repository (Policy):

  Repositorio donde se almancenan las **políticas de seguridad**.

- Policy Decision Point (PDP):

  Entidad del sistema toma **decisiones de autorización** para sí misma o para otras entidades del sistema que requieren autorización.

- Policy Enforcement Point (PEP):

  Entidad del sistema que aplica las políticas de seguridad para conceder o revocar el acceso al peticionario de recursos.

- Policy Administration Point:

  Entidad del Sistema en donde se definen y mantienen las políticas (p.e. reglas de control de acceso para un determinado recurso)

Arquitectura: Modelo conceptual SAML

- Funcionamiento:
  1. Una **entidad** del sistema (p.e. cliente) pretende enviar una **petición** de aplicación para acceder a un **recurso**.
  2. Para ello presenta sus **credenciales** (usuario, password) al **Credentials Collector** quien procede a la **autentificación**.
  3. La autentificación se produce a través de la **Authentication Authority** (que genera un aserto), la **Attribute Authority** (que genera otro aserto) y el **PDP** que genera otro, antes de que se conceda al cliente acceso (decisión basada en una **política**).
  4. El **PEP** concederá o no el acceso de acuerdo con los derechos de acceso garantizados por la política.

SAML es un modelo conceptual de emisión y consumo de asertos

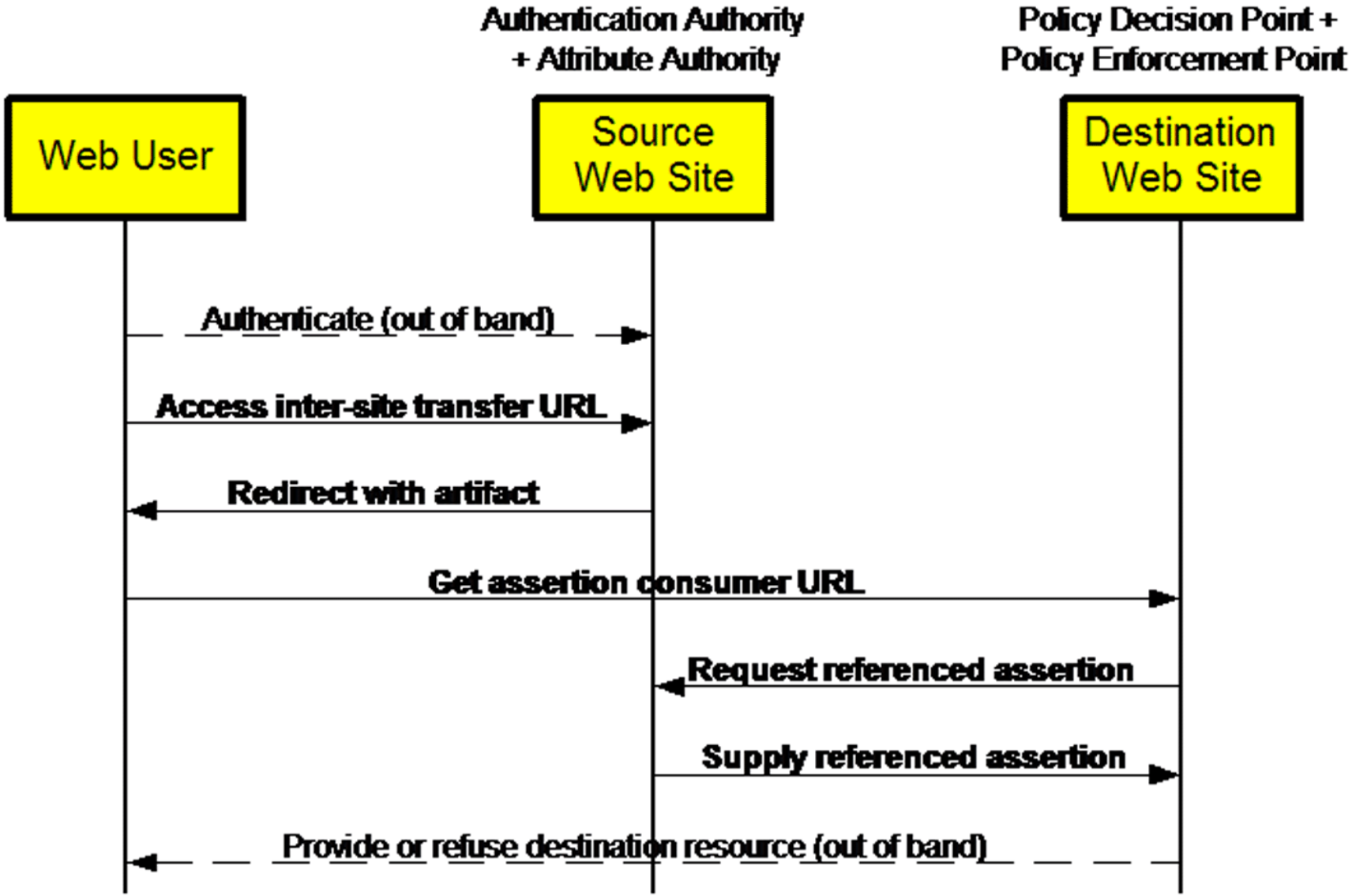
Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Arquitectura: Mapeo del Modelo SAML

- Funcionamiento para el caso SSO:
  1. El cliente pasa, p.e. a través del navegador, sus credenciales para autorizarse al **Source Site**. Se conecta a http://pepitoco.com
  2. Una vez autorizado clickea http://juanitoco.com que es donde desea realmente ir (**Destination Site**).
  3. Ese click le llevará realmente a una URL de transferencia entre sitios web: https://source.com/intersite?dest=juanitoco.com.
  4. La redirección se realiza a través de un **artefacto SAML** que no es más que un string de 8 bytes codificado en base 64.
  5. El usuario es redireccionado a la URL https://juanitoco.com?SAMLart=artefacto (incluyendo el artefacto), la URL del **consumidor de asertos** o **Destination Site**.
  6. Después el sitio de destino pide un aserto al sitio fuente y éste le responde con el aserto correspondiente.
  7. A partir de este punto el cliente es aceptado o revocado por el

Arquitectura: Mapeo del Modelo SAML



Arquitectura: Mapeo del Modelo SAML

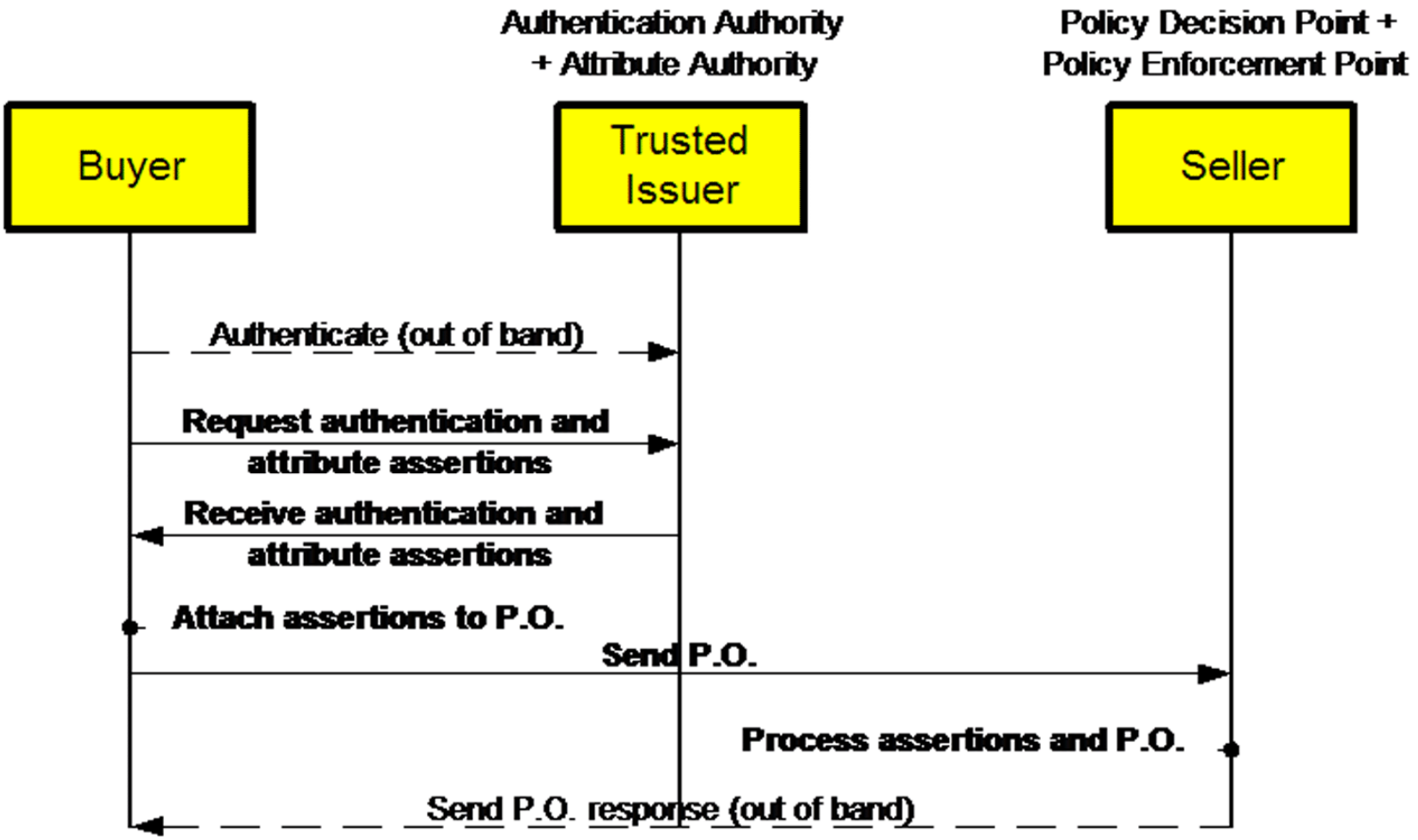
- Funcionamiento para transacción distribuída:
  1. El cliente (comprador) se autentifica ante un sitio web:

  Trusted Issuer

  2. Después le pide asertos de autentificación y de atributo.
  3. Recibidos dichos asertos los incorpora a un P.0. y los envía directamente al sitio vendedor **Seller** que usualmente es conocido por el **Buyer.** Sería deseable que el comprador se autentificase mediante certificados.
  4. Es en el **Seller** donde se procesan los asertos y el P.O.
  5. Finalmente el comprador recibe la respuesta en un P.O. con el resultado de la compra.

Como puede verse en ambos ejemplos la decisión final corresponde a un PDP/PEP y el intercambio de asertos depende del escenario considerado.

Arquitectura: Mapeo del Modelo SAML



Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Asertos SAML:

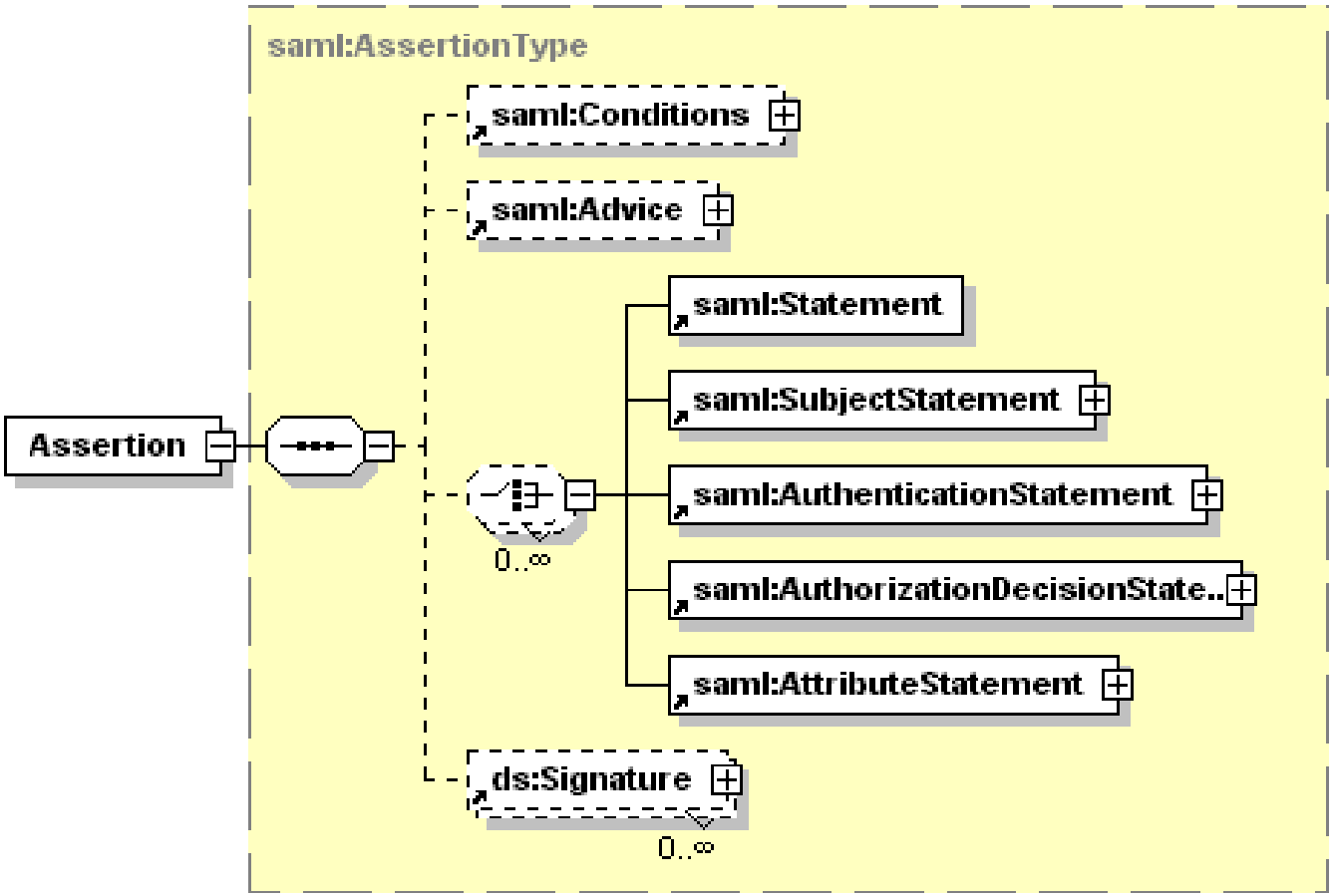
- Definición:
  - Declaraciones de hecho acerca de alguien
  - Compuestos de uno o de diversos **statements** acerca de un **Subject:**
    - Autentificación (**Authentication Assertion**)
    - Atributo (**Attribute Assertion**)
    - Decisión de autorización (**Authorization Decision Assertion**)
  - Pueden firmarse digitalmente.

Los asertos son el elemento central producidos por una autoridad SAML. Hay que recordar que SAML es “un modelo de producción-consumo de asertos”

Asertos SAML:

- Elementos comunes:
  - **AssertionID:** Identificación unívoca del aserto
  - **Issuer:** Identificador del emisor del aserto (String)
  - **IssueInstant:** Timestamp de emisión (¡importante!)
  - **Subject** (incluído en los statements).
  - **Conditions:** Condiciones bajo las cuales el aserto es válido.
    - Los clientes SAML deben rechazar asertos conteniendo condiciones que no se puedan cumplir.
    - Un tipo especial de condición es el assert validity period.
  - **Advices:** (Consejos) p.e. explican como se hizo el aserto.
  - **Signature:** Firma digital
  - **Statements:** acerca del Subject, Authentication, Authorization Decision y Attribute

Asertos SAML:



Asertos SAML:

```
<saml:Assertion
  MajorVersion="1" MinorVersion="0"
  AssertionID="128.9.167.32.12345678"
  Issuer="Pepito Corporation"
  IssueInstant="2001-12-03T10:02:00Z">
  <saml:Conditions
    NotBefore="2001-12-03T10:00:00Z"
    NotOnOrAfter="2001-12-03T10:05:00Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>...URI...</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:Advice>
    ...a variety of elements can go here...
  </saml:Advice>
  ...statements go here...
</saml:Assertion>
```

Indice

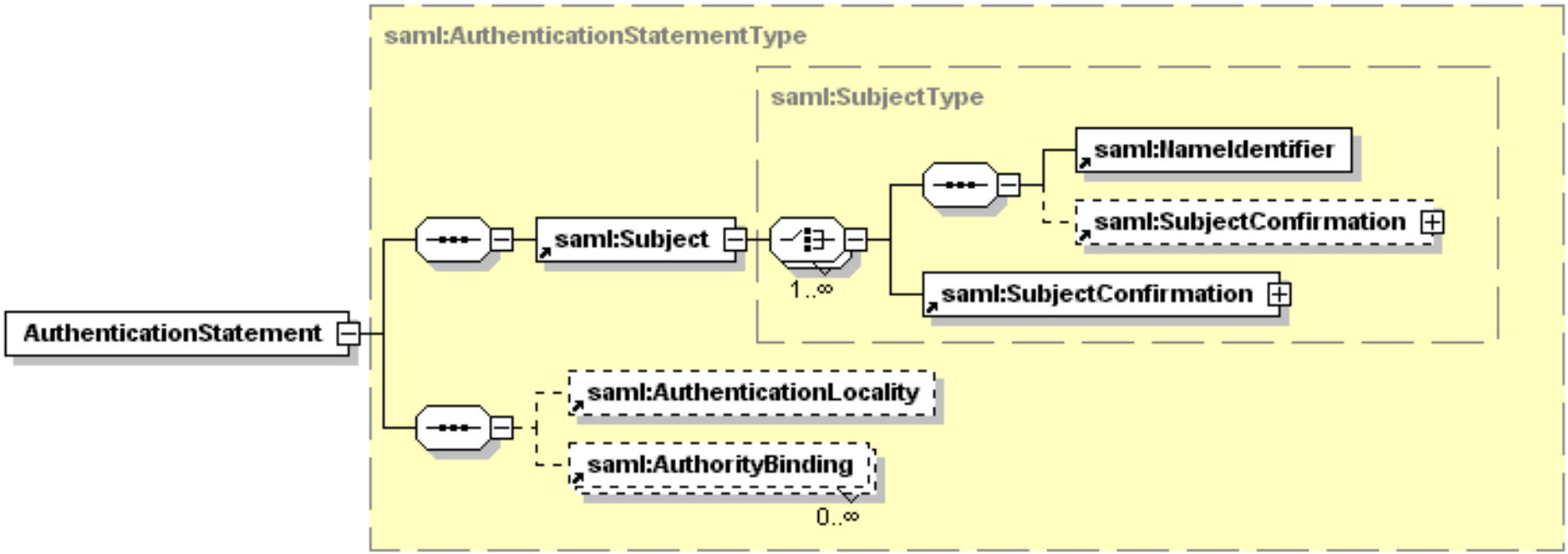
- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Statements SAML: Authentication

- Definición:
  - Una autoridad emisora aserta que el sujeto S se autentificó por medio de M en el instante T.
  - Está específicamente dedicada a implementar SSO.
  - **Importante:** la autoridad solo emite el aserto pero SAML no se ocupa de verificar si el cliente se autentificó o no con éxito (el chequeo de las credenciales).
  - SAML proporciona un link.

Los asertos de autentificación se emiten p.e. desde el sitio de destino a la autoridad autentificadora para que quede claro que la atuentificación se realizó.

AuthenticationStatement:



AuthenticationStatement:

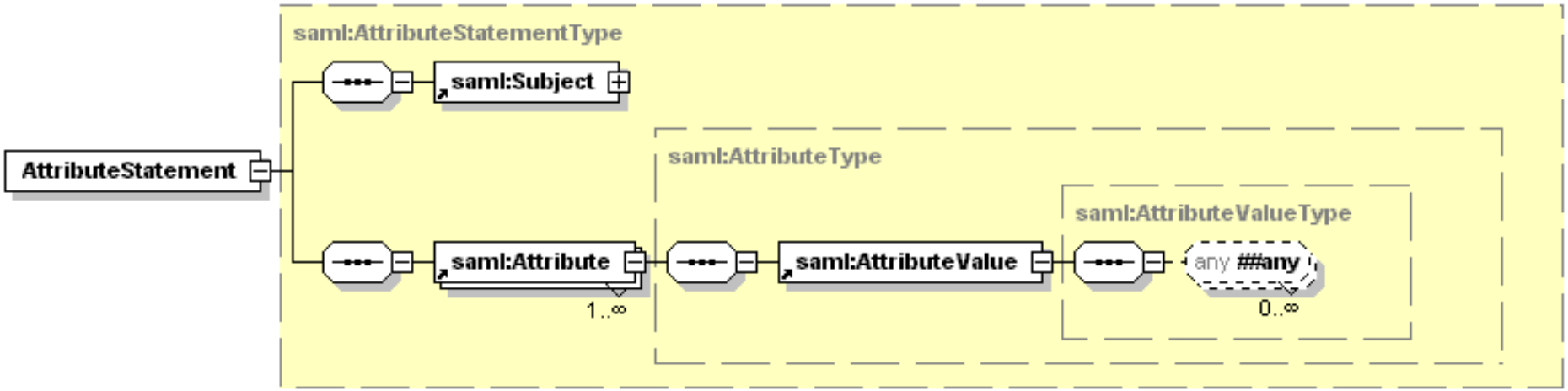
```
<saml:Assertion …>
  <saml:AuthenticationStatement
    AuthenticationMethod="password"
    AuthenticationInstant="2001-1203T10:02:00Z">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="pepitoco.com"
        Name="juanuser" />
      <saml:ConfirmationMethod>
        http://…core-25/sender-vouches
      </saml:ConfirmationMethod>
    </saml:Subject>
  </saml:AuthenticationStatement>
 </saml:Assertion>
```

Statements SAML: Attribute

- Definición:
  - Una autoridad emisora aserta que el sujeto S está asociado con los atributos A, B y C con valores “a”, “b”, “c”.
  - Esta indicada para transacciones distribuida (pares atributo valor) y servicios de autorización.
  - Típicamente esta información se obtiene de un LDAP:
  - Ejemplo: “juanuser en “pepitoco.com” está asociado con el attributo “Departamento” cuyo valor es “Recursos Humanos”

En una transacción distribuida los statements de atributo se piden desde el comprador a la autoridad emisora y esta los envía con lo cual quedan claro aspectos que relacionan al sujeto con el estado de la transacción.

AttributeStatement:



AttributeStatement:

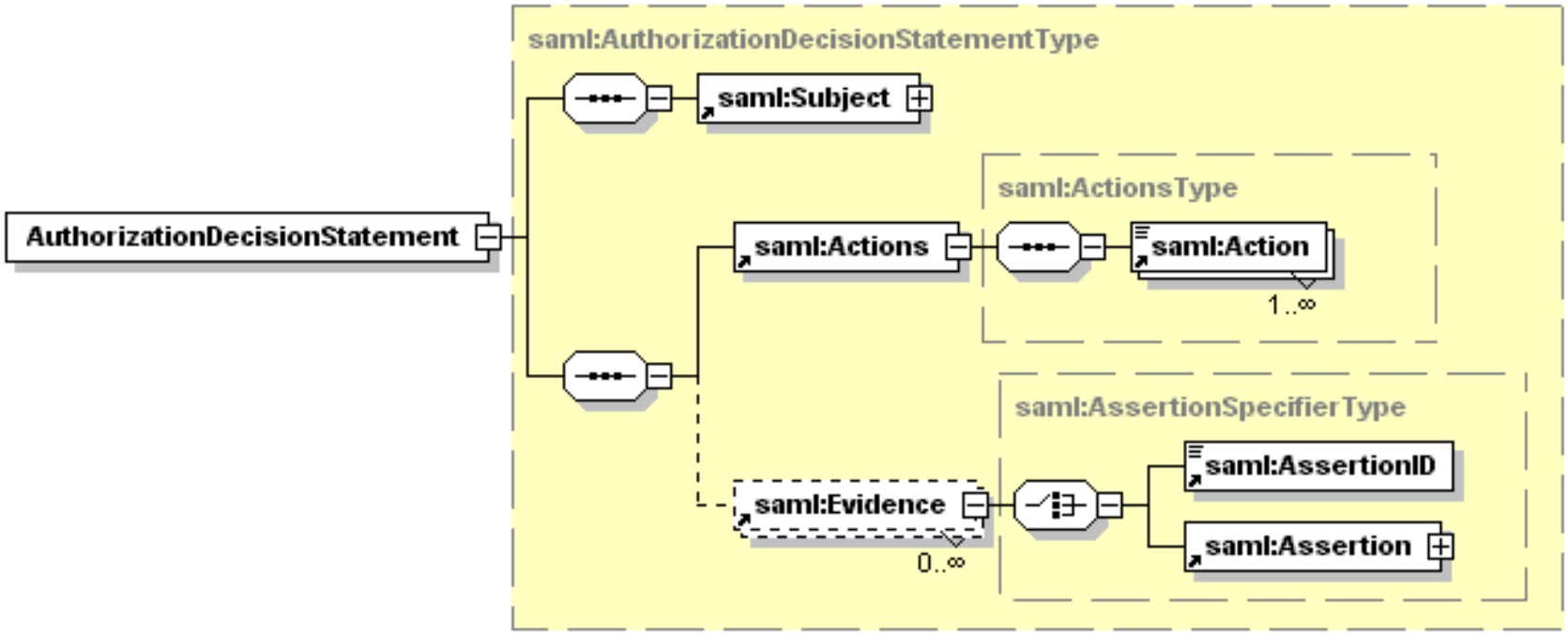
```
<saml:Assertion …>
  <saml:AttributeStatement>
    <saml:Subject>…</saml:Subject>
    <saml:Attribute
      AttributeName="EstadoPago"
      AttributeNamespace="http://pepitoco.com">
      <saml:AttributeValue>
        Pagado
      </saml:AttributeValue>
    </saml:Attribute>
 <saml:Attribute
      AttributeName="LimiteCredito"
      AttributeNamespace="http://pepitoco.com">
      <saml:AttributeValue>
        <my:amount currency="USD">500.00
        </my:amount>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Statements SAML: AutorizationDecision

- Definición:
  - Una autoridad emisora decide si garantizar o denegar al sujeto S un acceso de tipo A a un recurso R dada la evidencia E.
  - Esta indicada para transacciones distribuida y servicios de autorización.
  - El sujeto puede ser un humano o un programa.
  - El recurso puede ser p.e. una página web, o un servicio web.

En una transacción distribuida se puede permitir a un determinado sujeto acceder a una determinada página web pero especificando solo permisos de lectura, p.e.

AutorizationDecision:



AutorizationDecision:

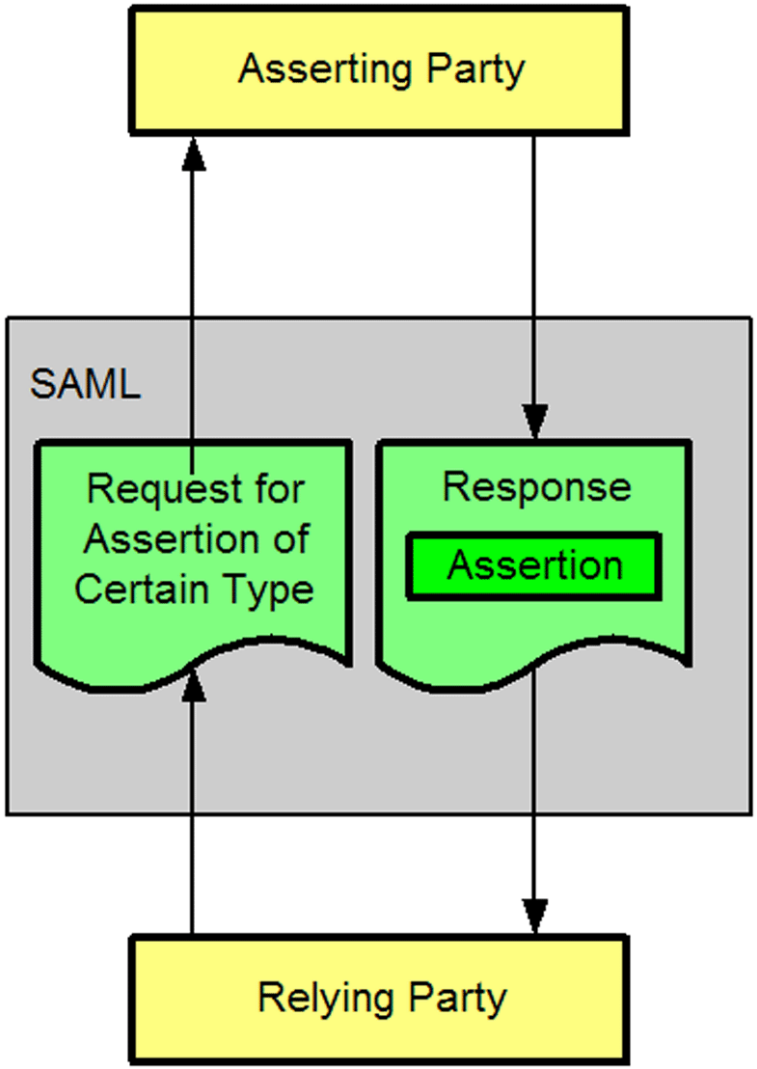
```
<saml:Assertion …>
  <saml:AuthorizationStatement
    Decision="Permit"
    Resource="http://juanitoco.com/rpt_12345.htm">
    <saml:Subject>…</saml:Subject>
    <saml:Actions
      ActionNamespace="http://…core-25/rwedc">
      <saml:Action>Read</saml:Action>
    </saml:Actions>
  </saml:AuthorizationStatement>
</saml:Assertion>
```

Indice

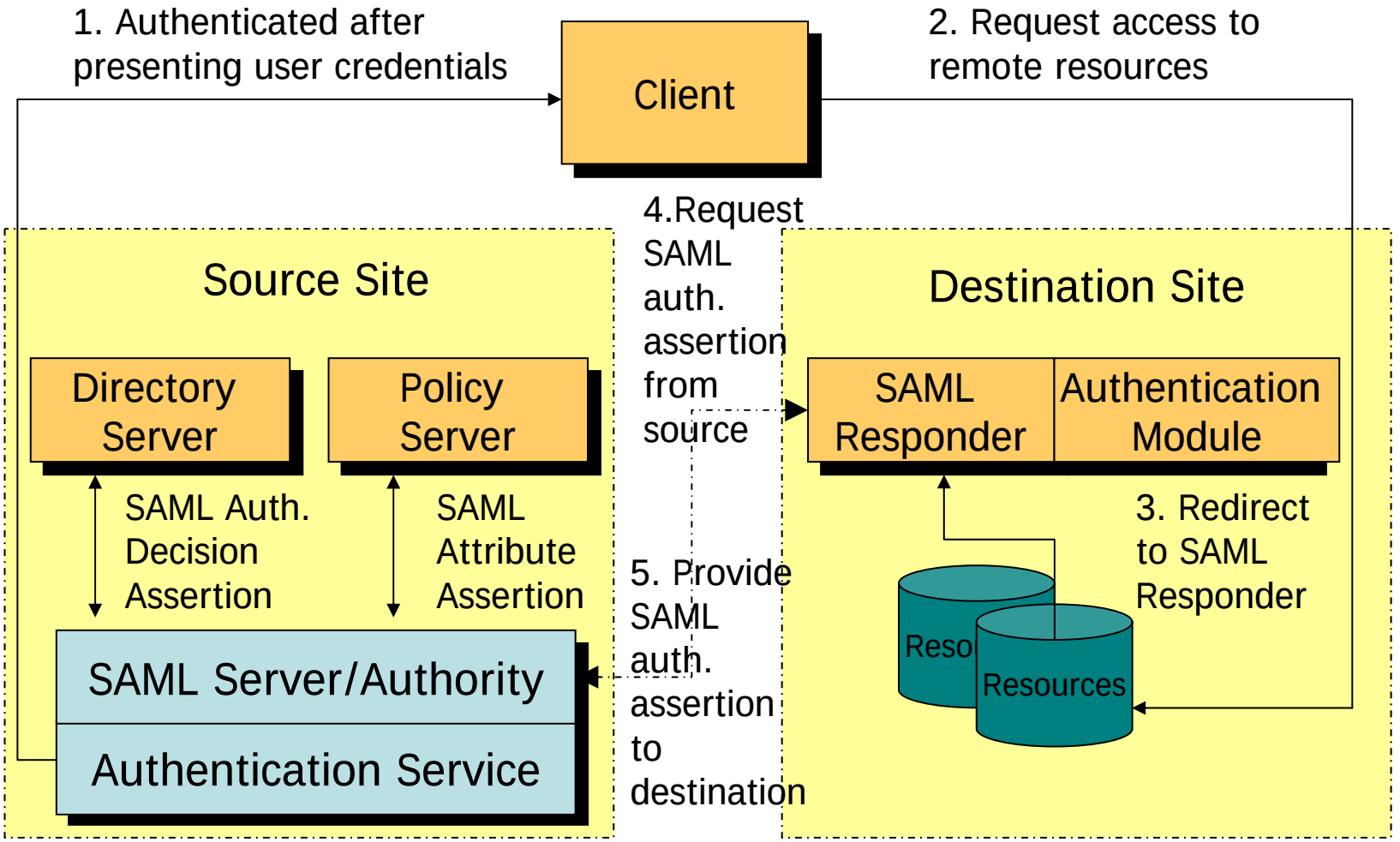
- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Protocolo SAML:

- Definición:
  - SAML usa un modelo *request-reply*.
  - Implementa la relación entre una **Relying Party** y una **Asserting Party**
  - Se ajusta por tanto al consumidor/productor de asertos.
  - En SSO, p.e., la AP suele ser el sitio contra el que se autentifica el cliente y la RP suele ser el sitio al que desea acceder.



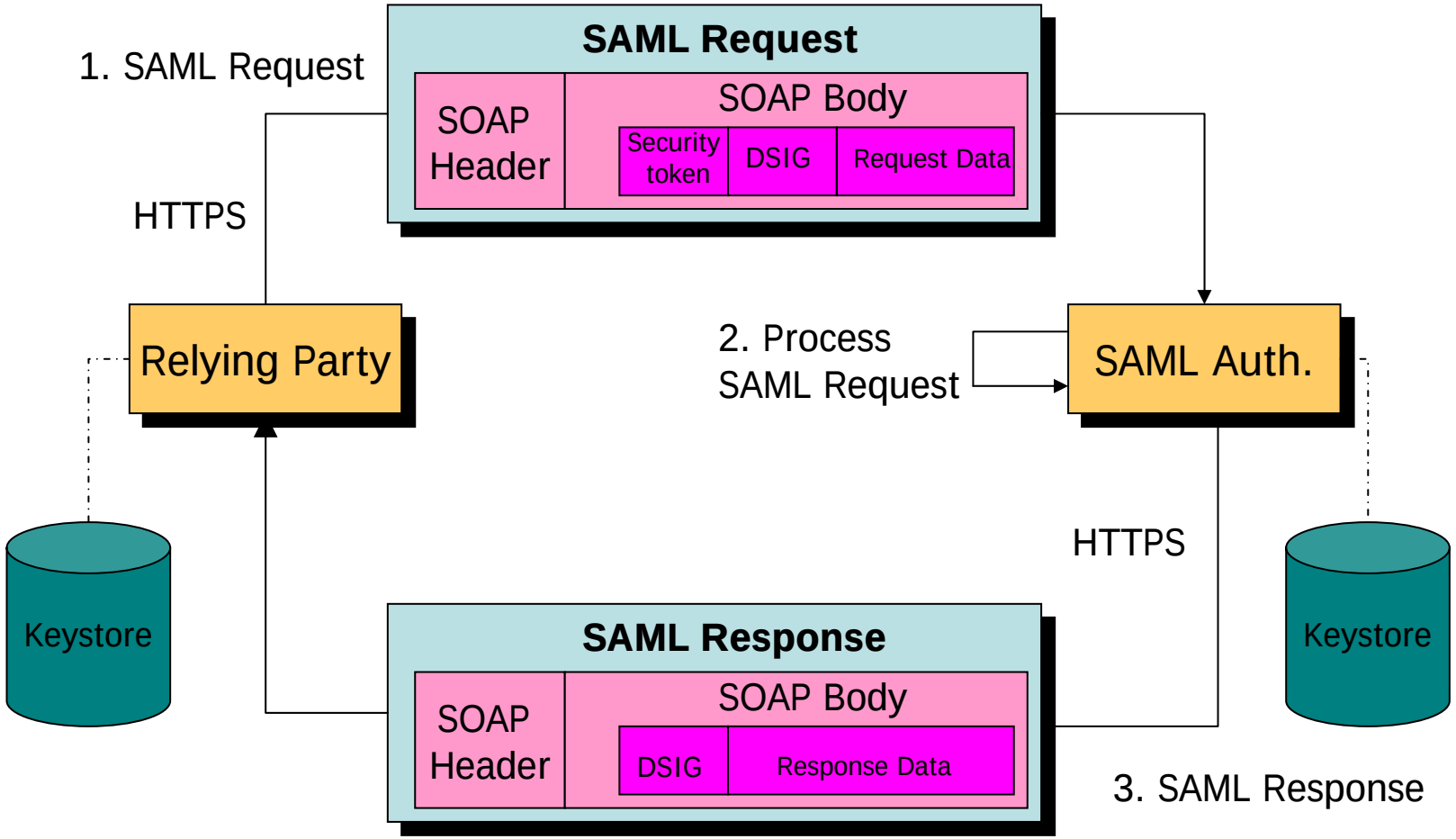
Protocolo SAML:



Protocolo SAML:

- Protocolo SOAP (envuelve peticiones-respuestas)
  - En el cuerpo de un mensaje de petición (p.e. autentificación por password):
    - Se encapsulan las credenciales del usuario (p.e. el ID y el password si ya se conoce a través de JAAS, certificados...para un futuro contraste) en un **Security Token** junto con una firma digital (usando firma XML) y el **Requested Data** (p.e. autentificación por password).
    - Todo ello se encapsula en un envelope SOAP y se envía via HTTPS.
    - A nivel XML en el cuerpo del mensaje suele ir la propia petición.
    - También suele generarse una firma digital y añadirse al mensaje.
  - En el cuerpo del mensaje de respuesta vienen los asertos.

Protocolo SAML:



Indice

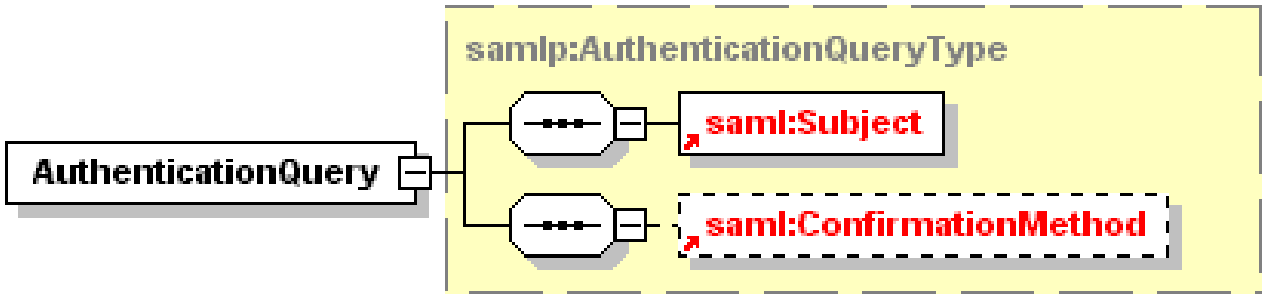
- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

Queries:

- Request:
  - La petición en sí es la **Request** y suele incluir distintos tipos del **queries**:
    - **Authentication Query**
    - **Attribute Query**
    - **Autorization Decision Query**
  - Se puede preguntar por un aserto con un ID particular:
    - Proporcionando la referencia del ID
    - Proporcionando un **artefacto SAML**
  - El recurso puede ser p.e. una página web, o un servicio web.

Authentication Query:

- Definición:
  - “Por favor, proporcione información de autentificación para este sujeto, si tiene alguna”.
  - Se asume que el **requester** y el **responder** tienen una relación de confianza
    - Están hablando acerca del mismo sujeto.
    - La respuesta con un aserto es una “carta de presentación” para el sujeto.

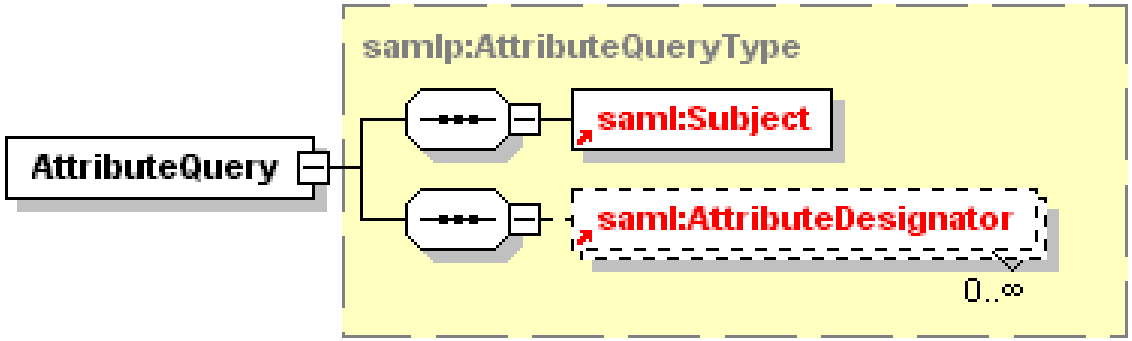


Authentication Query:

```
<samlp:Request
 MajorVersion="1" MinorVersion="0"
  RequestID="128.14.234.20.12345678" >
  <samlp:AuthenticationQuery>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="pepitoco.com"
        Name="juanuser" />
    </saml:Subject>
  </samlp:AuthenticationQuery>
</samlp:Request>
```

Attribute Query:

- Definición:
  - “Por favor, proporcione información de los atributos listados para este sujeto”.
  - Si no se lista ningún atributo, se está preguntando por los disponibles.
  - Si al requester se le deniega el acceso a alguno de los atributos solo los atributos permitidos deberían ser devueltos.
  - Esta situación viene indicada en el codigo de estado de la respuesta.

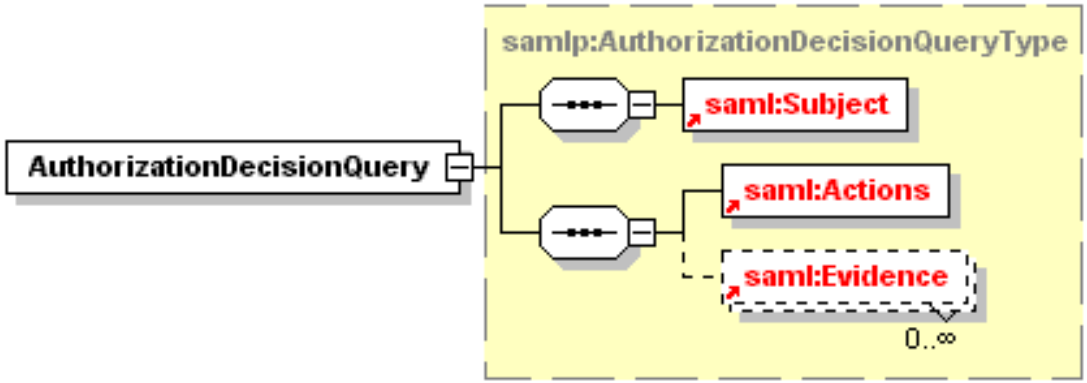


Attribute Query:

```
<samlp:Request … >
  <samlp:AttributeQuery>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="pepitoco.com"
        Name="juanuser" />
    </saml:Subject>
    <saml:AttributeDesignator
      AttributeName="EstadoPago"
      AttributeNamespace="pepitoco.com">
    </saml:AttributeDesignator>
  </samlp:AttributeQuery>
</samlp:Request>
```

Autorization Decision Query:

- Definición:
  - ¿Se permite a este sujeto acceder al recurso especificado en la forma especificada dada esta evidencia?
  - La respuesta es SI o NO.
  - No se puede responder, “NO, pero no puede acceder a otros recursos?” o “SI” pero solo se le permite realizar estas otras acciones?”.



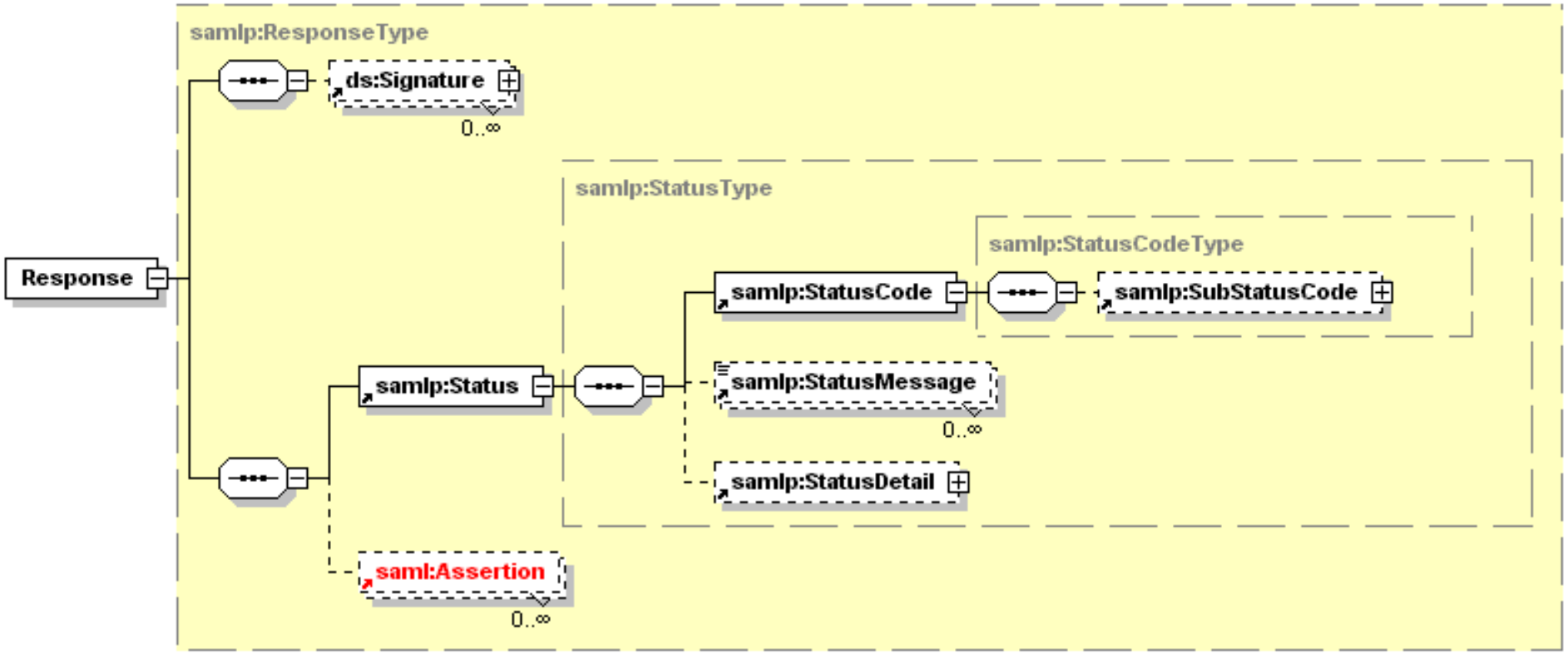
Autorization Decision Query:

```
<samlp:Request …>
  <samlp:AuthorizationQuery
    Resource="http://juanitoco.com/rpt_12345.htm">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="pepitoco.com"
        Name="joeuser" />
    </saml:Subject>
    <saml:Actions
      ActionNamespace="http://…core-25/rwedc">
      <saml:Action>Read</saml:Action>
    </saml:Actions>
    <saml:Evidence>
      <saml:Assertion>…</saml:Assertion>
    </saml:Evidence>
  </samlp:AuthorizationQuery>
</samlp:Request>
```

Responses:

- Definición:
  - Las respuestas deben contener una o más assertions.
  - Si algo fue mal, no se devuelven assertions, solo status.
  - La información de estado puede tener una estructura compleja.
  - Los status codes más usuales son:
    - Success
    - VersionMismatch
    - Receiver
    - Sender
  - Se espera que las respuestas estén firmadas.

Responses:


samlp:ResponseType
ds:Signature
0..∞
samlp:StatusType
samlp:StatusCodeType
Response
samlp:StatusCode
samlp:SubStatusCode
samlp:Status
samlp:StatusMessage
0..∞
samlp:StatusDetail
saml:Assertion
0..∞

Responses:

```
<samlp:Response
 MajorVersion="1" MinorVersion="0"
  RequestID="128.14.234.20.90123456"
  InResponseTo="128.14.234.20.12345678"
  StatusCode="Success">
  <saml:Assertion
    MajorVersion="1" MinorVersion="0"
    AssertionID="128.9.167.32.12345678"
    Issuer="Pepito Corporation">
    <saml:Conditions
      NotBefore="2001-12-03T10:00:00Z"
      NotAfter="2001-12-03T10:05:00Z" />
    <saml:AuthenticationStatement ...>...
    </saml:AuthenticationStatement>
  </saml:Assertion>
</samlp:Request>
```

Indice

- Identity Management (SSO)
- Motivación de SAML: Escenarios
- Arquitectura: Modelo Conceptual SAML
- Arquitectura: Mapeo del Modelo SAML
- Assertions SAML
- Statements SAML
- Protocolo de comunicación SAML
- Queries y Responses
- Firmas XML

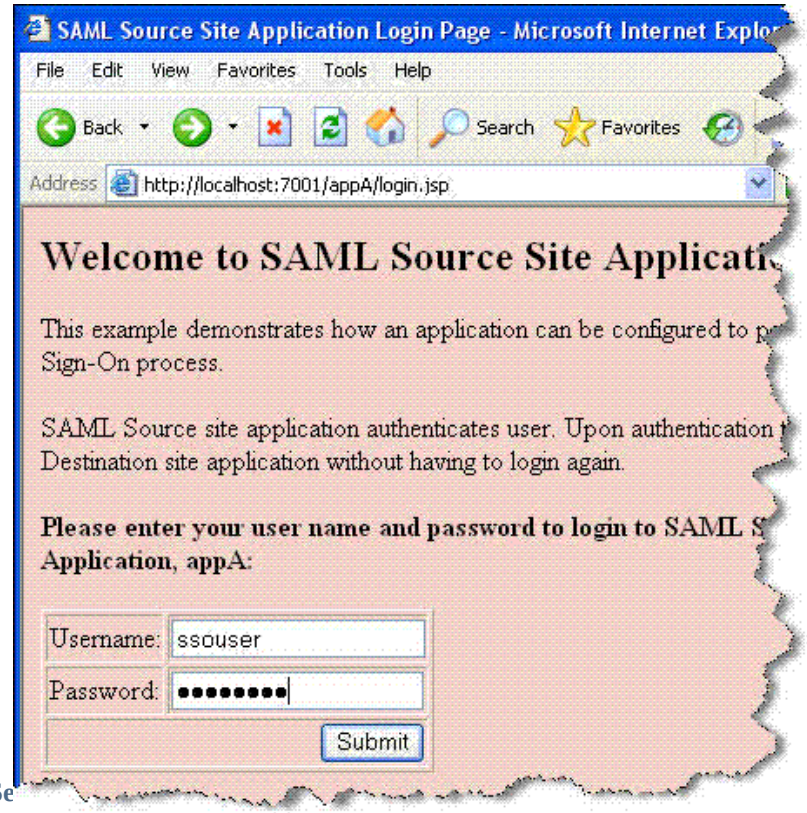
Firmas XML:

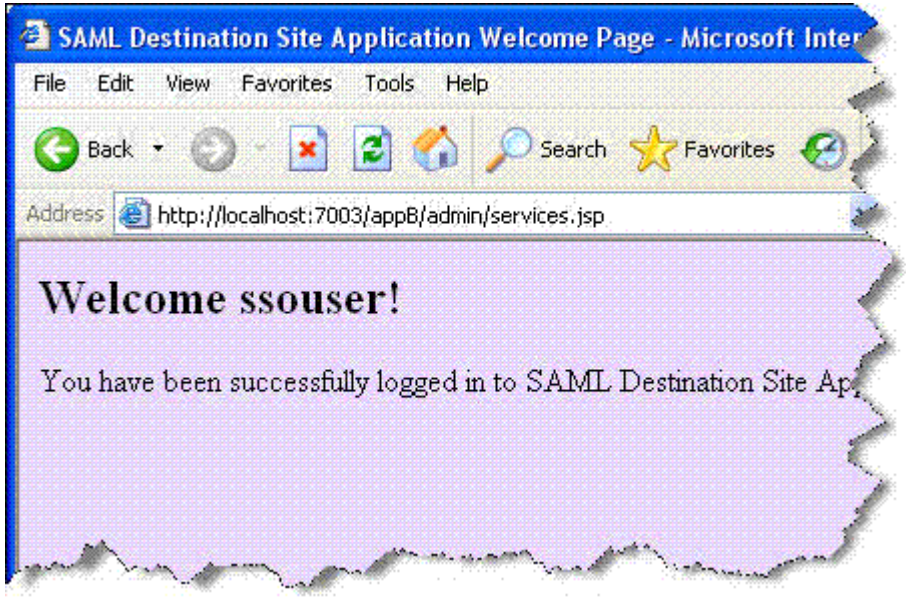
- Definición:
  - La firma digital en XML (**XML Signature**) proporciona un mecanismo de integridad y no-repudio en transacciones SAML.
  - Esta firma se usa para representar la autoridad que firma el mensaje y puede colocarse en el aserto, la petición o la respuesta.
  - Una de estas firmas contiene un certificado X.509 con una clave pública y también la firma generada. Cuando el mensaje firmado es recibido por la relying party, ésta la verifica con la clave pública de la autoridad.
  - Esta verificación asegura:
    - que el mensaje no ha sido modificado durante la transmisión
    - la autenticidad del firmante e identifica el contenido
    - las porciones del mensaje firmado (p.e. la parte que sensible cómo como el número de la tarjeta de crédito)

Ejercicios…

- SSO en Weblogic

  Configurar Weblogic para un SSO entre dos aplicaciones JSP situadas en dominos distintos.





Ejercicios…

- Pasos

1.Browser accede a appA

2. Se recogen sus credenciales y se pasan al ASP

3. Si la autentificación tiene éxito se muestra página bienvenida.

4. Desde ahí, clickear para acceder a appB. Lanza el ITS

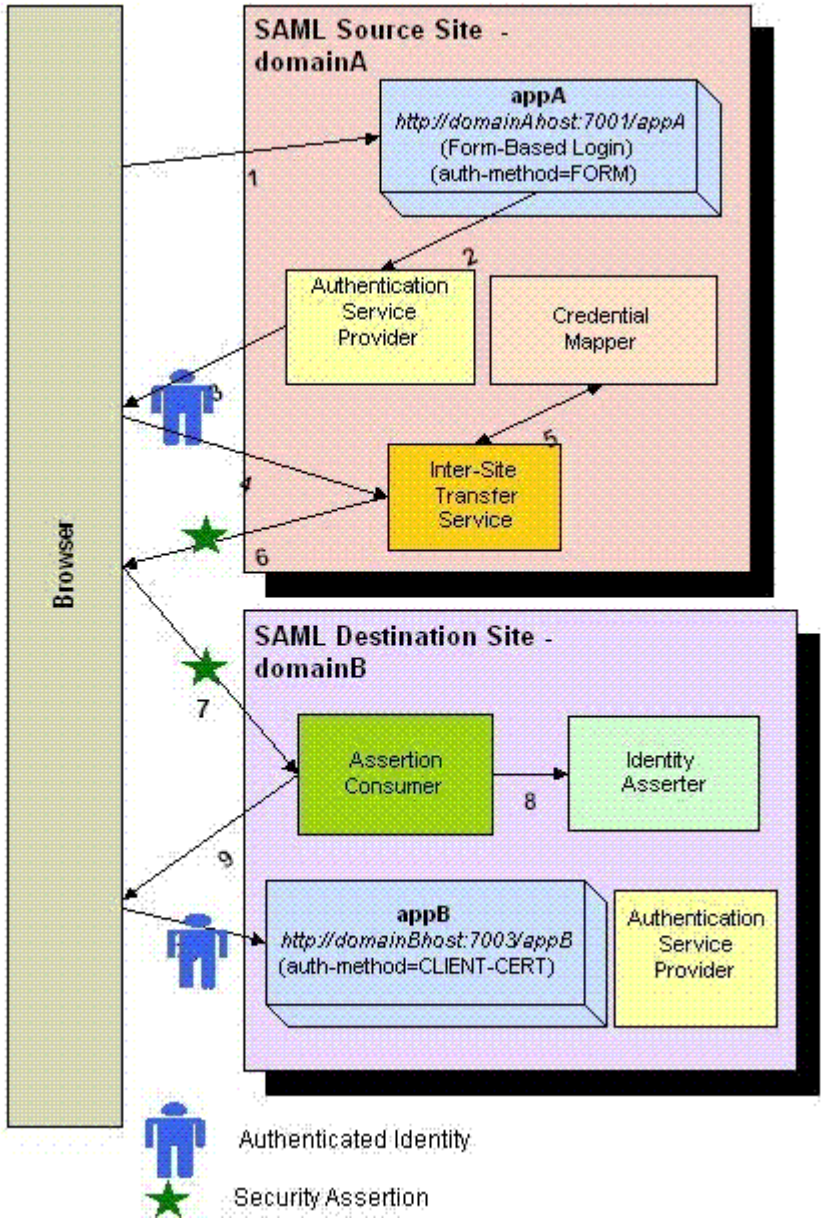
5. ITS llama al SAML Credential Mapper para pedir una caller assertion.

6. El SAML ITS genera respuesta SAML con el aserto.

7. Browser POST el aserto en ACS

8. Se valida el aserto .

9. Si éxito -> entrar en appB.



Ejercicios…

- Pasos de configuración:

1. Crear dominios
2. Crear usuarios
3. Desplegar aplicaciones appA y appB
4. Generar los certificados SSL
5. Configurar domainA como SAML source site
6. Configurar propiedades de la relying party
7. Configurar SAML en el source site
8. Configurar domainB como SAML destination site
9. Configurar las propiedades de la asserting party
10. Configurar el SAML 1.1. destination site

Testar SSO