Capítulo 6

Otras iniciativas de identidad federada

Contenido

- 6.1 Introducción
- 6.2 Liberty Alliance
- 6.3 WS-Federation
- 6.4 Microsoft Passport

6.1 Introducción

Además de SAML y Shibboleth, han surgido en los últimos años otras alternativas en el terreno de la gestión electrónica de identidad. En general, comparten objetivos y, en algunos aspectos, presentan similitudes.

La gran proliferación de servicios en Internet que cuentan con control de acceso, provoca que un usuario medio tenga que recordar numerosos identificadores y contraseñas. Este problema afecta también a los empleados de grandes empresas con múltiples dominios de seguridad. Esto ha llevado a intentar desarrollar soluciones que

faciliten el acceso a estos servicios, mediante el uso de una identidad única o identidad federada.

Una gran motivación en el desarrollo de estas soluciones la constituye, sin duda, el comercio electrónico. Las páginas de agencias de viajes, subastas, supermercados, etc. exigen generalmente poseer un nombre de usuario y una contraseña para poder adquirir sus servicios. Se busca que el usuario, una vez autentificado en una de estas páginas, pueda pasar a otra asociada a ella y siga comprando sin necesidad de tener que volver a autentificarse. Una parte considerable de la población mira aún con recelo la compra por Internet, tanto por temor al posible robo de datos privados (número de tarjeta de crédito y cuentas bancarias, contraseñas, etc.), como por el hecho de percibir el proceso que conlleva como algo engorroso. Para eliminar las trabas que frenan al potencial comprador, es necesario, por una parte, simplificar la mecánica del proceso y, por otra, que el usuario lo perciba como algo seguro y que no invade su intimidad. El objetivo final consiste en animar a más clientes a superar la barrera que supone Internet a la hora de gastar su dinero.

En el fondo se trata siempre de una serie de servidores o bases de datos independientes que deciden compartir información sensible, así que el fundamento técnico que subyace bajo la mayoría de estas iniciativas no es otro que la federación de sistemas.

A continuación, realizamos un breve análisis de algunas de estas iniciativas.

6.2 Liberty Alliance

El proyecto conocido con el algo pomposo nombre de Liberty Alliance ("Alianza por la Libertad") se formó en el año 2001. Actualmente las entidades de las que está constituido suman más de 150, entre empresas, organizaciones sin ánimo de lucro y agencias gubernamentales. Su objetivo es desarrollar especificaciones y estándares abiertos para el soporte de una infraestructura completa de identidad federada que sea compatible con los dispositivos de red actuales y futuros.

La organización promueve federaciones de sistemas (**círculos de confianza**, según su propia terminología) donde el intercambio de información sobre los usuarios está controlado, mediante permisos, por los propios usuarios. Se trata, por tanto, de una iniciativa que tiene muy presente el respeto a la privacidad y el anonimato en Internet.

El desarrollo de las especificaciones de Liberty Alliance se ha dividido en tres fases, cada una de las cuales añade funcionalidades al conjunto:

- **Fase 1**

  La primera de las fases se centró en proporcionar un sistema single sign-on a través de la federación de cuentas de portales con una relación de confianza, creando la estructura **Liberty Identity Federation Framework (ID-FF)**.
  Liberty definió esta estructura añadiendo funcionalidades extra a la versión 1 del estándar SAML, la cual sirvió como base. La versión 1.0 de ID-FF apareció en Julio de 2002, y su revisión 1.1 en enero de 2003. Reconociendo el valor de contar con un único estándar para la identidad federada, Liberty Alliance remitió la versión 1.2 al Security Services Technical Comittee de OASIS, para que fuera tenida en cuenta durante la construcción del estándar SAML v2.0. Las especificaciones de esta primera fase están ya disponibles en muchos productos, actuando como base para todos los elementos venideros.

- **Fase 2**

  Esta segunda fase está enfocada al desarrollo de los Servicios Web basados en la identidad digital. El resultado es la estructura **Identity Web Services Framework (ID-WSF)**, que pretende ser la primera piedra sobre la que se asiente el uso y explotación de todo el potencial que se atribuye a los servicios web. Un concepto muy importante que se introduce es el de los perfiles de seguridad. Los perfiles de seguridad permiten a los sistemas, entre otras cosas, compartir información sobre los usuarios federados, siendo los propios usuarios los que eligen qué atributos o datos personales serán revelados. Esta información compartida será la que utilicen los distintos sitios o portales para ofrecer a los usuarios una personalización de sus servicios. La estructura ID-

WSF utiliza aserciones SAML como base para el intercambio de información de seguridad, siendo compatible con la versión 2.0 de este estándar.

- **Fase 3**

  La tercera fase, no publicada aún, tiene como objetivo una colección de especificaciones llamadas Liberty Alliance Identity Services Interface Specifications (ID-SIS), que proveerán a las empresas de modos estándar de construir servicios interoperables como perfiles de registro, libros de contactos, calendarios, localización geográfica, etc.

Las especificaciones Liberty Alliance tienen mucho en común con las de SAML, apareciendo elementos ya conocidos como el Identity Provider, Service Provider, etc. La comunicación necesaria para los procesos se realiza, por tanto, a través de XML, que se transporta sobre SOAP y HTTP. Se usan también redirecciones del navegador y envío de formularios HTML. En cuanto a las medidas de seguridad en las comunicaciones, puede usarse XML Signature para la autentificación de los asertos SAML. Igualmente, también puede utilizarse SSL, al emplear HTTP como mecanismo de transporte.

Liberty Alliance lleva a cabo pruebas de interoperabilidad de los programas basados en sus especificaciones, para las empresas que así lo soliciten. Para conseguir la certificación oficial del consorcio, el producto debe ser capaz de interoperar de forma satisfactoria con, al menos, dos programas del mismo tipo de otros fabricantes. Si las pruebas se superan con éxito, el producto recibe un sello oficial, el **Liberty Interoperable Logo**, que lo certifica como software compatible con el estándar de la alianza. El programa Liberty Interoperable Logo ha sido ofrecido por Liberty Alliance desde 2003, y 15 fabricantes con más de 30 productos ya lo han completado con éxito. Desde Julio de 2005, las pruebas de interoperabilidad incluyen tests específicos de compatibilidad con SAML v2.0.

Una de las posibilidades contempladas en las especificaciones Liberty Alliance (también en las de SAML) y que Shibboleth no implementa es el ***single sign-out***. De la misma forma que resulta útil necesitar tan sólo un proceso de autenticación para tener

acceso a numerosos sistemas asociados, es igualmente interesante tener la capacidad de cerrar con un solo clic de ratón todas las sesiones que hemos establecido con dichos sistemas.

Para llevar a cabo este proceso, que se ilustra en la figura 20, son necesarios los siguientes pasos:

1. El usuario realiza una petición al Identity Provider en el que está registrado, para que éste cierre su sesión en todas las aplicaciones web en las que se encuentre autentificado.

2. El Proveedor de Identidad envía peticiones de cierre de sesión a todos y cada uno de los Service Providers en los que el usuario se había autentificado.

Figura 20: Proceso de single sign-out

6.3 WS-Federation

Microsoft, IBM y otras empresas que no forman parte de Liberty Alliance han creado sus propias especificaciones abiertas en respuesta a los trabajos de la alianza. Se trata de una serie de especificaciones (hasta siete) que persiguen exactamente los mismos objetivos que la Liberty Alliance.

Una descripción general de las especificaciones puede encontrarse en el documento **Security in a Web Services World: A Proposed Architecture and Roadmap**, publicado conjuntamente por IBM y Microsoft. Cada especificación se basa en las aparecidas anteriormente. La última publicada, WS-Federation, es el equivalente a la fase 1 de las especificaciones de Liberty. A continuación presentamos una breve descripción de cada una de ellas:

- **WS-Policy:** descripción de las políticas de seguridad de cada integrante de la red de confianza.
- **WS-Trust:** descripción de los modelos de confianza que permiten operar a los servicios web con seguridad.
- **WS-Privacy:** descripción de las cuestiones referentes a la privacidad de la información de usuarios y sistemas.
- **WS-Security:** comunicación segura de las credenciales de usuarios y sistemas. Sería el equivalente de SAML en Liberty Alliance.
- **WS-Federation:** federación de cuentas y gestión de identidad.
- **WS-SecureConversation:** comunicación segura de mensajes.
- **WS-Authorization:** descripción de la gestión de los datos y políticas de autorización.

Los desarrollos que Microsoft e IBM están emprendiendo en el campo de la federación no son aún compatibles con SAML aunque algunas de sus especificaciones, como WS-Security ya han sido remitidas a organizaciones como OASIS para su estandarización. Una vez que todas se hagan públicas (sólo faltan las dos últimas), las dos compañías esperan remitirlas como un único conjunto a la Web Services Interoperability Organization (WS-I) para su consideración.

6.4 Microsoft Passport

Passport es un sistema de firma única o Single Sign-On desarrollado por Microsoft para los clientes de sus sitios web. Aunque, en principio, se permitía que otras empresas asociadas al programa pudieran incluir sus propios servidores dentro del servicio, Microsoft ha confirmado que detendrá este uso de Passport por parte de entidades ajenas a su propia compañía.

Passport y el proyecto basado en él, HailStorm, no son especificaciones abiertas sino un servicio ofrecido por Microsoft a los usuarios de sus páginas. Gracias a este servicio, un usuario que se haya autenticado en una página de un servidor perteneciente a Microsoft, no tendrá que volver a hacerlo al visitar otra de los sitios de esta compañía.

Passport fue criticado por abogados de la Electronic Frontier Foundation por considerarlo como una amenaza para la privacidad de sus usuarios. Esto forzó a Microsoft a modificar los términos en los que se ofrecía el servicio, para acallar las críticas en este sentido.

A pesar de la aparición en algunos medios de comunicación de noticias relativas al abandono de este proyecto, Microsoft llevó a cabo una extensa actualización del servicio en Mayo de 2005.