Capítulo 4

El estándar SAML

Contenido

- 4.1 Introducción
- 4.2 La arquitectura SAML
- 4.3 Los perfiles SAML

4.1 Introducción

SAML (*Security Assertion Markup Language*) define una infraestructura para el intercambio de credenciales entre distintos dominios de seguridad. Consiste en una serie de especificaciones para construir, intercambiar e interpretar información de autenticación y autorización cuya validez sobrepasa las fronteras entre redes autónomas. Es un estándar basado en XML desarrollado por el *Security Services Technical Committee* (SSTC) de la *Organization for the Advancement of Structured Information Standards* (OASIS).

Dedicaremos este capítulo completo al estudio del estándar. Debido a lo extenso de las especificaciones, no haremos una descripción exhaustiva del mismo, sino que pretendemos proporcionar una visión “operativa” general.

El problema principal al que SAML trata de encontrar solución es el de la firma simple o firma única, conocido en inglés como **single sign-on** (SSO). Al existir ya numerosos intentos de abordar esta cuestión, cabe preguntarse el porqué de la aparición de una nueva iniciativa en esta misma dirección. Cuatro son las razones principales que lo motivan:

- **Limitación de las cookies del navegador:** el protocolo HTTP, ampliamente usado en Internet como soporte para las interacciones servidor-cliente, carece, por su propia definición, de un medio para mantener el estado durante el intervalo que separa una de dichas interacciones de la siguiente. La mayoría de los productos single sign-on existentes utilizan **cookies** para superar esta limitación. Sin embargo, no es posible transferir cookies de un dominio DNS a otro. Si el cliente obtiene una cookie de, digamos, www.dominio-A.com, dicha cookie no será enviada en ningún mensaje HTTP a, por ejemplo, www.dominio-B.com. Esto podría ocurrir también dentro de una misma organización que disponga de varios dominios de nombre diferentes. Esta limitación es superada por los productos SSO actuales mediante el uso de diferentes técnicas.

- **Interoperabilidad de las soluciones SSO:** numerosos productos han aparecido en el mercado, tratando de solucionar el problema de la firma simple. Esto ha llevado a la proliferación de tecnologías propietarias sin que exista, en la mayoría de los casos, la posibilidad de interacción entre ellas. Si deseamos una implementación de firma simple que vaya más allá de los límites de nuestra organización, nos veremos obligados a utilizar el mismo producto en todos los dominios de seguridad afectados. SAML aspira a convertirse en el estándar definitivo que sirva como base para soluciones compatibles en este ámbito.

- **Servicios Web (Web Services):** no existe aún un estándar de seguridad en el ámbito de los Servicios Web. La mayoría de los esfuerzos van encaminados a garantizar la confidencialidad, autentificación e integridad de los datos de extremo a extremo de la comunicación. El estándar SAML proporciona los medios necesarios para el intercambio de información de autenticación y autorización entre las partes implicadas en dicha comunicación.

- **Simplificar la gestión de identidades:** resulta frecuente que un usuario disponga de múltiples identidades, una en cada dominio de seguridad al que tiene acceso. En muchos casos sería conveniente simplificar dicho conjunto, reduciéndolo a una única identidad global, la **identidad federada**.

En esta memoria nos referiremos, en general, a la versión 2.0 de SAML, que vio la luz oficialmente como estándar el 15 de Marzo de 2005.

Entidades fundamentales

Antes de describir los casos generales para la aplicación de SAML, es preciso definir dos conceptos fundamentales que se usan en dicho estándar:

- **Identity Provider o Proveedor de Identidad (IdP)**

  Sistema o dominio administrativo que expide información sobre un sujeto determinado (generalmente un usuario). Un Proveedor de Identidad puede asegurar, entre otras cosas, que un usuario ha sido autentificado y que posee determinados atributos. Por ejemplo, un IdP podría afirmar que el usuario se llama Paco Teleco, tiene como dirección de email paco.teleco@telecosunidos.com y que se autentificó mediante la introducción de una contraseña.

  Las funciones que realiza el Proveedor de Identidad se corresponden con las que nosotros asignamos al agente de autenticación y al agente de credenciales. En capítulos posteriores veremos con detenimiento cómo se establece esta correspondencia.

La especificación SAML usa también la denominación *SAML authority* y *Asserting Party* para dichos sistemas. A lo largo de esta memoria se usarán indistintamente los nombres Identity Provider, Proveedor de Identidad e IdP para referirnos a ellos.

- **Service Provider o Proveedor de Servicios (SP)**

  Sistema o dominio administrativo donde residen los recursos a los que el usuario desea acceder y que depende de la información que le proporciona el Proveedor de Identidad. Confiar o no en las afirmaciones que el IdP realiza sobre un usuario es una decisión propia del Proveedor de Servicios, si bien SAML define mecanismos que permiten otorgar dicha confianza. Hay que resaltar que, el hecho de que un SP confíe en las afirmaciones de un Proveedor de Identidad sobre la identidad o los atributos de un determinado sujeto, no significa necesariamente que dicho sujeto pueda acceder a los recursos de dicho Proveedor de Servicios, siendo las políticas locales de acceso sobre las que recae, en último término, la responsabilidad de esta decisión.

  SAML denomina también estos sistemas como *Relying Parties*. En este texto aparecerán los nombraremos indistintamente con los términos Service Provider, Proveedor de Servicios y SP.

Escenarios de aplicación de SAML

La especificación SAML distingue dos casos básicos para la aplicación de dicha tecnología:

- **Federación**

  Este escenario, ilustrado en la figura 3, recibe también la denominación de *Account Linking* (“Enlace de Cuentas”) en la especificación SAML. La misma persona se ha registrado con nombres de usuario diferentes en dos Proveedores de Servicio distintos. En concreto ha usado “jdoes” para el registro en un sitio de

alquiler de coches, “CarRentalInc.com” y “johnd” para una página de reservas hoteleras, “HotelBooking.com”. El Proveedor de Identidad (en este caso, el sitio web de una línea aérea) permitiría el establecimiento de un pseudónimo para enlazar ambas cuentas. Dicho pseudónimo es lo que nosotros llamamos identidad federada.

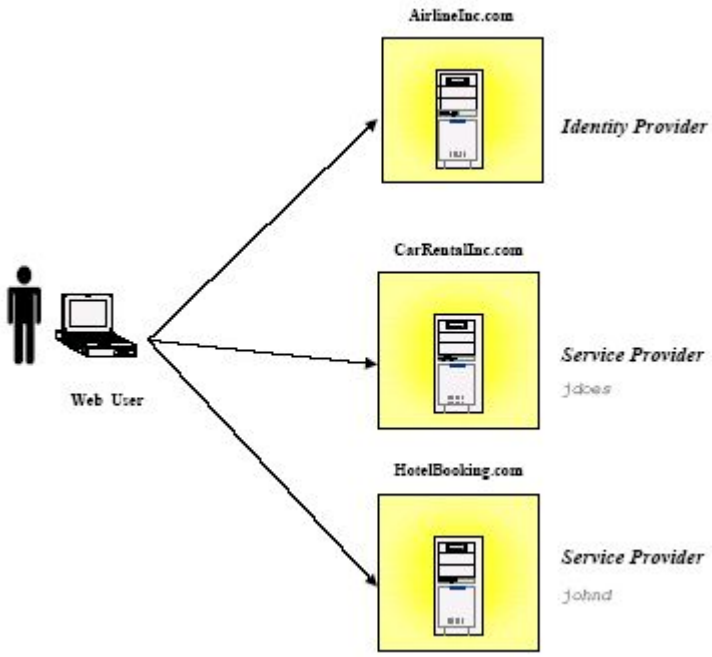

Figura 3: La federación según SAML

La norma SAML en su versión 2.0 no da más información sobre este escenario que la que se ha presentado más arriba. Para construir el sistema que queremos implementar nos basaremos en la idea general de la figura 3, pero usando las técnicas del escenario que abordamos en el siguiente apartado, y que sí se describe en profundidad en la especificación SAML.

- **Firma Simple**

Este escenario de la especificación SAML se ilustra en la Figura 4:

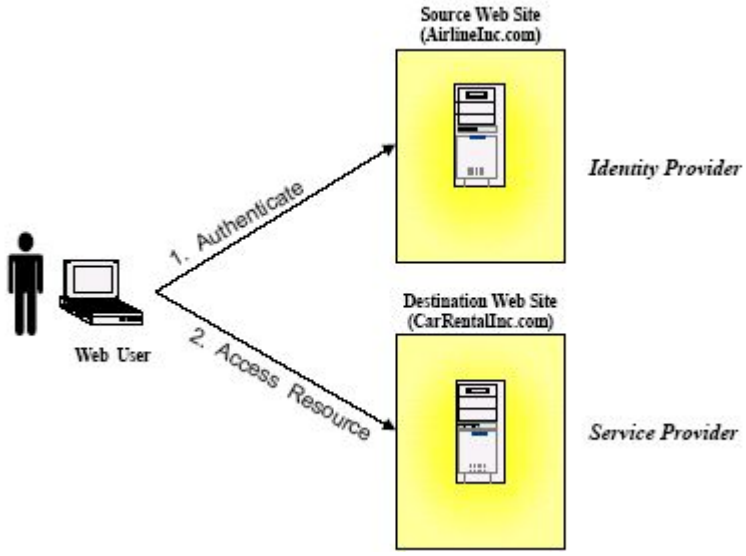

Figura 4: El caso de uso Single Sign-On en SAML

1. Un usuario se ha identificado en un Proveedor de Identidad, "AirlineInc.com", tiene establecida una sesión y está accediendo a recursos en dicho servidor.

2. En un momento determinado, ya sea explícitamente o de forma transparente, el usuario es dirigido a un recurso situado en el Proveedor de Servicios situado en "CarRentalInc.com", en un dominio de seguridad diferente. Al mismo tiempo, el Identity Provider envía al Service Provider información de credenciales en formato SAML, conteniendo ciertos atributos correspondientes a la sesión que el usuario posee en el servidor de la línea aérea. El Proveedor de Servicios confía (mediante el uso, por ejemplo, de un certificado SSL) en el Proveedor de Identidad, de manera que confirma la validez del usuario y crea una sesión para el mismo, basándose en los atributos SAML que acaba de recibir.

El usuario lleva a cabo, por tanto, sólo un proceso de autenticación para el acceso a dos servidores autónomos. En este caso, hemos supuesto que en el Proveedor de Identidad residen recursos accesibles para los usuarios, con lo cual estamos afirmando implícitamente que dicho sistema funciona al mismo tiempo como Proveedor de Servicios. Se deja a elección de los administradores del

sistema unir las funciones de ambos proveedores en un mismo sistema, como ocurre en este caso, o bien utilizar servidores dedicados para cada tarea.

Este caso de uso sí está desarrollado en la especificación SAML. De hecho, en el texto del estándar se plantean situaciones relacionadas con este escenario, donde aparecen interacciones más complejas. Por ejemplo, es posible que el usuario trate, en primer lugar, de acceder a un recurso en el Service Provider, éste le reenvíe al Identity Provider para llevar a cabo un proceso de autentificación, del cual regresará con un conjunto de credenciales confiables que el Proveedor de Servicios utilizará como base para decidir sobre el acceso al recurso deseado. El envío de credenciales sería **requerido**, mientras que en el caso de la figura 4 dicho envío era directo, sin solicitud previa.

Basaremos el sistema Java implementado en este Proyecto en las técnicas perfiladas en este apartado.

La seguridad en SAML

El envío, por parte de una autoridad SAML, de información de credenciales a otra entidad, la cual confía en dicha información y toma decisiones relativas al acceso a recursos protegidos basándose en los datos que recibe, plantea problemas de seguridad. Dentro de las interrogantes que se plantean podemos citar, por ejemplo, cómo puede la entidad que recibe la información dar crédito a lo recibido, cómo se pueden prevenir ataques del tipo *man-in-the-middle* que capturen aserciones para ser retransmitidas posteriormente de forma maliciosa, etc. La especificación SAML trata de dar respuesta a estas cuestiones.

SAML está diseñado para integrarse con **XML Encryption** y **XML Signature**, estándares relativamente recientes del Consorcio World Wide Web (W3C), cuya finalidad es, respectivamente, incrustar información cifrada y firmas digitales en un documento XML. La mayoría de los estándares de cifrado que se utilizan hoy en día usan técnicas de nivel de transporte, tratando la comunicación completa entre emisor y

receptor como un todo. Cualquier intermediario en dicha comunicación tendrá "visibilidad cero" con respecto a los contenidos transmitidos.

A diferencia de esto, XML Encryption puede convertir fragmentos de documentos XML en texto cifrado, manteniendo el resto de elementos de dicho documento como texto ordinario. Esto permite controlar granularmente qué partes de un mensaje deben ser visibles y cuáles deben permanecer privadas. El concepto que subyace bajo XML Signature es análogo, haciendo posible la firma digital no sólo del total de la comunicación entre dos puntos, sino también de documentos XML de forma independiente.

XML Signature se utiliza en SAML para proveer autentificación, es decir, determinar la identidad de la otra parte en una transacción, así como integridad de datos, esto es, la capacidad para confirmar que el mensaje recibido no presenta alteraciones con respecto al transmitido.

XML Encryption proporciona confidencialidad, de forma que, de todas las posibles entidades por las que el mensaje pueda pasar, sólo los destinatarios originales podrán leer el contenido cifrado que en él esté contenido.

Al no gozar aún estos dos estándares de difusión mayoritaria y para garantizar la seguridad no sólo a nivel de mensaje, sino también por debajo del protocolo SAML, el estándar recomienda el uso de **Secure Sockets Layer (SSL)** y su sucesor**, Transport Layer Security (TLS)**.

En los casos en que se requiere integridad y confidencialidad del mensaje, se recomienda el uso de SSL 3.0 o TLS 1.0. Los mismos protocolos deben usarse cuando se requiere autentificación tanto de servidor como de cliente.

La especificación SAML dedica un documento completo a consideraciones de seguridad, detallando las cuestiones relativas a este tema que surgen cuando empleamos determinados protocolos para transportar elementos del estándar.

4.2 La arquitectura SAML

Definición y relación entre los componentes

La especificación define la estructura y el contenido de cuatro elementos principales:

- **Assertions :** contienen información de identidad, autentificación y autorización sobre un sujeto determinado. Se definen mediante un Esquema XML y pueden ser enviadas de forma directa o expedirse como consecuencia de una solicitud, tal y como ya se distinguió en el apartado anterior. En esta memoria nos referimos a ellas también con los términos traducidos “aserto” y “aserción”.

- **Protocols :** definen cómo se solicitan las *assertions* y cómo se responde a dicha solicitud. Poseen su propio Esquema XML.

- **Bindings :** especifica cómo los mensajes de los protocolos SAML pueden transportarse utilizando protocolos de más bajo nivel, tal como HTTP o SOAP.

- **Profiles :** los protocolos, bindings y assertions de SAML se combinan para formar perfiles. Un perfil puede ser considerado como el conjunto de elementos e interacciones entre ellos que son necesarios para satisfacer un caso concreto de utilización de SAML.

La figura 5 ilustra la relación entre los componentes citados:

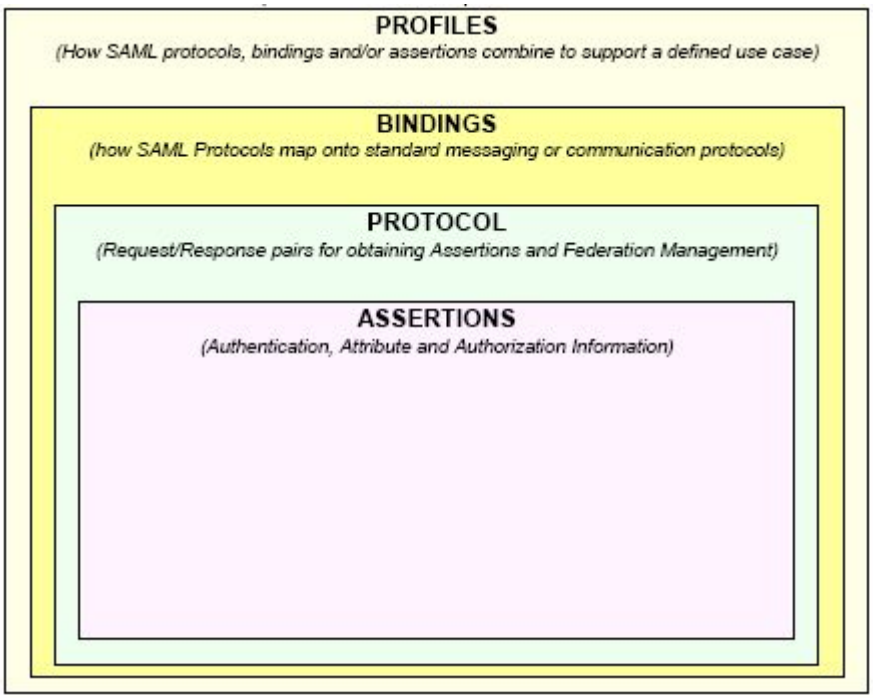

Figura 5: Relación entre los componentes de la arquitectura SAML

Los elementos de protocolo contienen a las aserciones, los correspondientes a los bindings contienen a los de protocolo y así sucesivamente. Un profile es, por tanto, el concepto más amplio dentro de la jerarquía de la arquitectura SAML e incluye a los otro tres. Las aserciones, en cambio, constituyen la base primordial sobre la que podemos construir un intercambio fiable de información de seguridad.

Enumeración de componentes

Ahondando un poco más en la relación anteriormente citada, una definición más detallada de los elementos que componen SAML sería la siguiente:

- **Assertions**

  Mediante una aserción o aserto SAML, una entidad (en principio, un Proveedor de Identidad) puede emitir una afirmación sobre las características y atributos de un usuario. Podría, por ejemplo, afirmar que el usuario es “Juan Teleco”, tiene “alumno” como rol en un dominio determinado, pertenece al grupo

"doctorandos", etc. Una aserción SAML puede transportar en su interior tres tipos de "statements" (declaraciones):

- **Authentication statements**

  Son expedidas por la entidad que ha llevado a cabo el proceso de autentificación del usuario. En una declaración de este tipo se recoge quien la ha emitido, el sujeto autentificado, el período de validez de la misma, además de otros datos relacionados con la autentificación. Nos referiremos a ellas también como declaraciones o afirmaciones de autentificación.

- **Attribute statements**

  Contienen detalles específicos sobre el usuario, nombre, dirección de email, rol, grupo al que pertenece, etc. Nos referiremos a ellas también como declaraciones o afirmaciones de atributos.

- **Authorization statements**

  Recogen datos sobre lo que le está o no permitido hacer al usuario. Por ejemplo, si está o no autorizado a acceder a un determinado recurso. Nos referiremos a ellas también como declaraciones o afirmaciones de autorización.

■ **Protocols**

Especifican cómo solicitar y proporcionar las aserciones SAML. Están codificados en esquemas XML como un conjunto de pares solicitud / respuesta. Los protocolos que se definen son:

- **Authentication Request Protocol**

  Define un mensaje `<AuthRequest>` que provoca como respuesta uno del tipo `<Response>`, el cual contiene una o más assertions, relativas a un determinado sujeto. Generalmente, la

solicitud es emitida por un Proveedor de Servicios y contestada por un Proveedor de Identidad tras haber completado con éxito un proceso de autentificación del usuario.

- **Assertion Query and Request Protocol**

  Se definen una serie de métodos para obtener asertos SAML ya existentes. Pueden solicitarse facilitando a un Proveedor de Identidad una referencia a dicho aserto, como el identificador único de aserción, mediante el uso del elemento `<AssertionIDRequest>`. Otros ejemplos incluyen el elemento `<AuthQuery>`, con el cual un SP solicitaría a un IdP las aserciones disponibles que contengan declaraciones de autentificación para un determinado usuario; el elemento `<AttributeQuery>`, mediante el cual se piden los valores de determinados atributos del usuario (es decir, una aserción que contenga "attribute statements"); y el elemento `<AuthzDecisionQuery>` para preguntar a un Proveedor de Identidad si un usuario está autorizado a realizar una determinada acción sobre un recurso determinado (la respuesta sería una aserción que contendría una declaración de autorización).

- **Artifact Protocol**

  Proporciona un mecanismo mediante el cual los mensajes del protocolo SAML pueden ser transportados por referencia en lugar de por valor. Tanto solicitudes como respuestas pueden ser obtenidas por referencia usando este protocolo especializado. El remitente, en vez de enviar un mensaje SAML sobre un protocolo de transporte, envía un pequeño fragmento de datos denominado ***artifact***. Dicho "artifact" puede tomar diversas formas pero necesariamente debe proveer un medio mediante el cual el destinatario pueda determinar quién lo envió. Si dicho destinatario lo desea, puede utilizar este protocolo en conjunción

con un binding SAML diferente para resolver el artifact, obteniendo el mensaje SAML original.

El uso más común para este mecanismo tiene lugar cuando el binding (véase apartado siguiente) SAML habitual no puede llevar de forma idónea un mensaje SAML por limitaciones de tamaño o también para permitir que emisor y receptor realicen la comunicación del mensaje por medio de un canal alternativo con, por ejemplo, medidas de seguridad especiales.

- **Otros protocolos**

  SAML proporciona mecanismos para implementar el "Enlace de Cuentas" (*Name Identifier Mapping Protocol*), para permitir el cierre cuasi-simultáneo de todas las sesiones abiertas pertenecientes a un mismo usuario (*Single Logout Protocol*), así como para modificar el valor o el formato del nombre de un sujeto (*Name Identifier Management Protocol*).

- **Bindings**

  Las especificaciones para "mapear" un protocolo SAML sobre un determinado protocolo de transporte reciben el nombre de binding. Se definen los siguientes:

  - **SAML SOAP Binding**

    Define cómo los mensajes del protocolo SAML se transportan contenidos en mensajes de SOAP 1.1. Especifica, adicionalmente, cómo dichos mensajes SOAP se transportan sobre HTTP.

  - **HTTP Redirect Binding**

    Cómo usar mensajes de redirección HTTP (por ejemplo, las respuestas HTTP con código de estado 302) para transportar mensajes SAML.

- **HTTP POST Binding**

  Especifica cómo se envía información SAML dentro del contenido de un formulario HTML con codificación base64.

- **HTTP Artifact Binding**

  Define cómo el protocolo HTTP transporta una referencia a una solicitud o respuesta SAML. Existen dos mecanismos: uno usa un formulario HTML, el otro, parámetros añadidos a la dirección URL.

- **Otros "bindings"**

  Puede citarse como ejemplo el *Reverse SOAP (PAOS) Binding*, que se utiliza en determinados perfiles SAML para dar soporte a pasarelas WAP.

■ **Profiles**

Un perfil describe cómo combinar determinadas aserciones, protocolos y bindings para componer en la práctica un escenario de uso de la especificación SAML.

- **Web Browser SSO Profile**

  Especifica cómo se puede proporcionar un servicio de firma Simple mediante un navegador web, utilizando para ello mensajes del Authentication Request Protocol en combinación con los bindings HTTP Redirect, HTTP POST y HTTP Artifact.

- **Assertion Query/Request Profile**

  Se define cómo el protocolo SAML del mismo nombre hace uso del SAML SOAP Binding.

- **Artifact Resolution Profile**

  Se define cómo el Artifact Protocol utiliza el SOAP Binding.

- **Enhanced Client and Proxy (ECP) Profile**
  Se describe la especificación usada para que los mensajes del protocolo Authentication Request sean usados conjuntamente con el Reverse SOAP (PAOS) Binding. Este perfil está diseñado para dar soporte a dispositivos móviles mediante pasarelas WAP.

- **Identity Provider Discovery Profile**
  Define los medios para que un Proveedor de Servicios descubra qué Proveedor(es) de Identidad está utilizando un determinado usuario.

- **Otros perfiles**
  Perfiles como el *Name Identifier Mapping Profile* , el *Single Logout Profile* y el *Name Identifier Management Profile* describen cómo utilizar los protocolos del mismo nombre, en conjunción con diversos bindings, tales como SOAP Binding, HTTP Redirect, etc.

Ejemplos de estructuras SAML

En esta sección proporcionamos ejemplos típicos de elementos del estándar. De nuevo seguimos como guía la figura 5, recorriendo los tres elementos más interiores: assertions, protocols y bindings. Nos ocuparemos de los profiles en una sección posterior.

- **Assertions :** como se ha descrito anteriormente, una aserción consta de una o más declaraciones (“statements”) de autentificación, autorización o de atributos. La **SAML authentication assertion** mostrada en la figura 6 contiene un elemento `<saml:AuthenticationStatement>` y ningún atributo:

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  MajorVersion="1" MinorVersion="1"
```

```
  AssertionID="a75adf55-01d7-40cc-929f-dbd8372ebdfc"
  IssueInstant="2004-12-05T09:22:02Z"
  Issuer="https://idp.example.org/shibboleth">
  <saml:Conditions
    NotBefore="2004-12-05T09:17:02Z"
    NotOnOrAfter="2004-12-05T09:27:02Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>http://sp.example.org/shibboleth</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AuthenticationStatement
    AuthenticationInstant="2004-12-05T09:22:00Z"
    AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:mace:shibboleth:1.0:nameIdentifier"
        NameQualifier="https://idp.example.org/shibboleth">
        3f7b3dcf-1674-4ecd-92c8-1544f346baf8
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>
          urn:oasis:names:tc:SAML:1.0:cm:bearer
        </saml:ConfirmationMethod>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

Figura 6: Aserción SAML de autenticación

Normalmente esta aserción SAML la emitirá un Proveedor de Identidad como parte de una **SAML Response** tras un proceso de autenticación de un usuario. La propiedad `Issuer` del elemento raíz de la aserción nos indica la entidad que ha expedido la aserción. La autenticación ha sido realizada gracias a la introducción de una contraseña, como podemos deducir del valor de `AuthenticationMethod`, y tiene una validez temporal dada por los límites que marcan `NotBefore` y `NotOnOrAfter`.

El valor del elemento `<saml:NameIdentifier>` es un ***handle***: un identificador numérico temporal y opaco que se asocia al usuario autenticado. Los mensajes posteriores usarán dicho identificador en vez de la identidad real del usuario.

El elemento `<saml:ConfirmationMethod>` tiene el siguiente valor:

`urn:oasis:names:tc:SAML:1.0:cm:bearer`

Debido a esto la aserción anterior se denomina también una *bearer assertion*. Cuando usamos un artifact para solicitar una aserción, el elemento anterior tendrá un valor distinto, como podemos comprobar en la figura 7:

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  MajorVersion="1" MinorVersion="1"
  AssertionID="003c6cc1-9ff8-10f9-990f-004005b13a2b"
  IssueInstant="2004-12-05T09:22:05Z"
  Issuer="https://idp.example.org/shibboleth">
  <saml:Conditions
    NotBefore="2004-12-05T09:17:05Z"
    NotOnOrAfter="2004-12-05T09:27:05Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>http://sp.example.org/shibboleth</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AuthenticationStatement
    AuthenticationInstant="2004-12-05T09:22:00Z"
    AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <saml:Subject>
      <saml:NameIdentifier
       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
       NameQualifier="https://idp.example.org/shibboleth">
       user@idp.example.org
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>
          urn:oasis:names:tc:SAML:1.0:cm:artifact
```

```
        </saml:ConfirmationMethod>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

Figura 7: Una aserción SAML como respuesta a un artifact

En este caso, la aserción se emite tras haber recibido un artifact y, por ello, el valor de `<saml:ConfirmationMethod>` es :

`urn:oasis:names:tc:SAML:1.0:cm:artifact`

Algunos escenarios de uso de SAML requieren asociar a un usuario algo más que un identificador opaco. La aserción anterior ilustra este caso: el valor del elemento `<saml:NameIdentifier>` es una dirección de correo electrónico. Esta dirección identifica de forma unívoca al usuario con respecto al Proveedor de Servicios.

Las dos aserciones anteriores contienen afirmaciones de autentificación. En la que aparece en la figura 8 nos encontramos, en cambio, con información relativa a atributos, en concreto, un **Attribute Statement**:

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  MajorVersion="1" MinorVersion="1"
  AssertionID="a144e8f3-adad-594a-9649-924517abe933"
  IssueInstant="2004-12-05T09:22:05Z"
  Issuer="https://idp.example.org/shibboleth">
  <saml:Conditions
    NotBefore="2004-12-05T09:17:05Z"
    NotOnOrAfter="2004-12-05T09:52:05Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>http://sp.example.org/shibboleth</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AttributeStatement>
```

```
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:mace:shibboleth:1.0:nameIdentifier"
        NameQualifier="https://idp.example.org/shibboleth">
        3f7b3dcf-1674-4ecd-92c8-1544f346baf8
      </saml:NameIdentifier>
    </saml:Subject>
    <saml:Attribute
  AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue Scope="example.org">
        maría.lópez
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Figura 8: Aserción SAML de atributos

Dentro del elemento `<saml:Attribute>` aparece el nombre del atributo, recogido en la propiedad `AttributeName`. Su valor es el del campo <saml:AttributeValue>. Nótese que el valor del campo <saml:NameIdentifier>, que corresponde a un handle, es el mismo que en el primer ejemplo de aserción que vimos (figura 6). Esto implica que esta Attribute Statement es producto de la misma transacción y se obtiene posteriormente a la Authentication Statement de la figura 6.

- **Protocols:** como se ha explicado anteriormente, con el Authentication Request Protocol solicitamos una aserción de autentificación y respondemos a dicha solicitud. En la figura 9 aparece una petición de autentificación en la que se entrega una dirección de email como identificador del usuario:

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ForceAuthn="true"
  AssertionConsumerServiceURL="http://www.example.com/"
  AttributeConsumingServiceIndex="0" ProviderName="string"
```

```
  ID="abe567de6"
  Version="2.0"
  IssueInstant="2005-01-31T12:00:00Z"
  Destination="http://www.example.com/"
  Consent="http://www.example.com/" >
    <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        <saml:NameID
     Format="urn: oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
   paco.teleco@company.com
        <saml:NameID>
    </saml:Subject>
</samlp:AuthnRequest>
```

Figura 9: Petición de Autenticación de SAML

La figura 10 corresponde a la respuesta a la solicitud anterior. El mensaje completo contendría una aserción de autentificación, la cual no se ha incluido en la figura para mayor claridad.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  ID="abe567de6"
  InResponseTo="example-noname" Version="2.0"
  IssueInstant="2005-01-31T12:00:00Z"
  Destination="http://www.example.com"
  Consent="http://www.example.com">
  <samlp:Status>
    <samlp:StatusCode Value="samlp:success"/>
    <samlp:StatusMessage>Success</samlp:StatusMessage>
    <samlp:StatusDetail/>
  <samlp:Status>

    --- AQUÍ SE INSERTARÍA UNA ASERCIÓN SAML DE AUTENTIFICACIÓN ---


</samlp:Response>
```

Figura 10: Respuesta de Autenticación de SAML

- **SOAP Binding :** en entornos donde ambos extremos de la comunicación poseen capacidad SOAP, es posible utilizar dicho protocolo para intercambiar pares de mensajes SAML petición / respuesta. En la figura 11 se observa un elemento del protocolo SAML, una SAML Response, siendo transportada dentro del cuerpo de un mensaje SOAP (en este caso, no se muestra la cabecera SOAP). Dicha SAML Response contiene una aserción que, a su vez, lleva en su interior una Authentication Statement.

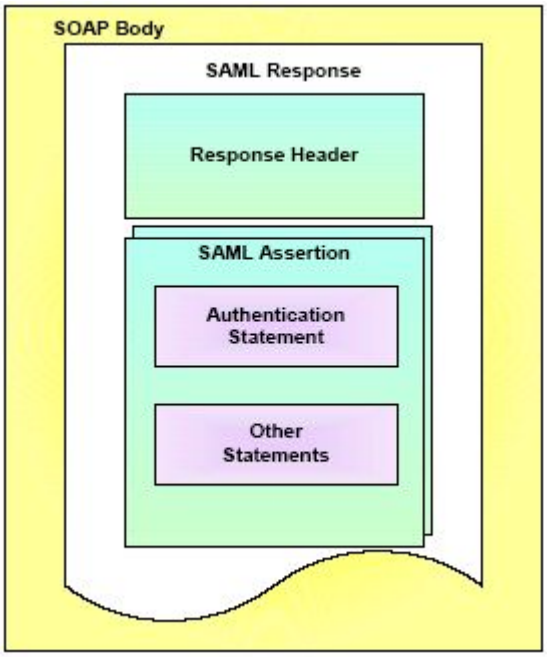

Figura 11: Transporte de aserción usando SOAP

La información SOAP será transportada generalmente utilizando el protocolo HTTP. La figura 12 ofrece un esquema de esta posibilidad: una SAML Request o SAML Response que se transporta dentro del cuerpo de un mensaje SOAP, embebido en HTTP.

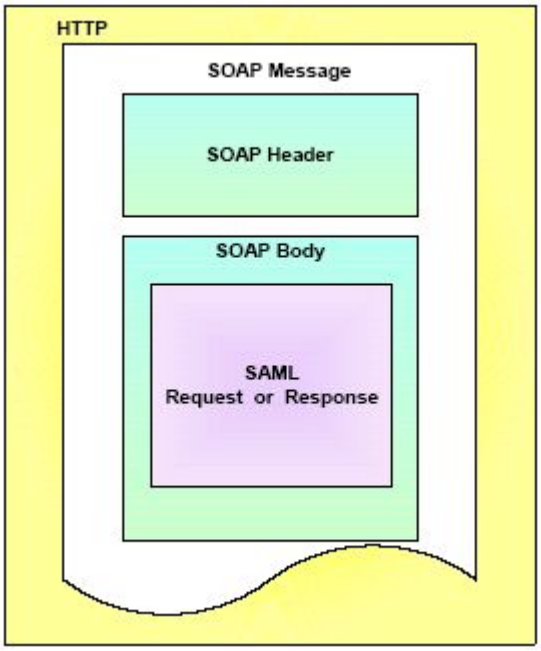

Figura 12: SOAP Binding transportado por HTTP

Un ejemplo del caso que acabamos de presentar aparece en la figura 13. En ella se envía una petición SAML, en concreto, una petición de atributos, dentro de un mensaje SOAP, usando el protocolo HTTP. Obsérvense las primera líneas, donde está ubicada la cabecera HTTP, y el elemento `Envelope`, que indica el inicio del contenedor SOAP:

```
POST /shibboleth/AA/SOAP HTTP/1.1
Host: idp.example.org
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security

<?xml version="1.1" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <samlp:Request
      xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
      xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
```

```
      MajorVersion="1" MinorVersion="1"
      IssueInstant="2004-12-05T09:22:04Z"
      RequestID="aaf23196-1773-2113-474a-fe114412ab72">
      <samlp:AttributeQuery
        Resource="https://sp.example.org/shibboleth">
        <saml:Subject>
          <saml:NameIdentifier
            Format="urn:mace:shibboleth:1.0:nameIdentifier"
            NameQualifier="https://idp.example.org/shibboleth">
            3f7b3dcf-1674-4ecd-92c8-1544f346baf8
          </saml:NameIdentifier>
        </saml:Subject>
        <saml:AttributeDesignator
        AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
        AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
      </samlp:AttributeQuery>
    </samlp:Request>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figura 13: Petición SAML transportada por HTTP

Como respuesta a la solicitud anterior, podríamos obtener la que aparece en la figura 14. En ella se insertaría una aserción de atributos, que no hemos incluido por razones de claridad. Como era de esperar, nos encontramos de nuevo con la cabecera HTTP y los elementos correspondientes a SOAP, como son `<SOAP-ENV:Header>` y `<SOAP-ENV:Body>`.

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn

<?xml version="1.1" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <samlp:Response
      xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
```

```
      InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
      IssueInstant="2004-12-05T09:22:05Z"
      MajorVersion="1" MinorVersion="1"
      ResponseID="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
      <samlp:Status>
        <samlp:StatusCode Value="samlp:Success"/>
      </samlp:Status>

      --- AQUÍ SE INSERTARÍA UNA ASERCIÓN SAML DE ATRIBUTOS ---


    </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figura 14: Respuesta SAML transportada por HTTP

4.3 Los perfiles SAML

La especificación SAML proporciona una potente infraestructura para dar soporte a multitud de casos reales de utilización. En los documentos que componen el estándar se mencionan tres de ellos:

- Web Browser Single Sign-On Profile
- Enhanced Client and Proxy (ECP) Profiles
- Federation

El perfil ECP se utiliza en casos especiales como, por ejemplo, el uso de una pasarela WAP como interfaz para dispositivos móviles que disponen de funcionalidad limitada, clientes donde no es posible usar redirección y situaciones dónde no existe la posibilidad de comunicación directa entre el Proveedor de Identidad y el de Servicios.

Con respecto al tercer perfil, como se comentó anteriormente, el uso de SAML para construir una federación no está descrito. La parte correspondiente al perfil “Federation” no se desarrolla en ninguno de los documentos oficiales de dicho estándar.

Así pues, nosotros nos ocuparemos exclusivamente del perfil denominado "Web Browser Single Sign-On", sobre el cual basaremos nuestro sistema.

Web Browser SSO Profile

SAML clasifica los posibles casos que pueden presentarse dentro de este perfil utilizando dos criterios:

- Según cómo se le proporcionan las aserciones al Proveedor de Servicios:

    - El Proveedor de Servicios recibe directamente la aserción, embebida en un mensaje SAML. Este caso se denomina ***push***.

    - El Proveedor de Servicios recibe una referencia a la aserción, un artifact, mediante el cual, a petición propia, podrá obtener la aserción referenciada. La especificación llama a este caso ***pull***.

Más adelante veremos casos tanto de tipo push (véase apartado "Redirección + POST", unas líneas más abajo), como pull (apartado "Redirección + Artifact"). Nuestro sistema Java se basará en un caso "push", es decir, se usará el envío de las propias aserciones SAML, en vez de referencias a las mismas.

- Según quién inicia el intercambio de mensajes:

    - Lo inicia el **Proveedor de Servicios**: el usuario desea acceder a un recurso en el propio SP, para el cual se requiere autorización. El Service Provider dirige entonces una petición al Identity Provider, solicitando que este último le envíe una aserción concerniente al usuario en cuestión.

    - Lo inicia el **Proveedor de Identidad**: el usuario está accediendo a recursos situados en el IdP (ya posee, por tanto, una sesión de

seguridad en el mismo) y desea iniciar el acceso a un recurso protegido en el SP. Éste recibirá, para ello, una aserción SAML, proveniente del Proveedor de Identidad, sin solicitud previa por parte del Service Provider.

Con respecto a la segunda clasificación, nuestro modelo de federación (véase apartado 1.4) define que la "entrada" a la misma se produce siempre por medio del intento de acceso, por parte de un usuario, a un recurso situado en uno de los servidores federados, el cual iniciará la secuencia de mensajes de identificación. Sólo consideraremos, por tanto, los casos en que el intercambio de mensajes sea iniciado por el Proveedor de Servicios.

A continuación vamos a describir dos ejemplos de uso dentro del perfil que nos ocupa. En ambos la acción se iniciará con un intento de acceso al Service Provider por parte de un usuario. En el primero se enviará una aserción SAML, mientras que en el segundo se usará un artifact.

- **Redirección + POST**

  El sistema Java implementado como parte fundamental de este proyecto se basa en este caso de uso. Más adelante describiremos exhaustivamente dicho sistema, explicando detenidamente todos los detalles técnicos de la implementación. A continuación nos referimos únicamente a lo que aparece sobre este caso en los documentos pertenecientes a la especificación SAML.

  En este caso disponemos de un navegador web(browser), de cuyo manejo se encarga el usuario. Existen asimismo un Proveedor de Servicios (www.abc.com) y un Proveedor de Identidad (www.xyz.com). El usuario trata de acceder a un recurso protegido situado en el Proveedor de Servicios. Al no disponer de una sesión de seguridad en dicho servidor , se envía una petición al Proveedor de Identidad, para que éste devuelva una aserción SAML que contenga información de autentificación sobre el usuario.

La figura 15 ilustra el intercambio de mensajes:

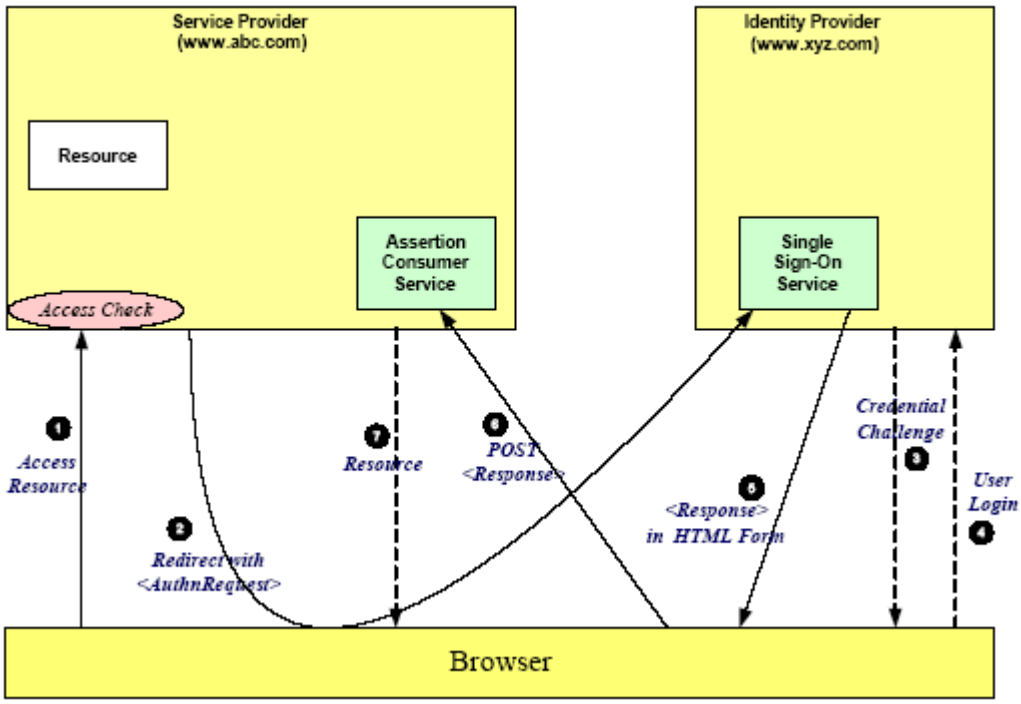

Figura 15: Caso de uso "Redirección + POST"

El proceso tiene lugar como describimos a continuación:

1. Mediante el uso de su navegador, el usuario trata de acceder a un recurso protegido ("Resource") que se encuentra en www.abc.com. Dicho usuario no dispone aún de una sesión iniciada en dicho servidor.

2. El Service Provider responde a la petición del navegador enviándole un mensaje de redirección, con código de estado HTTP 302 ó 303. Dicho mensaje contiene, en su cabecera, la dirección del Servicio Single Sign-On del Proveedor de Identidad, además de una petición SAML `<AuthnRequest>`. El browser procesa el mensaje de redirección y emite un GET dirigido al Single Sign-On Service, con la petición SAML como parámetro dentro del mensaje http.

3. El Servicio Single-On determina si el usuario dispone ya de una sesión de seguridad en el Proveedor de Identidad (en ese caso pasaríamos directamente al

paso 5) o si se requiere que se identifique, mediante algún proceso de autentificación.

4. El usuario proporciona una identificación válida, ya sea, mediante la introducción de un nombre y una contraseña o mediante otro método.

5. El Servicio Single Sign-On envía una página con un formulario HTML (HTML form) al navegador. Dicho formulario contiene una respuesta SAML dentro de la cual viaja una **SAML assertion** con información de autentificación sobre el usuario. La especificación SAML obliga a que dicha respuesta esté firmada digitalmente. La forma de incluir la información SAML en el formulario es utilizar un campo oculto del mismo.

6. Generalmente la página HTML que contiene al formulario mencionado en el apartado anterior incluirá algún mecanismo (como, por ejemplo, un botón "Submit" o una instrucción Javascript para reenvío automático) que tendrá como consecuencia que el navegador emita un mensaje POST cuyo destino será el Assertion Consumer Service del Proveedor de Servicios. Dicho mensaje POST transporta el mencionado formulario HTML.

7. El Assertion Consumer Service extrae la respuesta SAML del formulario HTML que acaba de recibir y valida la firma digital de la misma. Si es correcta, proporciona una **cookie** al navegador, estableciendo así una sesión de seguridad y lo redirige al recurso deseado. El control de acceso ("Access Check") comprueba el valor de la cookie del usuario y devuelve a éste el recurso solicitado.

El nombre de este primer caso de uso proviene del método utilizado para el envío de la petición SAML (una redirección HTTP) y para la respuesta (un HTTP POST con un formulario en su interior).

- **Redirección + Artifact**

En esta ocasión el escenario lo componen los mismos elementos que en la anterior: un usuario que dispone de un navegador, un recurso deseado en un Proveedor de Servicios y un Proveedor de Identidad. Al igual que antes, el Proveedor de Servicios envía una petición SAML al IdP para poder autentificar al usuario. La diferencia estriba en que, en este caso, el Proveedor de Identidad no proporciona como respuesta la propia aserción SAML, sino una referencia a la misma, un artifact. Dicha referencia podrá ser usada por el Proveedor de Servicios en un paso posterior para conseguir la aserción referenciada.

La figura 16 ilustra el caso:

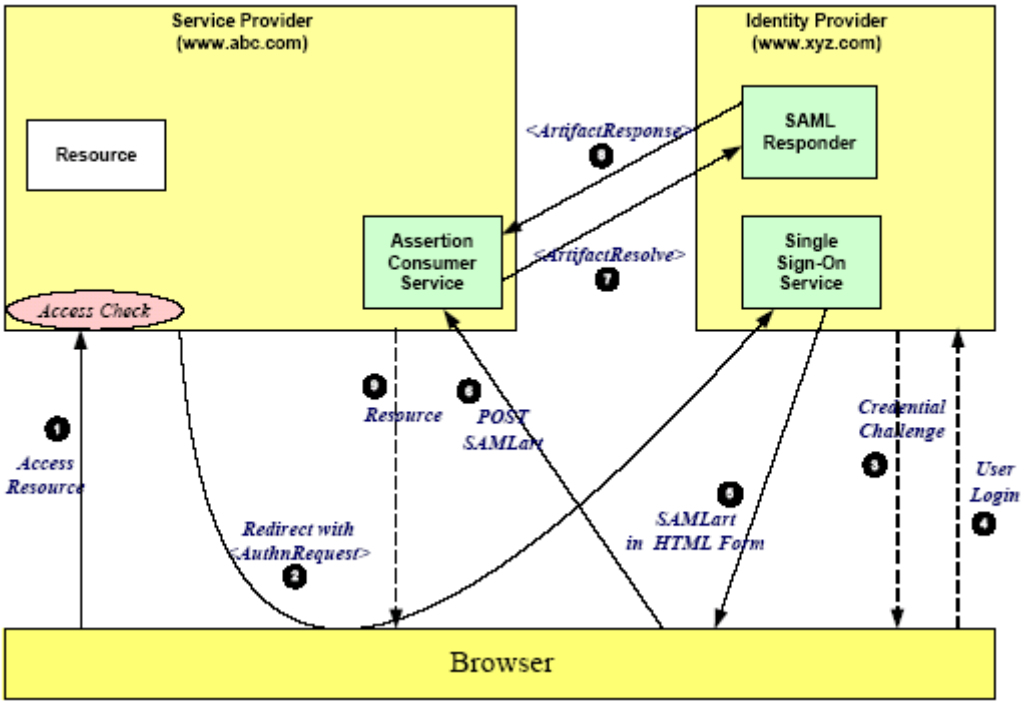

Figura 16: Caso de uso "Redirección + artifact"

El proceso tiene lugar como describimos a continuación (los pasos 1 – 4 son los mismos que en el caso anterior):

1. Mediante el uso de su navegador, el usuario trata de acceder a un recurso protegido (“Resource”) que se encuentra en www.abc.com. Dicho usuario no dispone aún de una sesión iniciada en dicho servidor.

2. El Service Provider responde a la petición del navegador enviándole un mensaje de redirección, con código de estado HTTP 302 ó 303. Dicho mensaje contiene, en su cabecera, la dirección del Servicio Single Sign-On del Proveedor de Identidad, además de una petición SAML `<AuthnRequest`. El “browser” procesa el mensaje de redirección y emite un GET dirigido al Single Sign-On Service, con la petición SAML como parámetro en la línea de dirección del navegador.

3. El Servicio Single-On determina si el usuario dispone ya de una sesión de seguridad en el Proveedor de Identidad (en ese caso pasaríamos directamente al paso 5) o si se requiere que se identifique, mediante algún proceso de autentificación.

4. El usuario proporciona una identificación válida, ya sea, mediante la introducción de un nombre y una contraseña o mediante otro método.

5. El Servicio Single Sign-On genera una aserción SAML y un artifact. Dicho artifact contiene un identificador único del SAML Responder de www.xyz.com y una referencia a la aserción creada, denominada **AssertionHandle**. El Servicio Single Sign-On envía una página con un formulario HTML (HTML form) al navegador. Dicho formulario contiene el artifact creado. La forma de incluir la información SAML en el formulario es utilizar un campo oculto del mismo. La especificación SAML permite también que la respuesta del Servicio Single Sign-On se efectúe usando una redirección HTTP (un mensaje con código de estado 302 ó 303) en lugar de con un formulario HTML.

6. Generalmente la página HTML que contiene el formulario mencionado en el apartado anterior incluirá algún mecanismo (como, por ejemplo, un botón “Submit” o una instrucción Javascript para reenvío automático) que tendrá como consecuencia que el navegador emita un mensaje POST cuyo destino será el

Assertion Consumer Service del Proveedor de Servicios. Dicho mensaje POST transporta el mencionado formulario HTML.

7. El Assertion Consumer Service extrae el artifact del formulario que acaba de recibir. En él lee el identificador único del SAML Responder de www.xyz.com y la referencia a la aserción. El Proveedor de Servicios poseerá algún medio para establecer la correspondencia entre dicho identificador único y la dirección del SAML Responder al que debe dirigirse. El Assertion Consumer Service envía entonces a dicha dirección un mensaje SAML `<ArtifactResolve>`, que contiene el "artifact" proporcionado por el Identity Provider.

8. El SAML Responder del Proveedor de Identidad devuelve una respuesta SAML `<ArtifactResponse>` en cuyo interior viaja la aserción que el propio IdP generó en el paso 5. Tan pronto como reciba la aserción válida, el Assertion Consumer establecerá una sesión de seguridad en www.abc.com para el usuario.

9. El Assertion Consumer Service redirige al navegador al recurso deseado, enviándole, asimismo, una cookie que identifica la sesión creada en el paso anterior. El control de acceso ("Access Check") comprueba el valor de la cookie del usuario y devuelve a éste el recurso solicitado.

El nombre de este primer caso de uso proviene del método utilizado para el envío de la petición SAML (una redirección HTTP) y para la respuesta (un artifact).