Primer Taller de Seguridad en Ingeniería del Software y Bases de Datos (SISBD'2004)

Málaga
9 de Noviembre de 2004

Eduardo Fernández-Medina y Mario Piattini (Eds.)

Primer Taller de Seguridad en Ingeniería del Software y Bases de Datos (SISBD'2004)

Málaga
9 de Noviembre de 2004

ACTAS

Iniciativa enmarcada en las actividades de la red RETISTIC (Red temática de investigación en el campo de la Seguridad en las Tecnologías de la Información), financiada por el Ministerio de Ciencia y Tecnología (TIC-2002-12487-E)

Presentación

La Seguridad en los sistemas de información es uno de los desafíos más importantes que están asumiendo actualmente muchas de las organizaciones. A pesar de que muchas empresas han descubierto lo crítico que resulta una correcta confidencialidad, integridad y disponibilidad de su información para el éxito de sus negocios y operaciones, muy pocas han adaptado sus sistemas para mantener la información segura, evitando accesos no autorizados, previniendo intrusos, e impidiendo el descubrimiento de información confidencial.

Actualmente, existen muchos avances tecnológicos que estimulan la utilización de sistemas de información en muchos entornos de negocio. Estos sistemas utilizan grandes cantidades de datos, que son gestionados y almacenados por bases de datos y almacenes de datos. A a menudo gestionan información que es especialmente sensible, puesto que se refieren a aspectos protegidos por las leyes de protección de datos personales (creencias, datos médicos, etc.). Por tanto, la adecuada gestión de la seguridad, así como la implantación de medidas técnicas que garanticen la seguridad de estos sistemas de información y la información que éstos gestionan resulta crucial.

Este taller se centra en analizar las aportaciones que desde la ingeniería del software y las bases de datos pueden realizarse con el fin de construir sistemas de información más seguros.

Organizadores

Eduardo Fernández-Medina (Universidad de Castilla-La Mancha)
Mario Piattini (Universidad de Castilla-La Mancha)

Grupos Participantes

- Asociación de Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones (ASIA)
- Excelentísima Diputación de Ciudad Real
- Informáticos Europeos Expertos
- Universidad Carlos III
- Universidad de Castilla La Mancha
- Universidad Católica del Maule (Chile)
- Universidad Complutense de Madrid
- Universidad Politécnica de Catalunya
- Universidad de Deusto
- Universidad de Lleida
- Universidad de Málaga
- Universidad de Murcia
- Universidad Rey Juan Carlos

Índice

Estado del Arte de la Federación de Identidades mediante Servicios Web

Carlos Gutiérrez García, Eduardo Fernández-Medina Patón, Mario Piattini Velthuis

Alarcos Research Group. Universidad de Castilla-La Mancha.
Paseo de la Universidad 4, 13071, Ciudad Real. (SPAIN). Tel: 34 926 29 53 00
{Carlos.Gutierrez, Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract. Las organizaciones hoy en día poseen estructuras muy complejas formadas por numerosas unidades de negocio, tanto internas como externas, que se encuentran ubicadas en distintos puntos geográficos y además tienen establecidas entre sí todo tipo de relaciones (comerciales, operativas, etc.). La espectacular evolución que ha sufrido Internet en los últimos 10 años la convierte sin lugar dudas en el medio de conexión o en la infraestructura idónea sobre la que materializar estas distribuciones corporativas. Un ejemplo evidente de este hecho es el uso generalizado del correo electrónico como principal medio de comunicación interorganizacional o la creación de portales corporativos. Pero no sólo vale con hacer presentes estas unidades organizativas en la Web, además, también se espera que las personas que trabajan en ellas (o sean clientes de ellas) puedan, de forma transparente, cruzar los límites de su organización para entrar en los dominios de otras corporaciones con las que su organización de origen tenga establecida una relación de confianza. Una ventaja inmediata que ofrece este escenario es que habilita un entorno Single Sign-On (SSO) en el que el usuario podrá navegar por aquellos sitios Web de confianza teniendo que identificarse solamente una vez en su sitio Web de origen. Este concepto de federación interorganizacional basada en Internet será el tema que trataremos con profundidad en este artículo. Básicamente el artículo se divide en dos partes. En la primera parte veremos los conceptos básicos de la federación de servicios Web, apartado 2, y en la segunda, apartado 3, haremos un breve repaso de los principales estándares y especificaciones existentes. El último apartado reflejará unas conclusiones finales.

1 Introducción al concepto de federación

El concepto de federación, tal y como se aplica en este contexto, consiste en la capacidad de interacción entre agentes pertenecientes a distintos dominios de confianza y, por tanto, con políticas de seguridad independientes [8] . El aspecto clave de los servicios federados es definir una forma estándar de establecer y reflejar la confianza entre las organizaciones. Obviamente estas relaciones deberán estar sujetas a un marco legal de forma que la privacidad de los usuarios y la reputación de las empresas que forman parte de una federación se sientan protegidas.

La federación tiene que ver directamente con los servicios de seguridad de autenticación y autorización. La **federación de las identidades** Web entre dominios de confianza permite que los usuarios puedan identificarse una vez y acceder a todos ellos de manera transparente. Debemos tener en cuenta que cuando hablamos de usuarios, pueden ser tanto personas como usuarios computacionales (otros servicios Web).

El proyecto Liberty Alliance Project o el proyecto Passport de Microsoft son dos ejemplos de marcos de trabajo cuyo primer objetivo es la federación de las identidades que habiliten servicios SSO. Como veremos en el apartado 3, la federación también garantiza que las identidades locales utilizadas por un mismo usuario en distintos sitios federados se encuentren conectadas mediante técnicas de gestión de la federación (por ejemplo mediante pseudónimos).

El potencial que podemos apreciar sobre la posibilidad de que nos autentiquemos una sola vez y a partir de ese momento seamos capaces de interaccionar con servicios ubicados en otros dominios de confianza puede no ser siempre tal. De hecho, en la práctica no nos interesa tener una única identidad en la Web sino varias: una identidad cuando accedemos desde casa, otra cuando accedemos desde la oficina, etc. En realidad el gran potencial de un servicio SSO está en que permita que una entidad defina el número exacto de las identidades Web que desea tener [11].

La **federación de la autorización** se consigue mediante la federación de los atributos de privilegio de los usuarios de forma que un servicio Web que actúa en cierto dominio de confianza pueda ejecutar sus políticas de acceso a partir de los privilegios de los usuarios pertenecientes a otros dominios de confianza federados. La arquitectura original basada en Internet que trata este problema es la definida por el proyecto Shibboleth [9]. Entre los estándares que permiten la portabilidad de los elementos de seguridad entre los diferentes dominios de confianza están WS-Trust [2], mediante los protocolos que permiten la emisión, renovación, validación y conversión de tokens de seguridad firmados por entidades de confianza, y SAML [6], mediante la expresión en XML de declaraciones de autenticación, autorización y de atributos.

Otro aspecto fundamental de la federación es la **privacidad**. En este contexto la privacidad se debe considerar de manera doble: privacidad de las identidades de los usuarios y la privacidad de los atributos federados entre los dominios de confianza.

La **privacidad de la identidad** consiste en que sea imposible (idealmente) conocer la traza de la actividad llevada a cabo por un usuario (identidad) en su navegación por los sitios ubicados por los distintos dominios de confianza federados. La solución a este problema se basa en el uso de pseudónimos que impidan a los distintos servicios accedidos por un usuario vincular sus acciones.

Por su parte la **privacidad de los atributos** consiste en el desvelamiento controlado por políticas de privacidad de los atributos federados. Es decir, se comparten los atributos de los usuarios entre los dominios pero se revelan de forma controlada mediante políticas de privacidad específicas definidas por los propios usuarios.

La federación comienza por lo tanto a partir de la noción de identidad federada. Es decir, el solicitante o alguien en quién éste delega (un servicio Web que actúa como proveedor de identidades con la autoridad propietaria de la información de identidad de los principales de su dominio) declara una identidad y un proveedor de identidades la verifica.

2 Proceso de federación

En este apartado vamos a recorrer los distintos conceptos relacionados con la federación mediante un escenario de ejemplo.

Imaginemos dos típicos portales ficticios ejemplo-vuelos.com y ejemplo-coches.com que se dedican a vender billetes de avión y a realizar alquileres de vehículos a sus usuarios registrados, respectivamente. Un buen día deciden establecer una relación comercial de forma que los usuarios que acceden desde alguno de los dos sitios al otro recibirán una rebaja de un x % en la compra o reserva de sus productos. Además, se desea que si un usuario se autentica correctamente en alguno de los dos sitios no tenga por qué volver a autenticarse en el otro.

Para ello, en primer lugar ambos sitios Web deberán **definir el marco legal** bajo el que colaborarán de forma que se sientan respaldados legalmente. Este marco legal será la protección respaldo tangible para la relación de confianza que establezcan.

Como primera medida ven la necesidad de **federar las identidades** de sus usuarios. Con este objetivo en mente, introducen en sus portales respectivos una nueva opción que invita a los usuarios, una vez autenticados, a federar su identidad con el otro portal. Si el usuario acepta esta propuesta, ambos sitios Web deberán, de alguna manera comunicarse las identidades locales de ese usuario de forma que puedan conocer con certeza qué usuario es en cada momento. Imaginemos que Juan tiene una única cuenta en ejemplo-vuelos.com, bajo la identidad JuanVuelos y que un día decide registrarse en el sitio ejemplo-coches.com bajo la identidad de JuanCoches. La siguiente vez que se autentica en ejemplo-vuelos.com se le invita a federar esa identidad con el sitio ejemplo-coches.com y, gracias a la llamativa rebaja, acepta sin dudar. En ese momento, entre ambos sitios Web deberán llevar a cabo algún proceso que les permita intercambiarse las identidades locales de Juan. Por ejemplo (ver figura 1), el portal ejemplo-vuelos.com podría redirigir el navegador de Juan al sitio ejemplo-coches.com incluyendo en la URL un testigo de petición de federación de la identidad de ese usuario redirigido (2). En ese momento ejemplo-coches.com autentica al usuario (2), es decir conoce que su identidad es JuanCoches, y procede a federar esa identidad con el identificador JuanVuelos incluido en el testigo (3). Así mismo redirigirá al usuario de nuevo a ejemplo-vuelos.com incluyendo en la URL un testigo de respuesta a la petición de federación que incluya la identidad de Juan en ejemplo-coches.com (4). En ese momento se completará la federación de las identidades locales de Juan en ambos dominios (5).

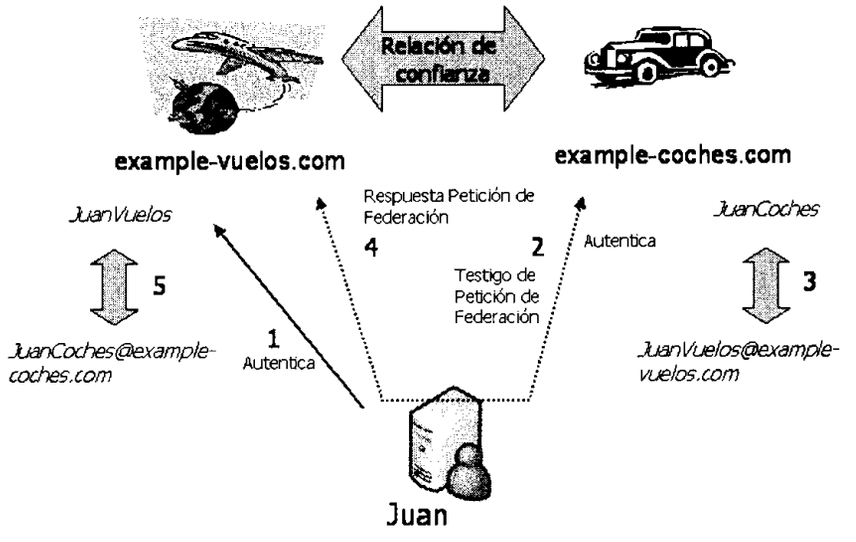

Fig. 1. Federación de identidades locales de un mismo usuario ubicadas en dominios de confianza federados.

Una vez Juan ha federado sus identidades, podrá utilizar el **servicio SSO** (ver figura 2). La siguiente vez que Juan se autentique en ejemplo-vuelos.com (1), realice su reserva de avión, y desee dirigirse a ejemplo-coches.com para realizar la reserva del coche, se le redirigirá adjuntándole algún tipo de testigo que evidencie que el sitio ejemplo-vuelos.com ya le autenticó (2). Ese testigo puede simplemente contener un identificador del testigo (un flujo de octetos lo suficientemente grande como para que no sea posible su adivinación) y otro identificador del sitio ejemplo-vuelos.com. Cuando ese testigo le llegue a ejemplo-coches.com, sabrá que procede de ejemplo-vuelos.com y entonces le realizará una petición, tomando el rol de servicio Web consumidor, solicitándole una confirmación de que, efectivamente, autenticó al usuario que le presenta ese testigo (3). El servicio Web ejemplo-vuelos.com devolverá una respuesta afirmativa en la que incluirá información acerca del proceso de autenticación que llevó a cabo para ese usuario incluyendo su nombre de usuario, JuanCoches, en el dominio del solicitante. En ese momento, ejemplo-coches.com sabrá que fue efectivamente JuanCoches quién fue autenticado y asociará todas las acciones que lleve a cabo con esa identidad. Este esquema SSO es un ejemplo de entre los muchos perfiles SSO que definen las especificaciones que veremos en el apartado 4.

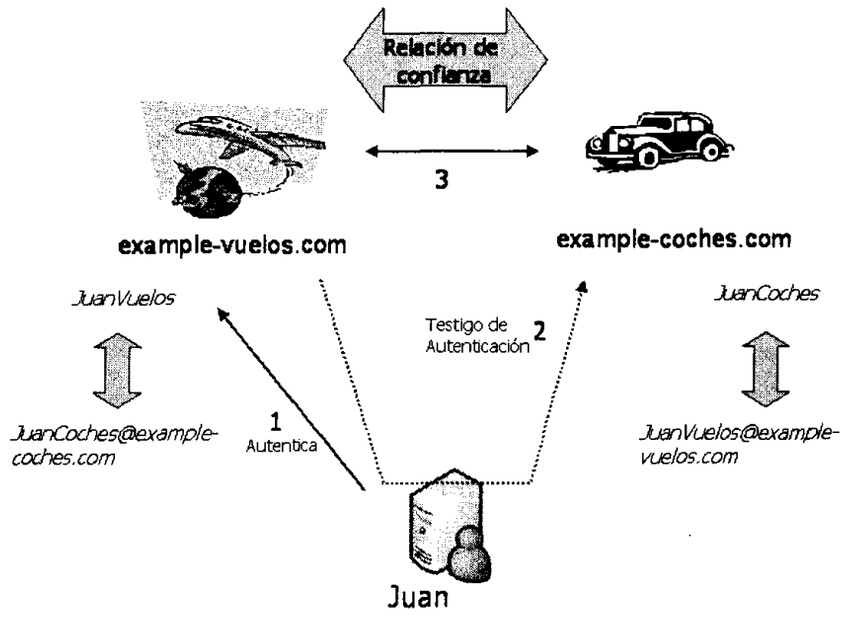

Fig. 2. Esquema general de autenticación SSO.

Fenomenal, pero todo esto parece poco realista, ¿cómo podemos pensar que una organización va a revelar su directorio de usuarios a otra organización? ¿Cómo va un servicio de banca en Internet a proporcionar las identidades de sus usuarios a un servicio de compra de acciones en bolsa sin la consiguiente preocupación sobre la privacidad de los usuarios?

Este problema se puede resolver si durante el proceso de federación, los dominios no se intercambian las identidades locales sino unos **pseudónimos** que estén asociados con las identidades locales de Juan en cada uno de los dominios. Durante el proceso de federación de las identidades, ejemplo-coches.com puede enviar un pseudónimo, por ejemplo *asdf* a ejemplo-vuelos.com, y después de que ejemplo-vuelos.com autentique al usuario le asocia el pseudónimo *poiuy* que comunica al servicio ejemplo-coches.com. De esta forma, ejemplo-vuelos.com sabe que cuando JuanVuelos deba ser redirigido a ejemplo-coches.com se deberá enviar la identidad *asdf* mientras que cuando ejemplo-coches.com haga la petición del testigo que confirma que el usuario fue autenticado, enviará el pseudónimo *poiuy*. Normalmente, y con el objetivo de mantener el anonimato, las partes cooperantes querrán, cada cierto tiempo renovar estos pseudónimos y, por lo tanto, deberán ser capaces de renovar los pseudónimos mediante algún **protocolo de federación de renovación de pseudónimos** sin deshacer la federación existente.

Si existiera un nuevo sitio Web que quisiera establecer una nueva relación de confianza con ejemplo-vuelos.com se federarán las identidades otorgando otro par de pseudónimos distintos de forma que entre en el nuevo sitio Web y ejemplo-coches.com será imposible relacionar las acciones que Juan ha realizado.

Una vez Juan haya completado sus actividades en el portal ejemplo-vuelos.com (o simplemente se termina su sesión por superar el tiempo de inactividad) podría señalizar su intención de terminar la sesión de forma que se deberá llevar a cabo un proceso de **Single Log-Out (SLO)**, también conocido como Single Sign-Out (ver figura 3). En este caso, el sitio Web ejemplo-vuelos.com deberá comunicar a ejemplo-coches.com que se dio por finalizada la sesión del usuario (3). A partir de ese momento ambos sitios limpiarán sus cachés locales que contienen la información sobre el proceso de autenticación SSO que llevó a cabo el usuario Juan de forma que la siguiente vez que desee volver a utilizar los servicios de la federación tenga que volver a autenticarse (2) y (4). Debemos tener en cuenta que cuando un usuario realiza logout podría pretender hacerlo en el contexto de la federación completa o tan sólo del sitio Web en el que se encuentra, por ello, normalmente el sitio Web dispondrá de dos opciones para realizar el logout de forma que se contemplen ambas posibilidades.

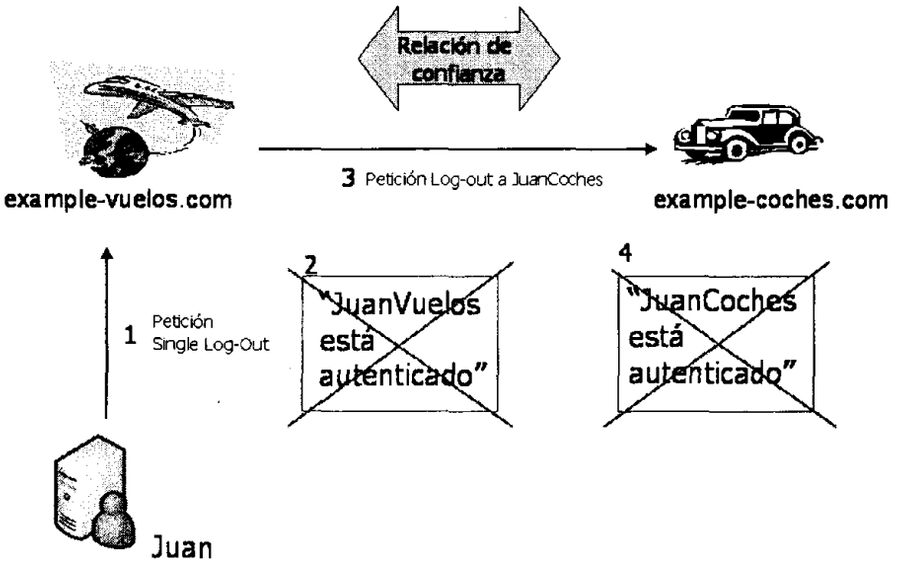

Fig. 3. Pasos seguidos durante el proceso de Single Sign-Out.

Surge otro problema más, la compañía propietaria del sitio Web ejemplo-coches.com ha sido comprada por otra empresa que impone, como una de las cláusulas para efectuar la adquisición que el sitio Web ejemplo-coches.com deshaga la federación con el sitio ejemplo-vuelos.com. Se deberá llevar a cabo un **proceso de terminación indefinida de la federación** de las identidades de forma que ejemplo-vuelos.com no disponga de ningún pseudónimo para Juan para el dominio ejemplo-

coches.com y viceversa. Para ello, ejemplo-coches.com deberá llevar a cabo algún tipo de protocolo con el servicio Web de ejemplo-vuelos.com que se encargue de la terminación de forma que se desvinculen las identidades Web de los usuarios de ambos dominios.

Existen más posibilidades dentro del marco de la federación como es la **federación de los atributos** de los usuarios. Esta posibilidad podría mejorar cualitativamente la experiencia de los usuarios de la Web. Imaginemos que cuando Juan se registró en su momento en ejemplo-vuelos.com, tuvo que introducir su dirección postal. Imaginemos también que durante el proceso de registro que Juan efectúo en ejemplo-coches.com no le fue preguntado tal atributo. Durante el proceso de federación de las identidades, y después de que Juan se autentique en ejemplo-vuelos.com, le es preguntado si acepta compartir su dirección postal con el sitio ejemplo-coches.com a lo que responde afirmativamente.

Cierto día Juan se autentica en ejemplo-vuelos.com y, tras solicitar su deseo de alquilar un coche, es redirigido a la Web ejemplo-coches.com, llevándose a cabo el proceso SSO. Una vez alquila su coche, el sistema ejemplo-coches.com realiza una petición, como servicio Web cliente, al servicio Web que sirve los atributos de los usuarios de ejemplo-vuelos.com, solicitándole la dirección postal de Juan. Esta petición se realizará en nombre del pseudónimo con el que ejemplo-coches.com sabe que se tiene que referir a Juan en el contexto ejemplo-vuelos.com. El servicio de atributos de ejemplo-vuelos.com responde con dicho atributo y el sitio Web ejemplo-coches.com, al ver que el usuario pertenece a cierta zona geográfica, aplica una tarifa aún más barata que es comunicada al usuario a través de la Web.

El uso de los atributos puede ser tan trivial como el mencionado o podría ser utilizado por el **servicio de autorización** de ejemplo-coches.com. Imaginemos que Juan es menor de edad y que esta información, que él introdujo en ejemplo-vuelos.com, fue también federada en el momento de federar la dirección postal. Cuando Juan es redirigido a ejemplo-coches.com, el servicio de autorización de ejemplo-coches.com podría solicitar el atributo que representa la edad de Juan al servicio de atributos de ejemplo-vuelos.com y, al ver que es menor de edad, no permitirle realizar el alquiler del coche.

Por supuesto, para que esto sea válido, la fuente de los atributos de cierta identidad deberá haber contrastado su autenticidad. Por ejemplo, durante el proceso de registro de Juan en el sitio ejemplo-vuelos.com, y como un paso más, tuvo que personarse con su NIF en una delegación de ejemplo-vuelos.com.

Otro aspecto más sobre la federación de los atributos es que los dominios de confianza federados deberán acordar una nomenclatura y semántica común para los nombres de los atributos.

Por último señalar que para que todos estos protocolos se puedan seguir, cada sitio Web cooperante deberá distribuir cierta **meta-información de federación** a los otros sitios Web de la federación como por ejemplo: la ubicación donde solicitar la federación de la identidad, enviar las peticiones de los testigos que confirman la autenticación de cierto usuario, o enviar los mensajes de SLO. Esta meta-información puede ser intercambiada *off-line* entre los participantes, como por ejemplo durante la creación del marco legal, o bien puede ser descubierta de manera dinámica utilizando los mecanismos definidos en ciertas especificaciones como por ejemplo XACML [1], WS-Policy [3] o WS-MetadaExchange [5].

En este apartado hemos visto un caso práctico (que a decir verdad es poco realista aunque cumple con sus fines didácticos) en el que se mencionan los conceptos fundamentales de la federación entre sitios Web.

A continuación daremos un repaso a las especificaciones y los estándares que actualmente se relacionan con este tema.

3 Estándares y especificaciones

3.1 Passport de .NET

La tecnología Passport de Microsoft pretende ofrecer una serie de funciones sencillas a partir de una red distribuida y uniforme. La función más importante es la autenticación. Esta funcionalidad permite que cualquier usuario que posea una credencial Passport pueda acceder a un conjunto de sitios Web que son conformes con el esquema Passport. Es decir, un usuario se autentica ante el sistema Passport y obtiene unas credenciales en forma de cookie que le permiten navegar por diversos sitios Web sin la necesidad de tener que volver a autenticarse (es decir, ofrece una solución SSO). Para que un sitio Web permita credenciales Passport primero deberá establecer e intercambiar una clave secreta con el sistema Passport. Esta clave secreta, intercambiada off-line mediante un anexo en un correo electrónico seguro utilizando cifrado de clave pública, permitirá que la cookie que se otorgue a un usuario cuando se autentique en el sistema Passport se encuentre cifrada.

3.2 WS-Federation

Dentro del camino de la seguridad en el mundo de los servicios Web definido por IBM y Microsoft en su documento *Security in a Web Services World: A Proposed Architecture and Roadmap* [7] se encuentra la definición de una pila de protocolos que abarca cada uno de los aspectos de seguridad tratados (ver figura 4).

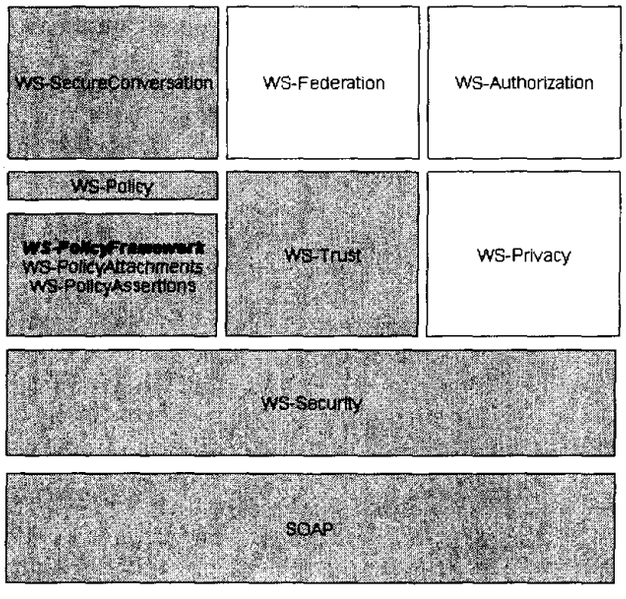

Fig. 4. Familia de especificaciones de seguridad de la familia WS-*.

De esta pila de especificaciones la única especificación que ya ha pasado por un organismo de estandarización, en este caso OASIS, es WS-Security. El resto se encuentran en estado de borrador. En la parte más alta de la pila nos encontramos con la especificación WS-Federation [4]. Esta especificación trata los aspectos señalados en el apartado 3 relativos con la federación aunque todavía se encuentra en una fase muy inicial de su desarrollo y, por tanto, no posee todavía carácter normativo (aunque se puede tomar como una declaración de intenciones del trabajo que se desarrollará en sus futuras versiones). Esta especificación se acompaña de dos perfiles que aplican los mecanismos que define en dos contextos: uno en el que los clientes de la federación son navegadores HTTP (denominados clientes pasivos) y otro en el que los clientes son servicios Web (clientes activos). WS-Federation define pues un modelo para construir, a partir de las especificaciones WS-* subyacentes, los siguientes mecanismos:

- Single Sign-On.
- Single Sign-Out.
- Intermediación de la confianza entre dominios.
- Servicio de atributos.
- Servicio de pseudónimos.

Como protocolo para realizar las comunicaciones entre los participantes de la federación se emplea aquel definido en la especificación WS-Trust.

3.3 Liberty Alliance Project

Este proyecto está compuesto por diversas organizaciones procedentes de diferentes sectores de la industria y su principal propósito es definir un marco general para la federación de las identidades en la Web. Tal y como se indica en el documento [10] el proyecto Liberty está desarrollando una serie de especificaciones que "habilitan la gestión de las identidades de red federadas". Su volumen de entregables es muy vasto, porque tal y como ellos mismos declaran su objetivo es "ambicioso" y necesita tener varios frentes abiertos al mismo tiempo. En terminología Liberty cualquier entidad (personal o computacional) que posee una identidad Web se denomina principal, mientras que el vínculo de confianza establecido entre los distintos proveedores de identidades y servicios se denomina círculo de confianza.

Con el objeto de organizarse dividen su esfuerzo en tres áreas:

Marco de Trabajo de Federación de las Identidades Liberty (ID-FF).

Este marco de trabajo ofrece un camino viable para implementar soluciones SSO mediante identidades federadas. Para ello define una serie de perfiles que abarcan las siguientes funcionalidades:

- SSO y Federación. Estos dos perfiles permiten que dos servicios federen sus identidades y puedan proporcionar SSO.
- Registro de nombres. En el caso de Liberty el protocolo de federación determina que quién inicialmente asigna un pseudónimo a la identidad sea el proveedor de identidades de forma que el proveedor del servicio se ve sujeto a utilizar este pseudónimo. Este perfil permite al proveedor de servicios solicitar a un proveedor de identidades de su círculo de confianza realizar un cambio de pseudónimo para cierta identidad federada de forma que se ajuste con la política aplicada por el proveedor de servicios en lo relativo a la asignación de identificadores de usuarios federados.
- Perfil de notificación de terminación de la federación. Este perfil define el protocolo que deben seguir las partes que forman parte del círculo de confianza que les permite finalizar de manera indefinida la federación sus identidades.
- Single Log-Out. Este perfil define el protocolo que se debe seguir por los proveedores de identidades y servicios a la hora de realizar Single Log-Out.
- Descubrimiento de un Proveedor de Identidad. Este perfil permite a un proveedor de servicios descubrir cuáles son los proveedores de identidades que un principal podría estar utilizando.
- Correlación de Identificadores de Nombres. Este perfil ofrece la posibilidad a un proveedor de servicios de obtener un identificador de nombre SAML con el cual se puede referir acerca de cierto principal de cara a una autoridad SAML determinada. Existe un perfil que además permite cifrar el valor de este identificador de nombre de forma que pueda cruzar sitios de terceras partes sin que estos puedan reconocerlo.

Marco de Trabajo de Servicios de Identidad Liberty (ID-WSF).

Define un marco de trabajo para crear, descubrir, y utilizar servicios de identidad. Básicamente se define un modelo conceptual que ofrece la terminología más importante para estos servicios de identidad. Un ejemplo de servicio proveedor de identidades que define es el servicio 'Discovery Service'.

Especificaciones de Interfaces de Servicios de Identidad Liberty (ID-SIS)
Este módulo define un conjunto de especificaciones que permite la creación de servicios interoperables basados en ID-WSF. Estos servicios, como por ejemplo servicios de agendas, de contactos, o de alertas, son interoperables gracias a la implementación que cada uno de ellos realiza de los protocolos Liberty.

3.4 Proyecto Shibboleth

El proyecto Shibboleth [9] es quizá el proyecto pionero en el mundo de la federación Web. Tal y como expresan en la especificación de su arquitectura, su propósito es el desarrollo de arquitecturas, marcos de trabajo, y tecnologías prácticas que permiten la compartición institucional de recursos que se encuentran sujetos a controles de acceso. Shibboleth define una arquitectura que permite el intercambio seguro de los atributos de privilegios (información de autorización de los sujetos) que pueden ser utilizados cuando se realizan decisiones de control de acceso.

Shibboleth trata de simplificar el proceso de administración de las identidades federadas entre instituciones cooperantes. En el marco de la administración federada, un proveedor de un recurso delega la administración de las identidades y los atributos de los usuarios al sitio original al que pertenecen. El proveedor de un recurso se apoya en el sitio de origen para obtener los atributos de los solicitantes y, de esta forma, poder realizar las decisiones de control de acceso oportunas.
Shibboleth es un sistema que permite la transferencia segura de atributos de un usuario desde su sitio de origen hasta el sitio al que pertenece el proveedor de los recursos. Shibboleth asume que el solicitante de los recursos está navegando utilizando un navegador HTTP común y los recursos están accesibles mediante tecnologías de Internet estándar.

Shibboleth tiene en cuenta el aspecto de la privacidad y permite que el usuario pueda escoger qué información (atributos) pueden ser revelados y a qué sitios. Ya que Shibboleth tiene en cuenta la privacidad, uno de sus componentes fundamentales es la entidad que libera los atributos de los usuarios. Esta entidad, conocida en la arquitectura Shibboleth, como la Autoridad de Atributos (AA) se encarga de almacenar y liberar, bajo las políticas de privacidad adecuadas, los atributos de los usuarios de un dominio de confianza.

Shibboleth no define por completo la implementación de una AA. Sin embargo, sí especifica una manera para que las AAs estructuren las políticas de revelación de los atributos. Cada dominio de confianza deberá proporcionar un servicio a través de su AA que permita a los usuarios definir las políticas de privacidad a aplicar sobre sus atributos.

Todas las interacciones entre los servicios Web, así como la información de seguridad intercambiada, que consiguen que el usuario navegue de manera transparente por los distintos sitios federados están diseñadas basadas en el estándar SAML. Así mismo, las políticas de control de acceso y privacidad están implementadas siguiendo el estándar XACML. No obstante, Shibboleth resulta ser lo suficientemente flexible como para admitir implementaciones que sigan otros estándares o especificaciones.

4 Conclusiones

Hoy por hoy la iniciativa con más solidez y experiencia en el campo de la federación de dominios de confianza mendiante servicios Web corre a cargo del Liberty Alliance Project que ya dispone de multitud de productos en el mercado basados en sus especificaciones.

El proyecto Shibboleth también representa una alternativa consistente y estándar (ya que está basada en los estándares SAML y XACML de OASIS) si se desea realizar la federación de organizaciones en la que los agentes participantes son humanos que emplean su navegador Web favorito para acceder a los servicios ofrecidos en los distintos sitios Web que forman parte de la federación.

Como vemos el tema de la federación Web está siendo objeto de un gran estudio y desarrollo por parte de los grandes de la industria tecnológica. Tal y como se puede apreciar tras leer el apartado 4, parece evidente que será necesario realizar un esfuerzo en paralelo que ofrezca soluciones de compatibilidad y convergencia entre las distintas soluciones ya que, como hemos visto, se encuentran hoy por hoy claramente solapadas en la aproximación que realizan sobre muchos de los aspectos que componen el concepto de federación.

Referencias

1. eXtensible Access Control Markup Language (XACML) Version 1.0. See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
2. Web Services Trust Language (WS-Trust) (2004). See ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf
3. Web Services Policy Framework (WS-Policy) (2004). See ftp://www6.software.ibm.com/software/developer/library/ws-policy.pdf
4. Web Services Federation Language (WS-Federation) (2003). See http://www-106.ibm.com/developerworks/webservices/library/ws-fed/
5. Web Services Metadata Exchange (WS-MetadataExchange) (2004). See http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-metadataexchange.pdf
6. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 (2003). See http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf
7. Security in a Web Services World: A Proposed Architecture and Roadmap (2002). See http://www-106.ibm.com/developerworks/webservices/library/ws-secmap/
8. Federation of Identities in a Web Services World (2003). See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/ws-federation-strategy.asp
9. Shibboleth-Architecture DRAFT v05 (2002). See http://shibboleth.internet2.edu/draft-internet2-shibboleth-arch-v05.html
10. Liberty Alliance Project. Introduction to the Liberty Alliance Identity Architecture (2003). See http://www.projectliberty.org/resources/whitepapers/LAP%20Identity%20Architecture%20Whitepaper%20Final.pdf
11. O'Neill, M., P. Hallam-Baker, S.M. Cann, M. Shema, E. Simon, P.A. Watters and A. White *Web Services Security*. McGraw-Hill. (2003)