(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 739**

(51) Int. CI.:

***G06F 21/62*** (2013.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.03.2012 PCT/EP2012/055281**

(87) Fecha y número de publicación internacional: **04.10.2012 WO12130782**

(96) Fecha de presentación y número de la solicitud europea: **26.03.2012 E 12713009 (4)**

(97) Fecha y número de publicación de la concesión europea: **27.11.2019 EP 2689372**

(54) Título: **Servicio de delegación de usuario a usuario en un entorno de gestión de identidad federada**

(30) Prioridad:

**25.03.2011 US 201161467646 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**14.07.2020**

(73) Titular/es:

**THALES DIS FRANCE SA (100.0%)**
**6, rue de la Verrerie**
**92190 Meudon, FR**

(72) Inventor/es:

**LU HONGQIAN, KAREN;**
**KRISHNA, KSHEERABDHI y**
**SACHDEVA, KAPIL**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Servicio de delegación de usuario a usuario en un entorno de gestión de identidad federada

**Campo de la invención**

La presente invención se refiere en general al servicio de delegación y más específicamente a un nuevo marco de delegación que soporta el servicio de delegación de usuario a usuario en un entorno de gestión de identidad federada.

**Antecedentes de la invención**

La delegación es el proceso de una entidad identificada, llamada delegante, que otorga un mandato o una afirmación de delegación a otra entidad identificada, llamada entidad delegada. La entidad delegada recibe el privilegio de actuar en nombre de la entidad que delega en un proveedor de servicios, que brinda servicios a un solicitante.

En esta memoria descriptiva, se ha utilizado la siguiente terminología:

- un privilegio es un derecho para acceder a recursos específicos o realizar ciertas tareas. Un usuario puede tener una cantidad de tales privilegios.

- una delegación es el acto de transferir temporal o permanentemente privilegios de una entidad a otra.

- una entidad que delega es la entidad que transfiere, es decir, delega todos o un subconjunto de sus privilegios a una Entidad delegada.

- una entidad delegada es la entidad que recibe todos o un subconjunto de los privilegios de la entidad que delega con el fin de utilizarlos en nombre de la entidad que delega.

- una afirmación de delegación es una afirmación de la corrección y autoridad para una delegación, emitida por una Autoridad de Delegación a una entidad delegada.

- una autoridad de delegación o autoridad de mandato es una entidad que controla la delegación y emite afirmaciones de delegación.

La delegación puede ser de usuario a usuario, de usuario a máquina, o de máquina a máquina. La investigación existente sobre la delegación en entornos de gestión de identidad federada se centra en las delegaciones de usuario a máquina o de máquina a máquina. La delegación de usuario a usuario ha sido estudiada en sistemas de control de acceso basado en roles (RBAC), y es utilizada típicamente con proveedores de servicios específicos. A medida que la Web se convierte en la computadora omnipresente, y más organizaciones, gobiernos, y empresas operan y dependen de entornos de gestión de identidad federada, la delegación de usuario a usuario en la web en tal entorno se convierte en una funcionalidad requerida. Además, la delegación también debería trabajar con diferentes modelos de control de acceso además de RBAC.

Los controles de acceso son mecanismos de seguridad que controlan cómo los sujetos, tales como los usuarios, las aplicaciones y los sistemas, acceden e interactúan con los objetos, tales como los recursos, otras aplicaciones y sistemas. El control de acceso incluye identificación, autenticación, autorización, y responsabilidad. Todas las organizaciones y sus sistemas o servicios deben tener políticas de control de acceso e implementaciones para proteger sus recursos y sistemas del acceso no autorizado.

La delegación es un mecanismo de transferencia de privilegios de acceso de un sujeto a otro. Tal transferencia de privilegios debe estar autorizada y no debe violar la política de control de acceso de la organización/sistema para impedir el acceso no autorizado debido a la delegación. Por lo tanto, la delegación debe ser especificada como parte de la política de control de acceso. Un mecanismo de delegación debe asociarse y estar autorizado por la máquina de control de acceso correspondiente. Sin embargo, las investigaciones recientes sobre delegación relacionadas con la identidad federada y las delegaciones de máquina a máquina se han centrado en los mecanismos y la semántica, pero no pudieron establecer el vínculo entre la delegación y el control de acceso.

Hay tres tipos principales de modelos de control de acceso: discrecional, obligatorio, y basado en roles. El modelo de control de acceso discrecional permite al propietario del recurso especificar qué sujeto puede acceder a un recurso específico. La mayoría de los sistemas operativos de los ordenadores personales, tales como Windows, Linux, Mac, tienen sus modelos basados en el control de acceso discrecional. En un modelo de control de acceso obligatorio, el sistema, no el propietario del recurso, toma decisiones basadas en un sistema de etiquetas de seguridad y un modelo matemático, con el que los datos son clasificados y los sujetos tienen etiquetas de autorización. En un control de acceso basado en roles, las decisiones de acceso se toman en función de un rol previamente especificado asignado al usuario. Esto es utilizado comúnmente en una empresa o una organización. Por ejemplo, un gerente puede acceder a ciertos recursos mientras que un empleado no puede. Un sistema también puede utilizar una combinación de estos modelos de control.

El Lenguaje de Marcado de Control de Acceso Extensible (XACML) es una especificación basada en estándares que

puede ser utilizada para especificar y comunicar políticas de control de acceso a través de sistemas informáticos, internos o externos a una organización. Una versión actual es XACML 2.0. Una versión XACML 3.0 está trabajando en progreso, lo que incluye el concepto y el proceso de delegación. Sin embargo, la delegación XACML se ocupa de la creación de nuevas políticas y del rastreo de "políticas confiables".

La delegación en el Control de Acceso Basado en Roles (RBAC) puede ser realizada para roles o para permisos individuales, otorgando o transfiriendo privilegios. La delegación otorgante permite que los privilegios delegados estén disponibles tanto para la entidad que delega como para la entidad delegada después de una operación de delegación exitosa. La delegación de transferencia transfiere los privilegios delegados a la entidad delegada después de una delegación exitosa. Esos privilegios ya no están disponibles para la entidad que delega. El sistema RBAC debe gestionar la delegación basándose en las políticas de control de acceso. Al hacerlo, debe responder las siguientes dos preguntas:

- ¿Está autorizada una entidad que delega para delegar un rol, privilegio o permiso que está disponible para él?

- ¿Se puede delegar un rol, privilegio o permiso a una entidad delegada?

En el contexto del servicio de delegación en un entorno de gestión de identidad federada, los proveedores de servicios gestionan sus propios controles de acceso y, por lo tanto, el permiso para delegar. El proveedor de servicios (SP) debe encontrar respuestas a la pregunta anterior cuando un usuario delega, cuando un usuario invoca una delegación, y cuando se han cambiado los privilegios de un usuario. Esto se aplica a cualquier modelo de control de acceso, no solo a RBAC.

El sistema llamado el Sistema Shibboleth es un paquete de software de código abierto basado en SAML 2.0 para un procedimiento de autenticación que habilita al usuario (SSO) a través o dentro de los límites de la organización. El Shibboleth propone una solución a un problema de autenticación de proxy: ¿cómo autenticar un servicio al que un usuario puede haberse autenticado, y quién desea invocar otro servicio en nombre del usuario? Por ejemplo, un usuario se autentica en un portal web a través de un proveedor de identidad (IdP), y luego el portal accede a un proveedor de servicios web como el usuario. Esta solución resuelve el problema de la delegación de usuario a máquina, es decir, el usuario delega algunos de sus privilegios en el portal web para acceder al proveedor de servicios en su nombre.

La solución Shibboleth usa dos SSO (Single Sign-On) a través del mismo IdP:

- Un SSO del navegador web al portal, es decir, inicio de sesión del usuario en el portal: una afirmación de SAML en respuesta a la solicitud de autenticación del IdP incluye un sujeto NameID y una confirmación de sujeto adicional para el portal que permite que el portal se utilice más tarde para autenticarse.

- Un Portal SSO para el SP: una afirmación SAML en respuesta a la solicitud de autenticación del IdP incluye el mismo sujeto NameID y la confirmación del sujeto que en la primera declaración de autenticación y una condición que tiene un elemento <Delegate> con el NameID como el portal.

La afirmación de delegación está habilitada por la primera declaración de autenticación y está integrada en la segunda declaración de autenticación. Por lo tanto, la afirmación de delegación es emitida y firmada por el IdP como se ha representado en la Figura 1.

Alrodhan y Mitchell también proponen un marco de delegación para el Proyecto Liberty Alliance, debido a la falta de soporte en las especificaciones Liberty. Sin embargo, este marco también está diseñado para la delegación de usuario a máquina. Extiende la declaración de atributo en la afirmación SAML para formar una afirmación de delegación. El IdP emite y firma la afirmación de delegación con el consentimiento del usuario, es decir, el consentimiento de la entidad que delega o del propietario del privilegio. Los perfiles del procedimiento de autenticación que habilita al usuario en la especificación Liberty ID-FF 1.2 proporcionan la base para este marco de delegación. Esta solución describió el marco basándose en tres perfiles: perfil de artefactos, perfil POST, y perfil de cliente habilitado. La función basada en el perfil del artefacto requiere un viaje de ida y vuelta adicional al IdP y la función basada en el perfil del cliente habilitado requiere la instalación de un cliente en el ordenador del usuario.

Este marco es similar a la delegación de Shibboleth en que la entidad delegada, a través del agente de usuario, obtiene una afirmación de delegación del IdP y luego la presenta al objetivo. Las diferencias incluyen utilizar de diferentes perfiles SSO, diferentes afirmaciones y diferentes formas de codificar la afirmación de delegación. Shibboleth utiliza la solicitud de Autenticación y una condición con el elemento <Delegate> mientras que el marco de delegación de Alrodhan y Mitchell utiliza una solicitud de afirmación general, y la declaración de atributo.

OAuth es un protocolo abierto que permite a los sitios web o aplicaciones llamadas Consumidores, acceder a recursos protegidos desde otro sitio web llamado Proveedor de Servicios, en nombre de un usuario, sin requerir que el usuario revele sus credenciales de inicio de sesión en el proveedor de servicios a los Consumidores. Como tal, OAuth proporciona un protocolo para la delegación de usuario a máquina, es decir, el usuario delega al consumidor para acceder a algunos de sus recursos en el Proveedor de Servicios. El protocolo OAuth tiene tres pasos:

- El Consumidor obtiene una Credencial de Solicitud no autorizada del Proveedor de Servicios, y redirige al usuario al Proveedor de Servicios.

- El usuario autoriza la Credencial de Solicitud en el Proveedor de Servicios, que redirige al usuario nuevamente al Consumidor después de la autorización.

- El consumidor intercambia la Credencia de Solicitud autorizada por una Credencial de Acceso, que es utilizada para acceder al recurso protegido en el Proveedor de Servicios en nombre del usuario.

OAuth es utilizado, por ejemplo, para que las aplicaciones web accedan a recursos específicos del usuario en sitios con la autorización del usuario sin revelar las credenciales de inicio de sesión del usuario. OAuth está diseñado para la delegación de usuario a máquina y no es adecuado para la delegación de usuario a usuario, ya que el usuario, es decir, la entidad delegada no puede procesar los mensajes de protocolo.

Las delegaciones existentes en los marcos de identidad federada se centran en la delegación de usuario a máquina. Esto permite que un proveedor de servicios A acceda a los recursos del usuario en el proveedor de servicios B en nombre del usuario.

Los métodos de delegación de usuario a máquina no pueden aplicarse a la delegación de usuario a usuario porque los humanos no pueden realizar operaciones criptográficas complejas.

El documento WO2009/027082 proporciona una solución de acuerdo con la cual un proveedor de servicios realiza una autenticación y un proveedor de identidad realiza la autorización. Alternativamente, una autenticación de la entidad delegada puede ser realizada en el proveedor de identidad sobre la base de credenciales de delegación y una autorización puede ser realizada en el proveedor de servicios.

Es entonces un objeto de la invención proporcionar un nuevo marco de delegación que admita el servicio de delegación de usuario a usuario en un entorno de gestión de identidad federada, proporcionando un servicio de delegación para que el SP individual no necesite gestionar delegaciones.

Para ello, la presente invención describe un método para proporcionar un servicio de delegación de usuario a usuario en un entorno de identidad federada, de acuerdo con la reivindicación 1.

De acuerdo con otro aspecto de la invención, el proveedor de identidad puede incorporar la afirmación de delegación elegida en la operación de autenticación y puede enviarla al proveedor de servicios.

De acuerdo con otro aspecto de la invención, la delegación puede ser una delegación simple, aplicable a un modelo de control de acceso discrecional, en donde la entidad que delega puede otorgar todos los privilegios a la entidad delegada durante un período de tiempo especificado.

De acuerdo con otro aspecto de la invención, una política de delegación puede estar en un metadato almacenado en el proveedor de servicios, aplicable a modelos de control de acceso discrecionales y basados en roles, en los que durante la operación de asignación, el proveedor de identidad puede verificar la política de delegación.

De acuerdo con otro aspecto de la invención, la delegación puede ser aplicable a cualquier modelo de control de acceso, en donde el proveedor de identidad puede pedirle al proveedor de servicios dinámicamente privilegios que la entidad que delega puede delegar a la entidad delegada.

De acuerdo otro aspecto de la invención, el método puede comprender una operación de revocación de delegación en la que el proveedor de identidad proporciona medios para que una entidad que delega revoque una delegación, dicha revocación está bajo la responsabilidad de la entidad que delega en el proveedor de identidad.

De acuerdo con otro aspecto de la invención, el método puede comprender una operación de revocación de delegación en la que el proveedor de identidad elimina la delegación a la entidad delegada por la entidad que delega de su registro.

De acuerdo con otro aspecto de la invención, la operación de revocación de delegación puede ser realizada por el proveedor de servicios en lugar de ser iniciada por la entidad que delega o por el proveedor de identidad.

De acuerdo con otro aspecto de la invención, el proveedor de identidad puede limpiar periódicamente su repositorio de delegación.

La invención también proporciona un sistema para proporcionar un servicio de delegación de usuario a usuario en un entorno de identidad federado. Este sistema puede comprender un proveedor de identidad, más de un proveedor de servicios, entidades que delegan, y entidades delegadas, en donde que el proveedor de identidad actúa como la autoridad de delegación, gestionando delegaciones para los proveedores de servicios.

La invención también proporciona una utilización de tal método para proporcionar un servicio de delegación de usuario a usuario en un entorno de identidad federada en dicho sistema.

Gracias a esta invención, la delegación permite que un usuario A delegue algunos de sus privilegios en un proveedor de servicios (SP) a un usuario B. El servicio de delegación incluye asignación de delegación, invocación de delegación, y revocación de delegación. El proveedor de identidad (IdP) actúa como la autoridad de delegación que gestiona las

delegaciones. La entidad que delegada asigna delegaciones en el IdP. La entidad delegada debe realizar las tareas delegadas en el proveedor de servicios (SP) especificado. El SP obtiene afirmaciones de delegación del IdP. Las delegaciones pueden ser revocadas tanto por la entidad que delega como por el SP.

Los modelos de control de acceso de los SP juegan un papel importante en el diseño de este marco de delegación. Los proveedores de servicios deben asegurarse de que las delegaciones no violen sus políticas de control de acceso. Con este propósito, el marco de delegación de acuerdo con la invención tiene mecanismos incorporados que permiten a los SP ejercer controles de acceso a lo largo de los ciclos de vida de las delegaciones. Estos mecanismos son ventajosamente independientes de los modelos de control de acceso de los SP.

El servicio de delegación es ventajosamente aplicable a cualquier modelo de control de acceso que utilicen los SP. La mayoría de los modelos de control de acceso, excepto algunas implementaciones de DAC, requieren que tanto la entidad que delega como la entidad delegada tengan cuentas con el sistema.

Los diferentes aspectos, características y ventajas de la invención serán más evidentes para los expertos en la técnica tras una cuidadosa consideración de la siguiente Descripción Detallada, proporcionada a modo de ejemplo de los mismos, con el dibujo adjunto descrito a continuación:

La Figura 1 muestra esquemáticamente un diagrama de flujo de acuerdo con la delegación Shibboleth;

La Figura 2 muestra esquemáticamente un diagrama de flujo de un ciclo de vida de delegación de acuerdo con la invención;

La Figura 3 muestra esquemáticamente un diagrama de flujo de una invocación de delegación de acuerdo con una realización de la invención;

La Figura 4 muestra esquemáticamente un diagrama de flujo de una asignación de delegación de acuerdo con una realización de la invención;

La Figura 5 muestra esquemáticamente un diagrama de flujo de una revocación por parte del proveedor de servicios de acuerdo con una realización de la invención.

**Descripción detallada**

La presente invención puede entenderse de acuerdo con la descripción detallada proporcionada en la presente memoria.

Como se ha explicado anteriormente, la delegación es un acto de transferencia de privilegios temporales o permanentes. Cuando una entidad que delega, delega en una entidad delegada, el IdP crea un registro de delegación, o llamada delegación, o simplemente delegación. El ciclo de vida de la delegación como se ha representado en la Figura 2, comienza con la creación y termina con la eliminación. Un registro de delegación incluye la entidad que delega, el proveedor de servicios (SP), la entidad delegada, los recursos a los que debe acceder la entidad delegada, las acciones que la entidad delegada puede realizar después de obtener el recurso, y otras cosas, tales como la fecha y hora de asignación, el período válido, la firma de la entidad que delegada, etc. Cuando la entidad que delega asigna una delegación, el proveedor de identidad (IdP) crea un registro de delegación; la delegación está en el estado creado. La invocación de la delegación por parte de la entidad delegada transfiere la delegación al estado aceptado.

Los proveedores de servicios (SP) en el mismo entorno, llamado círculo de confianza, pueden utilizar este servicio de delegación, en lugar de gestionar delegaciones individualmente. La delegación permite que un usuario A delegue algunos de sus privilegios en un proveedor de servicios (SP) a un usuario B. El servicio de delegación incluye asignación, invocación y revocación de delegación. El proveedor de identidad (IdP) actúa como la autoridad de delegación que gestiona las delegaciones. Los proveedores de servicios deben asegurarse de que las delegaciones no violen sus políticas de control de acceso. El marco de delegación brinda oportunidades para que los proveedores de servicios consulten sus máquinas de control de acceso para decidir si la entidad delegada debe estar autorizada para realizar los servicios solicitados. Por lo tanto, el marco no está vinculado a ningún modelo de control de acceso en particular.

La presente invención proporciona diferentes realizaciones, que permiten a los proveedores de servicios ejercer diferentes tipos de control de acceso y gestionar las complejidades de utilizar la delegación en consecuencia. Un proveedor de servicios especifica si permite la delegación, y si lo hace, qué opción de delegación admite, todo dentro de un metadato. La configuración predeterminada en los metadatos es "sin delegación".

Las interacciones entre los SP y el IdP siguen los estándares SAML 2.0 y XACML.

En una primera realización, los proveedores de servicios no realizan cambios o hacen cambios mínimos para utilizar el mecanismo de delegación proporcionado por el proveedor de identidad. Esta realización solo es aplicable al control de acceso discrecional y la entidad que delega otorga todos los privilegios en el proveedor de servicios a la entidad delegada durante un período de tiempo especificado.

En esta primera realización en la que los cambios de SP no son necesarios, una entidad que delega, delega siempre todos sus privilegios a una entidad delegada en un proveedor de servicios, es decir, la entidad que delega permite que le

entidad delegada inicie sesión en el proveedor de servicios como la entidad que delega. Por ejemplo, la entidad que delega puede dar sus credenciales de inicio de sesión, tales como nombre de usuario/contraseña o tarjeta inteligente/PIN, a la entidad delegada en el SP.

En una Asignación de delegación, el método comprende las siguientes operaciones: la entidad que delega se autentica en el IdP, especifica la entidad delegada, selecciona el SP al que desea que acceda la entidad delegada y especifica otras restricciones, tales como el período de validación. El IdP crea una delegación. La entidad que delega o el IdP informa a la entidad delegada acerca de la delegación.

En una Invocación de delegación, el método comprende las siguientes operaciones: la entidad delegada inicia sesión en el SP, que es redirigido al IdP. Al encontrar una delegación, el IdP pregunta si el usuario desea iniciar sesión como él mismo o como la entidad que delega. Si la entidad delegada selecciona a la entidad que delega, el IdP autentica al usuario y genera una afirmación de autenticación para la entidad que delega. Esto permite que la entidad delegada inicie sesión en el SP como la entidad que delega.

Este modelo es ventajosamente simple ya que no requiere cambios en los SP y permite la delegación anónima.

El IdP especifica la información de la entidad delegada de manera consultiva. El SP tiene la opción de procesar la información de la entidad delegada. Una forma de implementar esto es utilizar un <saml: SubjectConfirmation> adicional en la afirmación de que el IdP envía al SP como respuesta a la solicitud de autenticación. Un fragmento de código SAML 2.0 que ilustra una afirmación con la información de delegación es, por ejemplo:

```
<Assertion>
    <Issuer> … URI of the IdP … </Issuer>
    <ds:Signature> … IdP's signature … </ds:Signature>
    <Subject>
    <NameID> … URI of the delegator … <NameID>
    <SubjectConfirmation> // about the delegator
    <SubjectConfirmation Method="sender-vouches>
        <SubjectConfirmationData> // about the delegatee
    </SubjectConfirmation>
    </Subject>
    <Conditions>
    <AuthnStatement>
</Assertion>
```

Alternativamente, la información de la entidad delegada puede ser expresada en una declaración de atributo dentro de la afirmación. Un fragmento de código SAML 2.0 que ilustra una afirmación con la información de delegación es, por ejemplo:

```
<Assertion>
    <Issuer> ... URI of the IdP ... </Issuer>
    <ds:Signature> ... IdP's signature ... </ds : Signature>
    <Subject> ... Information about the delegator ... </Subject>
    <Conditions>
    <AuthnStatement>
    <AttributeStatement>
       <Attribute Name="Delegation">
           <AttributeValue>
               <Delegator>
               <Delegatee>
               ... other attribute values such as assignment time, valid period, and
               delegator signature ...
           </AttributeValue>
       </Attribute>
    </AttributeStatement>
</Assertion>
```

El proveedor de servicios tiene la opción de procesar la información de la delegación, decidir si proporciona o no servicios a la entidad delegada y registrar la delegación con propósitos de auditoría.

En una revocación de delegación, el IdP proporciona medios para que una entidad que delega revoque una delegación.

Es responsabilidad de la entidad que delega revocar la delegación en el IdP.

En una segunda realización, el proveedor de servicios puede expresar su política de delegación o un subconjunto de la política dentro de los metadatos. Esta realización es aplicable al control de acceso discrecional o al control de acceso simple basado en roles, con el cual el proveedor de servicios puede expresar las políticas de delegación sin especificar usuarios individuales. La entidad que delega puede especificar ventajosamente los privilegios que desea delegar. Los proveedores de servicios describen sus políticas de delegación utilizando XACML. Por ejemplo, el siguiente fragmento de código XACML 3.0 ilustra una política de delegación en donde el SP es un comerciante en línea, cuya política de delegación dice que cualquier usuario que tenga una cuenta en el SP puede delegar el seguimiento del pedido y el seguimiento del punto de adjudicación a cualquier persona que pueda ser autenticada por el IdP. La entidad delegada no necesariamente tiene una cuenta en el SP.

```
<Policy>
    <Description>
       Simple merchant delegation policy
    </Description>
    <Target> // <AnyOf>, <AllOf> are omitted for simplicity
       <Match>
          <AttributeValue> User Of IdP </AttributeValue>
          <AttributeDesignator Category="urn.oasis:names.tc:xacml:3.0:attribute-
category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:access-
subject">
       </Match>
       <Match>
          <AttributeValue> OrderInfo </AttributeValue>
          <AttributeDesignator Category="urn.oasis:names.tc:xacml:3.0:attribute-
category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:resource">
       </Match>
       <Match>
          <AttributeValue> AwardPoints </AttributeValue>
          <AttributeDesignator Category="urn.oasis:names.tc:xacml:3.0:attribute-
category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:resource">
       </Match>
       <Match>
          <AttributeValue> View </AttributeValue>
          <AttributeDesignator Category="urn.oasis:names.tc:xacml:3.0:attribute-
category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:action">
       </Match>
       <Match>
          <AttributeValue> User of this SP </AttributeValue>
          <AttributeDesignator
             Category="urn.oasis:names.tc:xacml:3.0:attribute-
category:delegate"/>
       </Match>
    </Target>
    <Rule RuleId="Rule1" Effect="Permit">
       <Target/>
    </Rule>
</Policy>
```

La Asignación de delegación comprende las siguientes operaciones en donde la entidad que delega primero se autentica en el IdP. Luego, la entidad que delega selecciona el SP en el que quiere delegar algunas tareas. El IdP lee la política de delegación en los metadatos del SP y presenta recursos y acciones delegables, si los hay, a la entidad que delega. La entidad que delega especifica a la entidad delegada, las tareas, es decir, los recursos y las acciones, y otras restricciones, tales como un período de validación. El IdP crea una delegación. El IdP también puede pedirle a la entidad que delega que firme digitalmente la delegación para no repudiar. Luego, la entidad que delega firma la delegación si es necesario. La entidad que delega o el IdP informa a la entidad delegada acerca de la delegación.

Cuando la entidad delegada solicita realizar una tarea delegada en el SP, invoca una delegación.

En la invocación de delegación, como se ha mostrado en la Figura 3, el método comprende las siguientes operaciones: la entidad delegada inicia sesión en el SP, que es redirigido al IdP. El IdP luego verifica la identidad de la entidad delegada. El IdP encuentra delegación(es) para la entidad delegada en el SP y le pregunta si quiere iniciar sesión como ella misma o como entidad delegada y para qué entidad que delega. La entidad delegada luego selecciona el inicio de sesión como una entidad delegada y especifica la entidad que delega. El IdP genera una afirmación de autenticación para la entidad delegada con una declaración de atributo de delegación que especifica la entidad que delega, los privilegios, y otras restricciones. El IdP luego envía la afirmación de autenticación al SP. El SP verifica la afirmación de autenticación y la declaración de delegación y consulta con su máquina de control de acceso tanto para la entidad que delega como para la entidad delegada. Si todo está bien, el SP presenta servicios para permitir que la entidad delegada realice las tareas delegadas.

El IdP genera una afirmación de autenticación en respuesta a la solicitud de autenticación del SP. El sujeto de la afirmación es la entidad delegada. La afirmación además incluye una declaración de atributo acerca de la delegación y un fragmento de código que ilustra la aserción es, por ejemplo:

```
<Assertion>
   <Issuer> ... URI of the IdP ... </Issuer>
   <ds:Signature> ... IdP's signature ... </ds : Signature>
   <Subject> ... Information about the delegatee ... </Subject>
   <Conditions>
   <AuthnStatement>
   <AttributeStatement>
      <Attribute Name="Delegation">
         <AttributeValue>
             <Delegator>
             <Delegatee>
             <Privilege>
                <Description> <Service> <Resource> <Action> ...
             </Privilege>
             ... other attribute values such as assignment time, valid period, and
             delegator signature ...
         </AttributeValue>
      </Attribute>
   </AttributeStatement>
</Assertion>
```

El SP debe procesar la información de la delegación, verificar la declaración de delegación, y consultar con su máquina de control de acceso para decidir si debe proporcionar los servicios solicitados. Específicamente, el SP verifica las siguientes operaciones:

- la delegación está en el período de validez.

- la solicitud de servicio está especificada en la declaración.

- el solicitante es la entidad delegada especificada en la declaración.

- la firma de la afirmación es válida y el certificado no es revocado.

- la entidad que delega está autorizada para realizar la tarea privilegiada delegada.

- la entidad que delega está autorizada para delegar la tarea privilegiada.

- la entidad delegada tiene el privilegio de realizar la tarea delegada.

Se entenderá que se pueden cumplir otras restricciones opcionales

La verificación de las autorizaciones es necesaria porque las condiciones pueden haber cambiado desde la última vez que el SP consultó a la máquina de control de acceso en relación a la entidad que delega y a la entidad delegada cuando el IdP solicitó la lista de privilegios para configurar la delegación.

En la revocación de la delegación, el IdP proporciona los medios para que una entidad que delega revoque una delegación. Es responsabilidad de la entidad delegada revocar la delegación en el IdP.

En una tercera realización, el método es independiente del mecanismo de control de acceso que tiene un proveedor de servicios. Un proveedor de servicios puede elegir esta opción si tiene un control de acceso basado en roles más complejo, un control de acceso obligatorio, o cualquier control de acceso que sea demasiado complejo o demasiado sensible para ser expresado en los metadatos con el IdP. Por ejemplo, las políticas de control de acceso de un SP pueden vincularse con individuos y almacenarse en una base de datos. En estos casos, la entidad que delega sabe lo que puede delegar, o la entidad que delega o el IdP deben preguntarle al proveedor de servicios qué puede delegar. El SP debe consultar a su máquina de control de acceso con el fin de proporcionar la lista.

Para la asignación de delegación, una entidad que delega quiere delegar algunas tareas a una entidad delegada, para que sean realizadas en un SP. El IdP no sabe qué privilegios puede delegar a la entidad que delega. La función del IdP es gestionar la delegación y decirle al SP que la entidad que delega, en efecto, ha delegado ciertos privilegios a la entidad delegada. El SP debe ejercer el control de acceso, es decir, para asegurar que la entidad que delega tenga y pueda delegar estos privilegios y que la entidad delegada esté autorizada para realizar las tareas.

Para hacerlo, la entidad que delega especifica el SP, a la entidad delegada, y los privilegios, es decir, los recursos y las acciones que desea delegar. El IdP crea una delegación. Esta realización supone que la entidad que delega sabe exactamente lo que puede delegar.

En una variante, el IdP le pregunta al SP si tal delegación puede ser autorizada. Esto puede ser realizado, por ejemplo, si el IdP realiza un <xacml- samlp: XACMLAuthzDecisionQuery>, que se especifica en el perfil XACML SAML, al SP. Si el SP responde con éxito, el IdP crea una delegación. De lo contrario, el IdP le pide a la entidad que delega que realice una modificación y repita el proceso. Esta variante supone que la entidad que delega probablemente sepa lo que puede delegar.

En una variante adicional de esta tercera realización, la entidad que delega especifica el SP y la entidad delegada. El IdP le pregunta al SP acerca de los privilegios que la entidad que delega puede delegar a la entidad delegada. El SP responde con una lista, que puede estar vacía. El IdP le pide a la entidad que delega que haga una selección. Cuando es necesario, el IdP le pregunta al SP si tal delegación puede ser autorizada. Si el SP responde con éxito, el IdP crea una delegación. La consulta de privilegios es implementada, por ejemplo, utilizando <xacml-samlp: XACMLPolicyQuery>. Esta variante adicional no hace suposiciones acerca de si la entidad que delega sabe lo que puede delegar. Para hacerlo, la asignación de delegación comprende, por ejemplo, las siguientes operaciones como se ha representado en la Figura 4:

- la entidad A que delega se autentica en el IdP.

- la entidad A que delega selecciona el SP al que quiere que acceda la entidad delegada B.

- el IdP encuentra a partir del SP los privilegios que la entidad A que delega puede delegar a la entidad delegada B.

- el IdP presenta una lista que contiene esos privilegios, es decir, recursos y acciones para la entidad que delega A.

- la entidad A que delega selecciona privilegios para delegar a la entidad delegada B de la lista y otras restricciones, tales como un período de tiempo válido.

- el IdP crea una delegación. Opcionalmente, el IdP le pregunta al SP si tal delegación puede ser autorizada antes de crear una delegación.

- el IdP puede pedirle a le entidad que delega que firme digitalmente la delegación para no repudiar.

- la entidad que delega firma la delegación si es necesario.

- la entidad que delega o el IdP informan a la entidad delegada acerca de la delegación.

La diferencia entre estas operaciones de esta tercera realización y la segunda realización es que en la segunda realización, el IdP encuentra lo que la entidad que delega puede delegar de los metadatos del SP, mientras que en la tercera realización, el IdP le pregunta al SP qué puede delegar a la entidad que delega.

En esta tercera realización, la Invocación de delegación comprende las mismas operaciones que la Invocación de delegación de la segunda realización.

Como se ha descrito anteriormente, el IdP es la autoridad de delegación que gestiona las afirmaciones de delegación. El SP obtiene la declaración de delegación del IdP como parte de la afirmación de autenticación. El SP no recibe la afirmación de delegación de nadie más. El SP puede almacenar la afirmación de delegación con propósitos de auditoría, pero no lo hace para su reutilización. La afirmación de delegación siempre es adquirida dinámicamente. Por lo tanto, el SP no necesita verificar el estado de la delegación.

Una revocación de delegación puede ser iniciada por la entidad que delega o por el SP. Después de recibir una solicitud de revocación, el IdP autentica y verifica la solicitud. Si la solicitud es auténtica y verificable, el IdP elimina la delegación de solicitud de su lista de delegaciones o base de datos, en lugar de crear una lista separada.

La situación de la delegación es muy diferente de la del certificado SSL. El SP recibe un certificado SSL de un tercero. Antes de utilizarlo, el SP verifica si el certificado sigue siendo válido consultando con la Lista de Revocación de Certificados (CRL) que contiene una lista de certificados revocados, o utilizando un servicio de Protocolo de Estado de Certificado Abierto (OCSP) que proporciona el estado de revocación de un certificado. El SP obtiene la afirmación de delegación de la autoridad de delegación, que es el IdP. El SP puede verificar la afirmación por sí mismo y no necesita verificar con el IdP la validez de la afirmación, y el IdP no necesita mantener una lista o proporciona un servicio para tal propósito.

En esta tercera realización, cuando la entidad que delega, por ejemplo, revoca una delegación en el proveedor de identidad que gestiona las delegaciones, el método comprende las siguientes operaciones:

- la entidad A que delega inicia sesión en el IdP.

- la entidad A que delega revoca su delegación a la entidad delegada B.

- el IdP retira la delegación a la entidad delegada B por la entidad A que delega de su registro. Por lo tanto, cuando la entidad delegada B se autentica en el IdP, no tendrá la opción de actuar como entidad delegada para la entidad A que delega.

Como se ha mostrado en la Figura 5, la revocación en otra realización es realizada por el SP en lugar de ser iniciada por la entidad que delega o por el IdP. Cuando se reducen o eliminan los privilegios de un usuario, el proveedor de servicios debe averiguar si hay delegaciones pendientes relevantes para este usuario. De ser así, el SP debe examinar cada una de las delegaciones para ver si aún son válidas. Si el usuario era una entidad que delega y ya no tiene el privilegio de delegar la tarea, o si el usuario era una entidad delegada y ya no tiene el privilegio de realizar la tarea delegada, entonces el SP envía una solicitud de revocación al IdP para revocar la delegación. El IdP luego informa a la entidad que delega y a la entidad delegada.

Alternativamente a la revocación por parte del SP y la revocación por parte de la entidad que delega, el IdP limpia periódicamente su repositorio de delegación. Para las delegaciones que no han sido activadas durante un tiempo o solo para alguna delegación, el IdP realiza una consulta de decisión de autorización XACML al SP. Si la respuesta es negativa, el IdP retira la delegación. Esto evita la utilización de la extensión SAML para la revocación de delegación.

La delegación de revocación de esta tercera realización ventajosamente no requiere mantener una lista de revocaciones ni una consulta separada sobre el estado de la delegación.

Una vez que la entidad delegada es informada de la asignación de la delegación, ya sea por la entidad que delega o por el proveedor de identidad, la entidad delegada examina la delegación, por ejemplo, a partir de la información recibida o el IdP proporciona un servicio para que la entidad delegada lo haga. La solicitud al SP por parte de la entidad delegada para realizar las tareas delegadas es una forma de aceptación de la delegación. El IdP también puede proporcionar un servicio para que la entidad delegada acepte explícitamente la delegación.

Si la entidad delegada rechaza la delegación, informa a la entidad que delega, quien modifica la delegación o revoca la delegación en el IdP. El IdP también puede proporcionar un servicio para que la entidad delegada rechace una delegación. La revocación de la aceptación puede ser realizada igual que el rechazo.

De acuerdo con la invención, la asignación de delegación, la consulta, la invocación, y la revocación requieren comunicaciones entre el SP y el IdP. Como se ha descrito anteriormente, las afirmaciones de SAML 2.0 son utilizadas como formato de intercambio de mensajes y extendidas según sea necesario. Los protocolos y enlaces SAML son utilizados para transportar los mensajes de delegación.

El protocolo SAML es un protocolo de solicitud y respuesta. El solicitante envía una solicitud, y el respondedor procesa la solicitud y envía una respuesta. El estándar SAML 2.0 es utilizado para formatear la solicitud y la respuesta de delegación.

La consulta de atributo SAML 2.0 <AttributeQuery> es utilizada para consultar atributos para el sujeto. La <AttributeQuery> es de AttributeQueryType, que extiende SubjectQueryAbstractType. <AttributeQuery> es utilizada para consultar los privilegios que la entidad que delega puede delegar a la entidad delegada, y las delegaciones existentes para una entidad que delega o entidad delegada. La respuesta a la <AttributeQuery> es una afirmación de atributo o un estado de consulta.

En la variante adicional de la tercera realización, cuando la entidad que delega especifica el SP y la entidad delegada, el IdP le pregunta al SP qué privilegios puede delegar la entidad que delega a la entidad delegada. Esto es realizado, por ejemplo, utilizando la consulta de política XACML <xacml-samlp: XACMLPolicyQuery> especificada en el perfil XACML SAML. Un fragmento de código que ilustra la consulta es, por ejemplo:

```
<xacml-samlp:XACMLPolicyQuery>
  <saml:Issuer>
  <ds:Signature>
  <Attribute ID>
  <Attribute IssurInstant>
  ... ...
  <xacml-context:Request>
   <xacml:Attributes>
      <Attribute name="user">
         <AttributeValue> name or id of the delegator </AttributeValue>
      </Attribute>
      <Category
         name="urn.oasis:names.tc:xacml: 3.0:attribute-category:delegate">
   </Attributes>
   <xacml:Attributes>
      <Attribute name="user">
         <AttributeValue> name or id of delegatee </AttributeValue>
      </Attribute>
      <Category name="urn.oasis:names.tc:xacml:3.0:attribute-
      category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:access-
      subject">
   </Attributes>
   <xacml:Attributes>
      <Category
         name="urn.oasis:names.tc:xacml: 3.0:attribute-category: delegate">
      <Category name="urn.oasis:names.tc:xacml:3.0:attribute-
      category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:resource">
      <Category name-"urn.oasis:names.tc:xacml:3.0:attribute-
      category:delegated:urn:oasis:names:tc:xacml:3.0:subject-category:action">
   </Attributes>
  </Request>
  <Attribute name="ReturnPolicyIdList">
   <AttributeValue>true</AttributeValue>
</Attribute>
... ...
</XACMLPolicyQuery>
```

En respuesta, el SP envía un <samlp: Response>, que contiene una afirmación XACMLPolicy que tiene una declaración del tipo xacml-saml: XACMLPolicyStatementType. Esta declaración contiene políticas que la consulta solicitó.

Cuando los privilegios de un usuario han sido retirados o reducidos, el SP examina todas las delegaciones pendientes asociadas con este usuario, ya sea como una entidad que delega o como una entidad delegada. Con este propósito, el SP envía una solicitud de consulta al IdP y el IdP responde con una afirmación de atributo que contiene declaraciones de delegación relevantes, si existen. Un fragmento de código que ilustra la consulta es, por ejemplo.

```
<samlp:AttributeQuery>
<saml:Issuer>
<ds:Signature>
<Attribute ID>
<Attribute IssurInstant>
... ...
<Subject>
   <NamdID id=... delegator or delegatee's id...>
   ... ...
</Subject>
<Attribute name="Delegation">
</AttributeQuery>
```

El IdP responde con una afirmación que contiene una o más declaraciones de atributos acerca de las delegaciones.

La solicitud de autenticación es el estándar SAML 2.0 <AuthnRequest>. Cuando se envía una solicitud de autenticación, el SP no sabe nada acerca de la delegación. La entidad delegada solicita realizar tareas de delegación en el IdP durante la autenticación o en el SP después de la autenticación.

Cuando los privilegios de acceso de un privilegio principal han cambiado y las delegaciones existentes ya no son válidas, el SP envía una solicitud de revocación de delegación al IdP para revocar las delegaciones relevantes. Si bien ni SAML 2.0 ni XACML 2.0/3.0 especificaron la revocación, la sintaxis de SAML es utilizada para definirla. La solicitud y la respuesta de revocación de delegación son similares a la solicitud y respuesta de autenticación, en la que el SP envía una solicitud al IdP. El IdP cumple con la solicitud y envía una afirmación en respuesta. Una solicitud es, por ejemplo:

```
<DelegationRevokeRequest>
<Issuer>
<ds:Signature>
... ...
<Subject>
<Attribute name="Delegation">
   <Delegator>, <Delegatee>, <Resource>, etc.
</Attribute>
 ... ...
 </DelegationRevokeRequest>
```

Los elementos en <Delegation> son opcionales. La solicitud tiene las siguientes reglas:

- Si ningún <Resource> es especificado, el SP solicita revocar todas las delegaciones asociadas con <Delegator>, <Delegatee>, o ambos.

- Si ninguno de <Delegator> y <Delegatee> existe, el SP solicita revocar todas las delegaciones asociadas con el sujeto y <Resource>.

- Si hay <Delegator> pero no <Delegatee>, el SP solicita revocar a todas las delegaciones en las que el sujeto es una entidad que delega y delegar <Resource> a cualquier entidad delegada.

- Si hay <Delegatee> pero no <Delegator>, el SP solicita revocar a todas las delegaciones en las que el sujeto es una entidad delegada y fue delegado para <Resource> por cualquier entidad que delega.

- Si hay <Delegator> y <Delegatee>, el SP solicita revocar todas las delegaciones asociadas a <Delegator>, <Delegatee> y <Resource>. El sujeto es una entidad que delega o una entidad delegada.

La respuesta del IdP contiene el estado de la revocación.

Se entenderá que el SP también puede elegir una combinación de la segunda y tercera realizaciones.

De acuerdo con la invención, la comunicación entre SP e IdP debe ser asegurada mediante SSL/TLS y conjuntos de cifrado fuertes. La declaración de delegación debe estar firmada por el proveedor de identidad que gestiona las delegaciones.

Todas las consultas y solicitudes entre el IdP y los proveedores de servicios deben estar firmadas por el solicitante para proporcionar autenticidad y no repudio. Todas las respuestas a consultas y solicitudes entre IdP y proveedores de

servicios deben estar firmadas por el respondedor para proporcionar autenticidad y no repudio. El SP no debe reutilizar la declaración de delegación.

Los proveedores de servicios que eligen utilizar la primera realización sin procesar la parte de delegación de la afirmación de autenticación deben comprender que el usuario puede no ser el que el proveedor de servicios piensa. La entidad delegada puede haber iniciado sesión en nombre de la entidad que delega. Esta realización solo debería ser utilizada por proveedores de servicios que no tengan información confidencial o privada de los usuarios y para quienes la seguridad no sea una preocupación.

Los proveedores de servicios que elijan utilizar la primera realización deberían procesar la parte de delegación de la afirmación de autenticación para comprender quién ha iniciado sesión realmente, consultar a su máquina de control de acceso para decidir si la entidad delegada debería estar autorizada para recibir los servicios solicitados, y registrar la transacción.

La declaración de delegación en la afirmación de autenticación proporcionada por el IdP no es una autorización de delegación. En cambio, el IdP garantiza que la entidad que delega, en efecto, ha delegado algunas tareas a la entidad delegada. Es responsabilidad del proveedor de servicios consultar a su máquina de control de acceso para decidir si la entidad delegada debería estar autorizada para recibir los servicios solicitados, y registrar la transacción.

La entidad delegada debe tener una cuenta en el IdP. De lo contrario, el IdP no puede identificar y autenticar a la entidad delegada.

Las políticas de control de acceso de los proveedores de servicios dictan si la entidad delegada debe tener una cuenta en sus sitios web.

Gracias a la invención, la entidad que delega puede firmar digitalmente la delegación (mandato) proporcionando no repudio. El Proveedor de Identidad gestiona las delegaciones de todos los proveedores de servicios que se han registrado con el IdP y expresaron el permiso y las políticas de delegación en sus metadatos. Los protocolos estándar son utilizados entre IdP y SP, como SSL/TLS, SAML y SACML. Los proveedores de servicios tienen que autorizar cualquier delegación. El IdP puede obtener autorización de los proveedores de servicios antes de crear mandatos. El no repudio es proporcionado mediante firma digital. La entidad que delega puede especificar restricciones, tales como un período válido.

**REIVINDICACIONES**

1. Método para proporcionar un servicio de delegación de usuario a usuario en un entorno de identidad federada, que comprende:

- asignar, en un proveedor de identidad (IdP), una asignación de delegación de un primer usuario, entidad que delega, especificando la asignación de delegación un proveedor de servicios, privilegios o tareas que han de ser realizadas en el proveedor de servicios (sP), y un segundo usuario, entidad delegada,

- operar el proveedor de identidad (IdP) para autenticar el segundo usuario, la entidad delegada, si la operación de autenticación es exitosa y si el proveedor de identidad encuentra delegaciones para el segundo usuario, la entidad delegada, proporcionar al segundo usuario, la entidad delegada, un mecanismo a partir del cual elegir qué delegación realizar, a partir del cual elegir qué delegación realizar, e incorporar, mediante el proveedor de identidad (IdP), una afirmación de delegación correspondiente a la selección de delegación en la operación de autenticación y enviar la afirmación de delegación al proveedor de servicio (sP),

- en respuesta a la recepción de la selección de delegación del segundo usuario, la entidad delegada, operar el proveedor de servicios (sP) para autorizar las delegaciones; y

- asociar una operación de invocación de delegación con una operación de autenticación de usuario mediante:

i. recibir una solicitud de inicio de sesión del segundo usuario, la entidad delegada, en el proveedor de servicios (sP), y

ii. operar el proveedor de servicios (sP) para delegar la autenticación del segundo usuario, la entidad delegada, al proveedor de identidad (IdP).

2. El método según la reivindicación 1, caracterizado porque el proveedor de servicios autoriza delegaciones basándose en las reglas de control de acceso.

3. El método según cualquiera de las reivindicaciones precedentes, caracterizado porque la delegación es una delegación simple, aplicable a un modelo de control de acceso discrecional, en donde la entidad que delega otorga todos los privilegios a la entidad delegada durante un período de tiempo especificado.

4. El método según las reivindicaciones 1 a 3, caracterizado porque una política de delegación está en un metadato almacenado en el proveedor de servicios, aplicable a modelos de control de acceso discrecionales y basados en roles, en donde el proveedor de identidad verifica la política de delegación.

5. El método según las reivindicaciones 1 a 3, caracterizado porque la delegación es aplicable a cualquier modelo de control de acceso, en donde el proveedor de identidad le pide al proveedor de servicios dinámicamente los privilegios que la entidad que delega puede delegar a la entidad delegada.

6. El método según las reivindicaciones 4 o 5, caracterizado porque comprende una operación de revocación de delegación en donde el proveedor de identidad proporciona medios para que una entidad que delega revoque una delegación, estando dicha revocación bajo la responsabilidad de la entidad que delega en el proveedor de identidad.

7. El método según la reivindicación 5, caracterizado porque comprende una operación de revocación de delegación en donde el proveedor de identidad retira la delegación a la entidad delegada por la entidad que delega de su registro.

8. El método según la reivindicación 6, caracterizado porque la operación de revocación de delegación es realizada por el proveedor de servicios en lugar de ser iniciada por la entidad que delega o por el proveedor de identidad.

9. El método según la reivindicación 7, caracterizado porque el proveedor de identidad limpia periódicamente su repositorio de delegación.

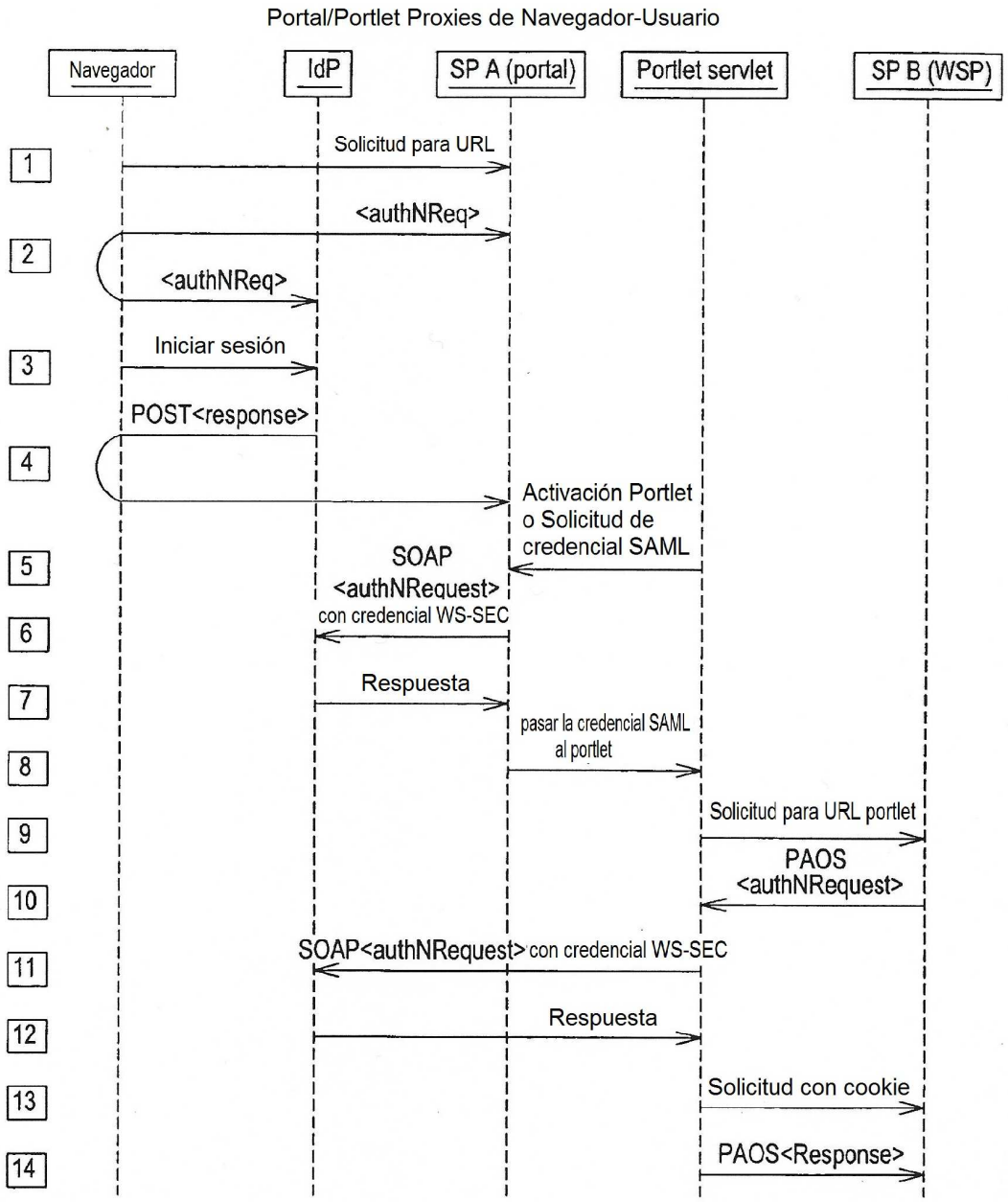
Portal/Portlet Proxies de Navegador-Usuario
Navegador
IdP
SP A (portal)
Portlet servlet
SP B (WSP)
1
Solicitud para URL
2
<authNReq>
<authNReq>
3
Iniciar sesión
4
POST<response>
Activación Portlet
o Solicitud de
credencial SAML
5
SOAP
<authNRequest>
con credencial WS-SEC
6
7
Respuesta
8
pasar la credencial SAML
al portlet
9
Solicitud para URL portlet
10
PAOS
<authNRequest>
11
SOAP<authNRequest> con credencial WS-SEC
12
Respuesta
13
Solicitud con cookie
14
PAOS<Response>

**Fig. 1**

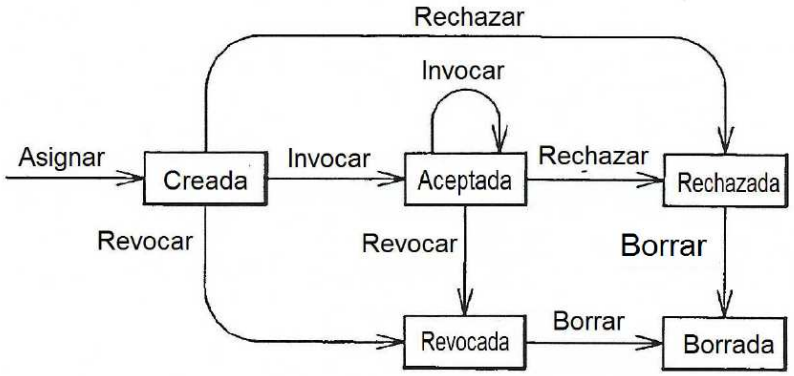
Rechazar
Invocar
Asignar
Creada
Invocar
Aceptada
Rechazar
Rechazada
Revocar
Revocar
Borrar
Revocada
Borrar
Borrada

Fig. 2

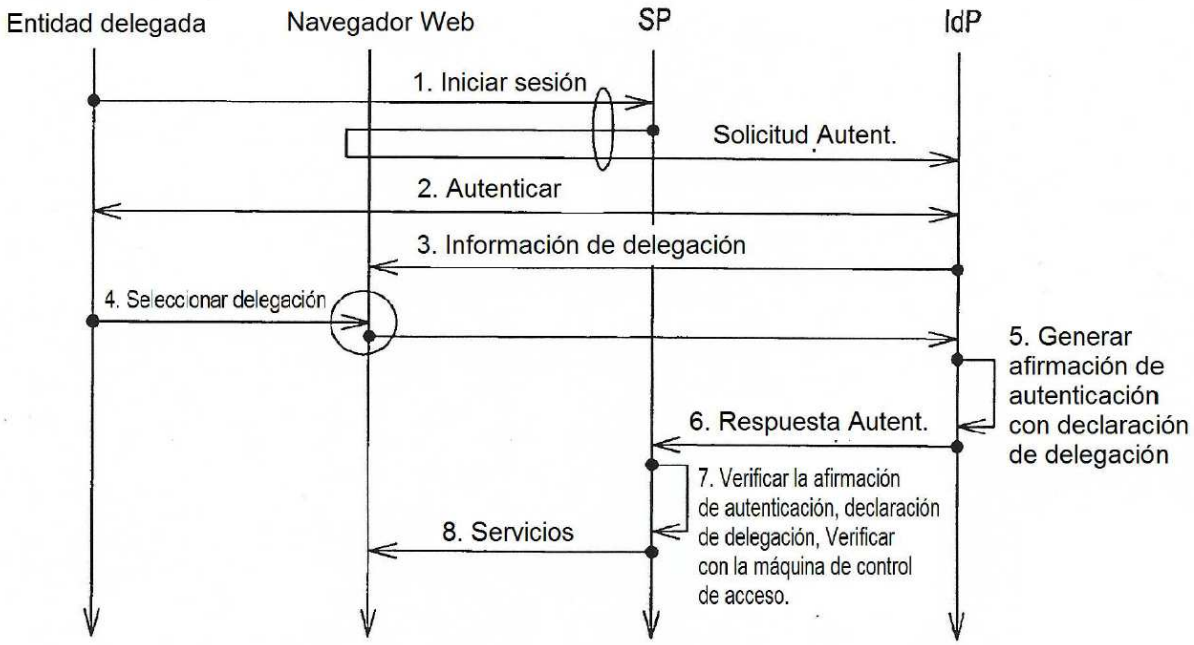
Entidad delegada
Navegador Web
SP
IdP
1. Iniciar sesión
Solicitud Autent.
2. Autenticar
3. Información de delegación
4. Seleccionar delegación
5. Generar afirmación de autenticación con declaración de delegación
6. Respuesta Autent.
7. Verificar la afirmación de autenticación, declaración de delegación, Verificar con la máquina de control de acceso.
8. Servicios

Fig. 3

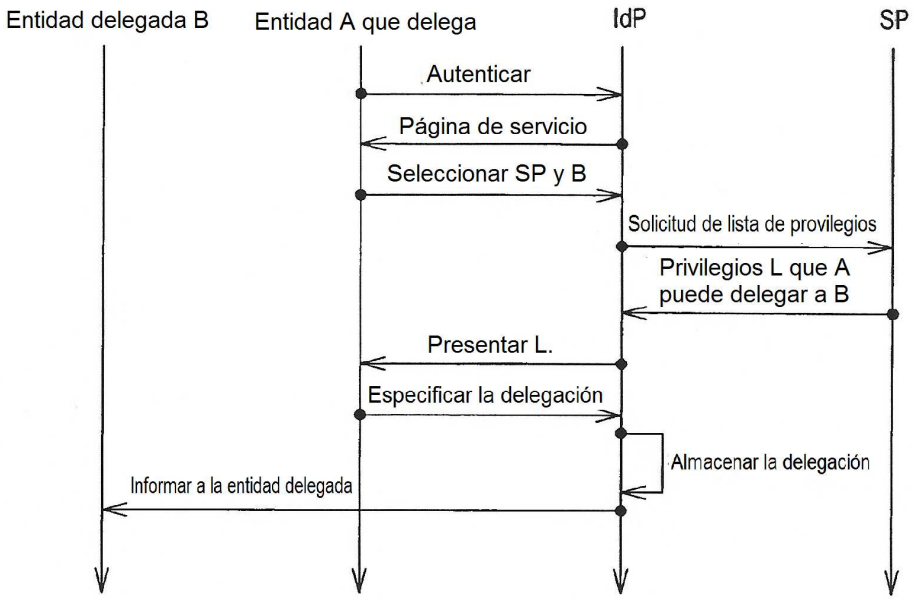
Entidad delegada B
Entidad A que delega
IdP
SP
Autenticar
Página de servicio
Seleccionar SP y B
Solicitud de lista de provilegios
Privilegios L que A puede delegar a B
Presentar L.
Especificar la delegación
Almacenar la delegación
Informar a la entidad delegada

Fig. 4

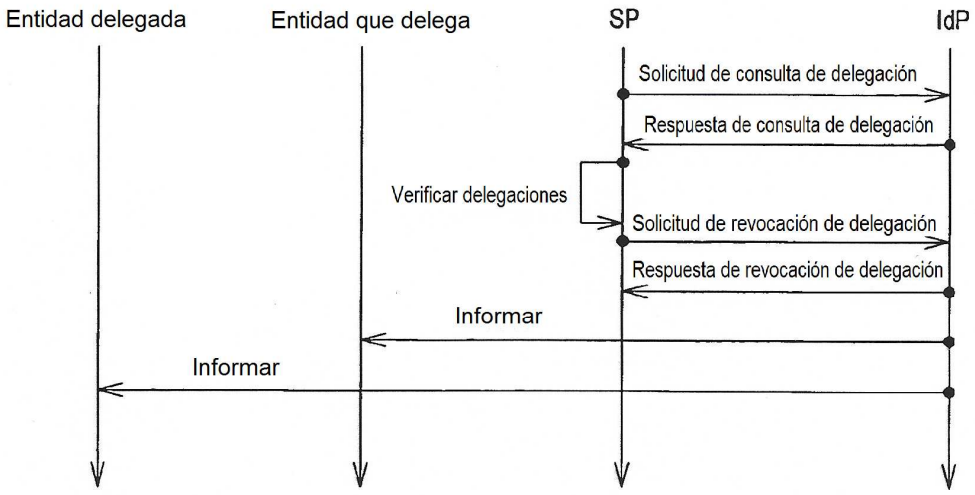
Entidad delegada
Entidad que delega
SP
IdP
Solicitud de consulta de delegación
Respuesta de consulta de delegación
Verificar delegaciones
Solicitud de revocación de delegación
Respuesta de revocación de delegación
Informar
Informar

Fig. 5