(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 426 135**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.03.2010 E 10715091 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2013 EP 2406931**

(54) Título: **Método para soportar la gestión y el intercambio de datos distribuidos de un usuario o una entidad**

(30) Prioridad:

12.03.2009 EP 09003600

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.10.2013

(73) Titular/es:

NEC EUROPE LTD. (100.0%)
Kurfürsten-Anlage 36
69115 Heidelberg, DE

(72) Inventor/es:

WINKLER, FLORIAN;
GIRAO, JOAO;
SANTOS, HUGO y
DA SILVA, JOAO

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Método para soportar la gestión y el intercambio de datos distribuidos de un usuario o una entidad

La presente invención se refiere a un método para soportar la gestión y el intercambio de datos distribuidos de un usuario o una entidad, en particular datos de información de perfiles de usuarios, en el que se proporciona un protocolo que emplea SAML (Lenguaje de Marcación de Afirmación de la Seguridad) como un protocolo de soporte de tal modo que los mensajes de SAML funcionan como contenedores para mensajes de DST (Plantilla del Servicio de Datos) o mensajes similares a DST para componer los mensajes DST de SAML, en el que dichos mensajes DST de SAML involucran mensajes de petición de DST de SAML o mensajes de respuesta de DST de SAML, en donde un mensaje de respuesta de DST de SAML incluye una petición de DST o similar a DST que se contesta por una respuesta de DST o similar a DST que se incluyen en un SAML. El mensaje de respuesta de DST, en el que dichos mensajes de DST o similares a DST incluyen información de procesamiento de datos, y en el que para dichos mensajes de DST o similares a DST se definen espacios de nombres de protocolo unificado como espacios de nombres específicos del protocolo.

Con una abundancia de servicios disponibles sobre la Internet de hoy en día y futura, que requieren cada uno la creación de cuentas, autenticación y almacenamiento de datos del perfil de usuario, los usuarios se enfrentan con el hecho de que sus perfiles se difunden entre una diversidad de proveedores de servicios diferentes, por ejemplo, bancos, librerías o servicios comunitarios como YouTube o Facebook.

La Gestión de Identidades (IdM) tiene por objeto la provisión de un inicio de sesión único (SSO) y un intercambio seguro y consciente de la privacidad de la información (perfil) de usuario entre los proveedores de servicios (SP) y los Proveedores de Identidades (IdP). La información de usuario se puede almacenar por un Proveedor de Identidades o las llamadas Autoridades de Atributos que se pueden consultar por el Proveedor de Identidades para datos de usuarios para distribuirlos a los SP solicitantes.

Además la mayor parte de los proveedores de servicios almacenan actualmente los datos de perfiles que son parte de sus definiciones de servicios en un formato propietario donde cada uno de los campos de datos tiene un nombre propietario y una semántica asociada. Esto significa que incluso si la Gestión de Identidades proporciona medios para la lectura de datos distribuidos desde diversas Autoridades de Atributos, hay siempre el requisito de mapear los identificadores de datos y/o las semánticas entre los dominios de los proveedores de servicios. Esto es tedioso, a menudo imposible y, si no se hace puede resultar un estrecho acoplamiento entre los consumidores de datos de perfiles y las autoridades que los proporcionan.

Los usuarios que quieren beneficiarse de las soluciones de la Gestión de Identidades querrán estar en el control de sus datos de perfiles distribuidos y de este modo necesitan un medio de gestionarlo en un modo conveniente. Esto incluirá la modificación y consulta siempre que se proteja por políticas de control de acceso y la capacidad de tener una clara visión general de qué datos personales están almacenados y dónde.

Adicionalmente, no solo los usuarios estarán interesados en la gestión de los perfiles y datos distribuidos, sino que también los SP estarán interesados en la provisión de servicios que incluyen tal manipulación. Al mismo tiempo, sin embargo, los SP que proporcionan los datos de perfiles de usuarios no querrán dar el control sobre los mismos, lo que requiere una solución que permita a los SP verificar/afirmar a las partes solicitantes y obligar a su propio control de acceso antes de distribuir los datos o permitir su manipulación.

Finalmente, una infraestructura que soporta la gestión de los perfiles de usuarios distribuidos tendrá que proporcionar los mapeos entre los identificadores de usuarios de los diferentes dominios de proveedores de servicios para asegurarse de que los usuarios que se identifican y se enlazan a un perfil específico en un dominio de SP se pueden identificar por un nombre diferente (lo más probable) en otro dominio de SP. Esta es una propiedad que es una parte inherente de las soluciones de gestión de identidad de hoy en día y una de las piedras angulares de protección de la privacidad.

SAML 2.0 es un lenguaje de marcación basado en XML desarrollado por el consorcio OASIS. Soporta el Inicio de Sesión Único, las transacciones distribuidas y la autorización basada en la afirmación a través de los diferentes dominios de seguridad. Se definen varias vinculaciones de protocolos que permiten el uso del SAML para servicios HTTP simples así como Servicios Web, es decir sobre SOAP (Protocolo de Acceso de Objetos Simples) y SIP (Protocolo de Iniciación de Sesión).

El uso de SAML, para SSO en combinación con el Subsistema Multimedia IP de 3GPP (IMS) se presentó en el documento "*Identity Management for IMS-based IPTV*", *IEEE Globecom* 2008. Además, la Alianza de Libertad adoptó el SAML para sus soluciones de IdM. De este modo, SAML constituye de hecho una normativa para el intercambio de información relacionada con la IdM en un entorno de empresa.

El SAML define varios tipos de peticiones y respuestas, por ejemplo consultar por los atributos de identidad o intercambiar reivindicciones acerca de las partes solicitante y respondedora. Además los mensajes de SAML pueden

transportar identificadores o identidades de usuarios virtuales. Dentro de este documento esos identificadores se denominan como seudónimos, ya que se pueden usar para ocultar una identidad real del usuario. Es importante observar, que los seudónimos pueden ser específicos del dominio, lo que significa que el mismo usuario se puede identificar por diferentes seudónimos en diferentes dominios de proveedores de servicios.

El SAML es solo para acceso de lectura, y no permite a los usuarios, ni a los Proveedores de Identidades o los SP gestionar, es decir escribir o modificar, la información de los perfiles en ningún modo.

Existe otro posible formato de mensaje que es la Plantilla de Servicios de Datos (DST) de la Alianza de Libertad especificada en https://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_data_services _template_v2_0_specifications. DST es la especificación de una plantilla de protocolo que define la estructura de los mensajes basados en XML que transportan la información para la gestión (creación, borrado, modificación y consulta) de los datos de perfiles. La DST asume que los datos de perfiles son accesibles en la estructura de XML y usa las expresiones XPATH para seleccionar los nodos de datos de perfiles que son objeto de procesamiento.

Como sugiere su nombre, la DST no es un protocolo sino una plantilla de los mensajes de protocolo que - como se ha establecido por la especificación - se entiende que se implementa por cada uno de los servicios de datos individualmente. La implementación incluye la definición de un espacio de nombres dependientes del servicio de datos tanto para los mensajes de protocolo como los datos que se gestionarán con DST. Sin embargo, esto hace a la DST completamente dependiente del servicio de datos de perfiles que la implementa, lo que no la hace unificada ni permite el desacoplamiento de los clientes y servidores de DST. De hecho, vincula los casos de plantillas de protocolo con el servicio de datos.

Actualmente no hay ningún medio para gestionar y modificar los datos de perfiles distribuidos en un modo seguro y consciente de la privacidad, lo que significa que un usuario tendrá que acceder a los servicios individuales para actualizar una parte de su información de perfil.

El documento del 3GPP TS 29.240 V8.0.0 (2008-12) "3nd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Generic User Profile (GUP); Stage 3; Network (Release 8)" trata del problema de la amplia distribución de datos asociados con un usuario debido a tener varios dominios dentro de un sistema móvil de 3GPP y varias tecnologías de acceso. Para posibilitar a los usuarios, abonados, operadores de red y proveedores de servicios de valor añadido crear, acceder y gestionar los datos relacionados con los usuarios localizados en diferentes entidades, se especifica un Perfil de Usuario Genérico de 3GPP que proporciona una arquitectura, descripción de datos e interfaz con mecanismos para manejar los datos.

Es un objeto de la presente invención mejorar y desarrollar adicionalmente un método del tipo descrito inicialmente para soportar la gestión y el intercambio de datos distribuidos de un usuario o una entidad, en particular datos de información de perfiles de usuarios, de tal modo que, empleando mecanismos que son fáciles de implementar, se posibilita a un usuario o una entidad gestionar y/o modificar sus datos distribuidos de un modo seguro y consciente de la privacidad.

De acuerdo con la invención, el objeto mencionado anteriormente se cumple por un método que comprende las características de la reivindicación 1. De acuerdo con esta reivindicación tal método se caracteriza por que cada una de dichas peticiones de DST o similares a DST incluye una instrucción de selección, en donde dicha instrucción de selección mantiene una expresión XPATH para indicar qué parte de dichos datos distribuidos se tiene que procesar, en donde dicha expresión XPATH se transmite al receptor futuro de dichas peticiones de DST o similares a DST, y en el que un espacio de nombres que se define en dichas peticiones de DST o similares a DST y que no es de uno de dichos nombres de espacio específicos del protocolo se usa en el interior de dicha expresión XPATH para referenciar elementos de dichos datos distribuidos.

De acuerdo con la invención se ha reconocido en primer lugar que en el contexto de proporcionar la gestión segura y consciente de privacidad e identidad y el intercambio de datos de usuario distribuidos se puede conseguir una enorme mejoría combinando SAML y DST en un modo específico. La combinación de SAML y DST se realiza proporcionando un protocolo que emplea SAML como protocolo de soporte, de tal modo que los mensajes de SAML funcionan como contenedores para los mensajes de DST o similares a DST para componer mensajes DST de SAML. Los mensajes de DST o similares a DST incluyen la información de procesamiento de datos para gestionar los datos distribuidos del usuario o entidad. Además se ha reconocido que el protocolo proporcionado puede ser independiente de los datos gestionados definiendo para los mensajes de DST o similares a DST espacios de nombres de protocolo unificado como los espacios de nombres específicos del protocolo. De este modo, estos espacios de nombres están vinculados a los propios mensajes de protocolo y se pueden distinguir de otras declaraciones de espacios de nombres en el interior de los mensajes de DST que se podrían usar para referirse a elementos de los datos distribuidos reales que se cambian, es decir se modifican y/ se gestionan. De este modo, el método de acuerdo con la invención posibilita la gestión y la modificación de los datos distribuidos por el usuario o entidad en un modo seguro y consciente de la privacidad.

Más específicamente, un mensaje DST de SAML involucra un mensaje de petición de DST de SAML o un mensaje de respuesta de DST de SAML, en donde un mensaje de petición de DST de SAML incluye una petición de DST o similar a DST que se contesta por una respuesta de DST o similar a DST que está incluida en un mensaje de respuesta de DST de SAML. De acuerdo con la invención, cada una de las peticiones DST o similares a DST incluye una instrucción de selección, en donde la instrucción de selección mantiene una expresión XPATH para indicar qué parte de los datos distribuidos tiene que procesarse. La expresión XPATH se transmite al receptor futuro de las peticiones DST o similares a DST, en particular al servicio de datos que se supone que devuelve información basada en la expresión XPATH, por ejemplo una consulta XPATH. Además se usa un espacio de nombres que se define en las peticiones de DST o similares a DST y que no es uno de los espacios de nombres específicos del protocolo dentro de la expresión XPATH para referirse a elementos de los datos distribuidos. Este espacio de nombres se puede usar por un Proveedor de Identidades para distinguir acerca de qué clase de información se solicitará para el usuario y qué proveedor de servicio de datos tiene que contactarse. Por ejemplo, el Proveedor de Identidades puede mantener un mapeo del espacio de nombres del servicio de datos de perfiles al espacio de nombre de los datos de perfiles (es decir el tipo) que proporciona este servicio. Este mapeo se puede mantener para cada uno de los usuarios.

De acuerdo con una realización preferida los mensajes DST de SAML pueden incluir un elemento que funciona como un contenedor - elemento contenedor - para transportar un único mensaje de DST o similar a DST. De este modo, es posible definir un nuevo tipo de mensaje de SAML que se deriva a partir de los tipos de mensajes SAML abstractos y que puede heredar todas las características del SAML pero adicionalmente puede actuar como un contenedor para un mensaje de DST o similar a DST. Se observará que también se pueden reutilizar los mensajes de SAML existentes como protocolo de soporte que funciona como contenedor para mensajes de DST o similares a DST.

De acuerdo con una realización preferida, los mensajes de petición de DST de SAML incluyen un elemento que funciona como un campo de tema para identificar al usuario o identidad cuyos datos están sujetos al procesamiento de DST especificado en el mensaje de DST o similar a DST contenido en el mensaje de petición de DST de SAML. De este modo, el campo de tema se puede usar para identificar al usuario. Un servicio de petición, que quiere recuperar información acerca de un usuario a través, por ejemplo, de un Proveedor de Identidades y usa DST, puede emplear el campo del tema para especificar al Proveedor de Identidades para qué usuario está tratando de capturar información. Este identificador de tema puede ser un seudónimo que se usa en el servicio de petición.

Ventajosamente, los mensajes de petición de DST de SAML pueden incluir un elemento que funciona como un campo de emisor para identificar al originador de los mensajes de petición de DST de SAML.

Además, los mensajes de petición de DST de SAML pueden incluir un elemento que funciona como un campo receptor para enviar los mensajes de petición de DST de SAML a un destino específico, en particular un servicio de datos específico. Por ejemplo, se puede emplear el campo receptor para una ID del proveedor de servicio receptor que puede ser bien un URL (Localizador de Recursos Uniformes) del punto final o un seudónimo del proveedor de servicios que se puede resolver por un Proveedor de Identidades.

Cada uno de los mensajes de petición de DST de SAML puede incluir exactamente un elemento contenedor que constituye la petición de DST o similar a DST.

Con respecto al procesamiento de DST, las peticiones de DST o similares a DST pueden transportar información de procesamiento de datos, en particular basada en XML, con respecto a la creación, modificación, borrado o consulta de los datos distribuidos. El tipo de procesamiento de DST no se da como un campo de mensaje específico. El tipo se puede inferir a partir del TipoPetición como se define en las especificaciones de DST. Este puede ser ModificarPetición, CrearPetición, BorrarPetición o ConsultarPetición.

Ventajosamente, la semántica de las peticiones de DST o similares a DST con respecto al proceso de creación y/o borrado se construyen de tal modo que el efecto de las peticiones está limitado solamente a la creación y/o borrado de datos dentro de un registro de datos de los datos distribuidos de un usuario o identidad, por ejemplo, dentro de un perfil de usuario.

Además, los mensajes de respuesta de DST de SAML pueden incluir un elemento que funciona como un campo de estado que indica el estado del mensaje de respuesta de DST de SAML.

Ventajosamente, los mensajes de respuesta de DST de SAML pueden incluir un elemento que funciona como un reintento de campo de tema para mantener la información acerca de un nombre de tema que se usará dentro de una petición de reintento. Esto es necesario en el caso de que los identificadores de tema se mapeen por un Proveedor de Identidades en un modo ad hoc entre dominios.

Cada uno de los mensajes de respuesta de DST de SAML puede incluir uno o más elementos de contenedor incluyendo las respuestas de DST o similares a DST. La necesidad de tener varios elementos de contenedor dentro de una respuesta de DST de SAML se puede deber al requisito potencial de que el Proveedor de Identidades puede

acumular varias respuestas DST o similares a DST dentro de una única respuesta de DST de SAML.

El uno o más elementos de contenedor incluidos por los mensajes de respuesta de DST de SAML pueden incluir un identificador que se usa para referirse al emisor de una respuesta de DST. Este identificador se puede usar por ejemplo por un proveedor de servicio solicitante para contactar con un proveedor de servicios específicos del servidor en el caso de respuestas insatisfactorias o inesperadas. Si una respuesta de DST específica indica un fallo, el cliente solicitante puede enviar otra petición solo al proveedor de servicio que falló el mensaje DST. El identificador se puede usar además para indicar a un usuario qué proveedores de servicios responden y cómo, por ejemplo, en una interfaz de usuario de gestión de perfiles de usuario distribuidos.

Ventajosamente, los mensajes DST de SAML pueden incluir un elemento de firma que contiene el resultado de firmar los mensajes DST de SAML.

Los mensajes DST de SAML se pueden intercambiar entre los proveedores de servicios solicitante y servidor para gestionar los datos distribuidos del usuario o la entidad.

Además, puede estar involucrado un Proveedor de Identidades en el intercambio de mensajes DST de SAML entre los proveedores de servicios solicitante y servidor.

Ventajosamente, el usuario o la entidad pueden acceder a un proveedor de servicios por un identificador de seudónimo, en el que el Proveedor de Identidades se emplea por los proveedores de servicios para resolver el identificador de seudónimo y/o mapearlo a la cuenta de usuario local.

Un proveedor de servicio solicitante puede enviar un mensaje de petición de DST de SAML incluyendo el identificador de seudónimo del usuario o la entidad como tema y un mensaje de DST o similar a DST al Proveedor de Identidades.

Además, el Proveedor de Identidades puede crear un identificador de seudónimo temporal que es válido en ambos proveedores de servicio solicitante y servidor.

Ventajosamente, el Proveedor de Identidades puede responder al proveedor de servicios solicitante con un mensaje de reintento DST de SAML indicando el identificador de seudónimo temporal.

Adicionalmente o alternativamente el Proveedor de Identidades puede sustituir el identificador de seudónimo por el identificador de seudónimo temporal dentro del mensaje DST de SAML.

El proveedor de servicios solicitante puede enviar un nuevo mensaje de petición de DST de SAML incluyendo el seudónimo temporal como tema y el mensaje de DST o similar a DST al Proveedor de Identidades.

Ventajosamente, el Proveedor de Identidades puede buscar qué proveedores de servicios son capaces de servir las peticiones de DST o similares a DST que afectan al tipo de datos distribuidos en los datos de información de perfiles de usuarios particulares, especificados en las peticiones de DST o similares a DST y retransmitir el mensaje de petición de DST de SAML a los proveedores de servicios servidores.

Los proveedores de servicios servidores pueden responder con mensajes de respuesta de DST de SAML al Proveedor de Identidades, en donde el Proveedor de Identidades acumula las respuestas DST o similares a DST incluidas en los mensajes de respuesta de DST de SAML de los proveedores de servicios servidores y devuelve un mensaje de respuesta de DST de SAML que contiene las respuestas acumuladas de DST o similares a DST al proveedor de servicios solicitante.

En una realización preferida, se puede prever que el Proveedor de Identidades se puede usar como el servidor de descubrimiento para un proveedor de servicio solicitante para descubrir los proveedores de servicios servidores. El Proveedor de Identidades puede comprobar la firma de un mensaje de petición de DST de SAML enviado desde el proveedor de servicio solicitante. Posteriormente, el Proveedor de Identidades puede buscar qué proveedores de servicios están capacitados para servir a las peticiones DST o similares a DST que afectan al tipo de datos distribuidos, en particular los datos de información de perfiles de usuario, especificados en las peticiones DST o similares a DST. El Proveedor de Identidades puede crear un identificador de seudónimo temporal y sustituir el tema en el mensaje de petición de DST de SAML para el seudónimo temporal - petición cambiada -. Finalmente, el Proveedor de Identidades firma la petición cambiada y envía el mensaje de respuesta de DST de SAML que contiene la petición cambiada y los Identificadores de Recursos Uniformes de los proveedores de servicio servidores buscados al proveedor de servicios solicitante.

Ventajosamente, el proveedor de servicios solicitante puede refirmar la petición cambiada y enviar la petición refirmada cambiada a los proveedores de servicios servidores buscados. Hay varios modos sobre cómo diseñar y desarrollar adicionalmente la enseñanza de la presente invención en un modo ventajoso. Para este fin, nos referiremos a las reivindicaciones de patente subordinadas a la reivindicación de patente 1 por una parte, y a la

siguiente explicación de los ejemplos preferidos de las realizaciones de la invención ilustradas por los dibujos por otra parte. En conexión con la explicación del ejemplo preferido de una realización de la invención por la ayuda de los dibujos, se explicarán las realizaciones preferidas en general y desarrollos adicionales de las enseñanzas. En los dibujos

la Fig. 1 es una visión general de la infraestructura esquemática de DST de SAML que ilustra un ejemplo de un escenario de aplicación de un método de acuerdo con la presente invención,

la Fig. 2 es una vista esquemática que ilustra un mensaje de petición de DST de SAML de acuerdo con una realización de la presente invención,

la Fig. 3 es una vista esquemática que ilustra un mensaje de respuesta de DST de SAML de acuerdo con una realización de la presente invención,

la Fig. 4 es un diagrama de secuencia que ilustra los flujos de mensajes de ejemplo para el caso de que el Proveedor de Identidades actúe como un proxy DST de SAML, y

la Fig. 5 es un diagrama de secuencia que ilustra los flujos de mensajes de ejemplo para el caso de que el Proveedor de Identidades actúe como un servidor de descubrimiento para un proveedor de servicios solicitante para descubrir posibles proveedores de servicios servidores.

La Fig. 1 muestra una visión general de la infraestructura y los componentes que se han previsto para un método de acuerdo con la presente invención para posibilitar la gestión de los perfiles de usuarios distribuidos y los datos sensibles a la IdM. Los usuarios accederán a los proveedores de servicios por un seudónimo determinado y es un caso común para los escenarios de IdM. Con la ayuda de un Proveedor de Identidad, el seudónimo se puede resolver por los SP y mapearse a cuentas locales del usuario, por ejemplo para proporcionar un inicio de sesión único. Cuando un proveedor de servicios necesita acceder y/o manipular la información de perfiles de usuarios que no está disponible localmente, enviará una petición de DST de SAML a un punto de extensión del Proveedor de Identidades que contiene por sí mismo como el emisor de la petición, el seudónimo del usuario como asunto del mensaje y una indicación de qué clase de datos de perfiles está afectada.

El Proveedor de Identidades, que actúa como un proxy DST de SAML, es entonces responsable de la identificación de los SP que albergan la clase de información de perfiles solicitada para el usuario determinado y para la creación de un mapeo entre el seudónimo del usuario en el SP solicitante y los identificadores del usuario usados en los SP servidores. Después de hacer esto, el Proveedor de Identidades redirige la petición a todos los SP que pueden servir la petición para el usuario. Los SP servidores, que mantienen la información de perfil del usuario pueden comprobar la validez de la petición, incluyendo las firmas del Proveedor de Identidades y las reivindicaciones y a continuación procesa la petición de DST enviada dentro del mensaje de SAML.

El procesamiento de la petición puede incluir la aplicación de las políticas de acceso y seguridad propietarias para cada uno de los SP individuales. Esto es para asegurar que la manipulación o la distribución de datos de perfiles están garantizadas. Después del procesamiento, cada uno de los SP servidores envía de vuelta una respuesta de DST de SAML al Proveedor de Identidades que acumula los resultados en una única respuesta de DST de SAML que incluye la información acerca del SP que envió cada una de las respuestas. Las respuestas acumuladas se envían a continuación de vuelta al SP solicitante.

Para proporcionar la infraestructura como se describe en el escenario de aplicación de la Fig. 1, se modifica la DST. Las modificaciones de DST, que se explicarán con más detalle en lo siguiente se denominan como mensajes similares a DST. En general, es importante observar que la DST es una plantilla, no un protocolo y usualmente vinculada por nombres de espacio al servicio de datos que proporciona la DST como una interfaz. Una implementación de DST requiere la definición de tres espacios de nombres, uno para los elementos XML de utilidad, otro para los mensajes base de DST de XML y otro para los esquemas de implementación de referencia de DST.

Para superar la limitación del propietario y de este modo vincular nombres de espacios, se definen nombres de protocolo unificados para los mensajes de DST que serán los siguientes:

1) um:eu:neclab:nw:util:2009-02 para los elementos de utilidad
2) um:eu:neclab:nw:dst:2009-02 para los mensajes base de DST
3) um:eu:neclab:nw:dst:2009-02:ref para el esquema de implementación de referencia de DST.

Definiéndolos como los nombres de espacio específicos del protocolo, es posible distinguirlos de las otras declaraciones de espacios de nombres que ahora se pueden usar para indicar diferentes clases de tipos de datos de perfiles que están sujetos al procesamiento de DST.

```
<ns3:Query xmlns:ns1 = "um:eu:neclab:nw:util:2009-02"
    xmins:ns2 = "um:eu:neclab:nw:dst:2009-02"
```

```
        xmins:ns3 = "um:eu:neclab:nw:dst:2009-02:ref"
        xmins:bp = "um:banking:profile:service">
    <ns3:QueryItem>
        <ns3:Select>/bp:Banking/bp:Accounts</ns3:Select>
    </ns3:QueryItem>
</ns3:Query>
```

Por ejemplo, la muestra de XML anterior representa una simple petición de consulta de DST que recupera todas las cuentas bancarias de un usuario. Se observará que la declaración de Selección contiene una consulta de XPATH que usa un espacio de nombres que no es el espacio de nombres del protocolo sino un espacio de nombres definido adicionalmente para indicar el tipo de perfil de usuario que se solicita. En la DST original, esto no está previsto. El espacio de nombres um:banking:profile:service en la muestra anterior se refiere a un perfil bancario de esquema definido. Como ya se ha comenzado por la Alianza de Libertades, se asume que habrá más esquemas de perfiles normalizados, por ejemplo, para los datos bancarios, datos de perfiles personales, etc. con nombres de elementos bien definidos y semánticas de datos definidas. Cada uno de estos tipos de perfiles estará bien definido, siguiendo una estructura determinada y especificando qué datos están contenidos en el interior de los perfiles de esa especificación. Esto hará posible recuperar una clase específica de información con semánticas bien definidas y en un modo normalizado. El método de acuerdo con la invención es independiente del tipo de perfil que se podría manipular y por lo tanto posibilitará una amplia interoperabilidad entre los SP.

Además, la semántica de los mensajes de Crear y Borrar DST está ligeramente cambiada. En la especificación de la Plantilla de Servicios de Datos de la Alianza de Libertad, los mensajes de Crear y Borrar se usan para crear y borrar las grabaciones enteras de datos, en la terminología de acuerdo con la presente invención, perfiles enteros o cuentas. Para crear o borrar datos dentro de un perfil, se usan las peticiones de Modificación. Estas semánticas se cambian limitando el efecto de los mensajes de Crear y Borrar solamente a la creación y borrado de datos dentro de un perfil específico. Esto se hace porque se asume que los SP tienen que estar en un control completo de creación y borrado de perfiles/cuentas enteras y por lo tanto el protocolo se hace más fácil y limpio. Este cambio en la semántica requiere la adición de una declaración de Selección para el mensaje de Crear para indicar con una expresión de XPATH dónde se deberían crear nuevos datos en el interior de un perfil.

Los datos de perfil, o servicios de datos como se denominan en la DST, se supone que están representados en la estructura XML. Esto no significa que los datos para el procesamiento de DST solo puedan ser datos estructurados de XML, sino que tendrán que ser una capa de abstracción para cualesquiera datos a procesar por el método de acuerdo con la presente invención que expone los datos como si estuviesen estructurados en XML.

Los mensajes de DST son desconocidos para el usuario (tema) cuyos datos de perfil están afectados por la petición. Además no transportan ninguna información que se podría usar para afirmar la parte solicitada o validar la integridad del mensaje. Finalmente, no hay ningún medio para proporcionar la Gestión de Identidades dentro de los mensajes de DST. Esta funcionalidad se tiene que proporcionar por el protocolo de soporte, es decir el protocolo que transporta los mensajes de DST. SAML 2.0 es de hecho la normativa para las soluciones de IdM de compañías. SAML 2.0 es un protocolo bien entendido y que ya se usa ampliamente. Para no afectar a la tecnología existente, se elige extender el protocolo de SAML definiendo un nuevo tipo de petición y respuesta.

La Fig. 2 es una vista esquemática que ilustra un mensaje de petición de DST de SAML de acuerdo con una realización de la presente invención. La petición de DST de SAML ilustrada es un nuevo tipo que se deduce del SubjetQueryAbstractType de SAML. Deduciendo a partir de un tipo de petición existente es seguro que los beneficios y propiedades de los mensajes de SAML se mantienen como necesarios para la Gestión de Identidades, por ejemplo, las firmas de mensajes, seguridad, objetos, etc. De este modo, una petición de DST de SAML contiene un campo de tema que identifica a un usuario, un campo de emisor que se puede usar para identificar el originador de la petición, y un elemento de firma que contiene el resultado de la firma del mensaje.

Como se ilustra en la Fig. 2, se define adicionalmente un nuevo elemento que contiene la petición de DST. Usando la DST de SAML, un SP solicitante puede especificar exactamente qué perfil de usuario - dado por el tema - estaría afectado por la petición de DST dentro del mensaje de SAML. Además, como el SAML soporta el intercambio de los mensajes de mapeo del identificador, es posible que el identificador del tema sea un seudónimo del usuario, y de ese modo no solo oculta la identidad real del usuario sino que también permite para el identificador de usuario el mapeo entre dominios de proveedor de servicios. Este es uno de los prerrequisitos de la aplicabilidad real de dominios cruzados.

La Fig. 3 muestra una vista esquemática que ilustra un mensaje de respuesta de DST de SAML de acuerdo con una realización de la presente invención que es la respuesta a una petición de DST de SAML. La respuesta de DST de SAML ilustrada en la Fig. 3 se deduce de un tipo de respuesta de SAML bien conocida (StatusResponseType), asegurando que una respuesta puede contener un estado, firma, etc.

La respuesta de DST de SAML contiene un elemento que mantiene información acerca del nombre del tema que se debería usar dentro de una petición de reintento. Este es necesario en el caso de que los identificadores de temas

estén mapeados por un Proveedor de Identidades en un modo ad hoc entre dominios. Además, se añade la posibilidad de declarar varios elementos de DSTContainer dentro de una respuesta de DST de SAML.

Cada uno de los elementos DSTContainer contiene la respuesta a la petición de DST así como un identificador que se puede usar para referirse al proveedor de servicios que emitió la respuesta de DST. Este identificador se puede usar por ejemplo por un SP solicitante para contactar con un SP servidor específico en el caso de respuestas insatisfactorias o inesperadas. Se puede usar además para indicar a un usuario qué SP responden y cómo, por ejemplo, en una interfaz de usuario de gestión de perfiles de usuario distribuida.

Se observará que cada SP servidor responderá con exactamente una respuesta de DST dentro del elemento de DSTContainer, ya que una petición de DST de SAML contiene exactamente una petición de DST. La necesidad de tener varios elementos DSTContainer dentro de una respuesta de DST de SAML se debe al requisito de tener el Proveedor de Identidades varias respuestas DST acumuladas dentro de una respuesta de DST de SAML. Sin embargo, este requisito es solo para el nodo proxy ilustrado en la Fig. 4.

La Fig. 4 es un diagrama de secuencia que muestra un mensaje de ejemplo para el caso de que el Proveedor de Identidades actúe como un proxy DST de SAML. Los mensajes DST de SAML se usan directamente entre los SP solicitante y servidor. Sin embargo para desacoplar los solicitantes y respondedores y proporcionar una gestión de datos de perfiles de dominios cruzados que respete la privacidad del usuario, el Proveedor de Identidades está involucrado en el intercambio de mensajes DST de SAML. Por lo tanto se implementa una extensión al Proveedor de Identidades y esta se integra dentro del flujo del mensaje.

Ilustrado en la etapa 1.0 de la Fig. 4, un usuario accede al SP-A por un seudónimo determinado. Para consultar o manipular el perfil del usuario el SP-A crea un mensaje DST de SAML con el seudónimo del usuario como tema y un mensaje DST que afecta a los datos específicos del usuario. En la etapa 1.2 el SP-A envía el mensaje DST de SAML al Proveedor de Identidades. Como el seudónimo del usuario solo es válido dentro del dominio de SP-A, el Proveedor de Identidades crea un seudónimo temporal que será válido en ambos SP solicitante y servidor. El Proveedor de Identidades responde a continuación con un mensaje de reintento de DST de SAML indicando el seudónimo temporal que se debería usar en la consulta. Esto es necesario si las firmas del mensaje de SP-A se mantienen intactas. Un enfoque más fácil sería que el Proveedor de Identidades intercambiase los seudónimos dentro del mensaje DST de SAML, pero esto invalidaría la firma del SP-A. Un SP servidor solo podría validar entonces la firma del Proveedor de Identidades pero ya no podría validar la firma del SP originador. Esto no siempre es un inconveniente, sino que depende de las relaciones de confianza y de negocio entre los SP.

En la etapa 1.5 de la Fig. 4, el SP-A envía un mensaje DST de SAML con el seudónimo temporal como tema. En la etapa 1.6 el Proveedor de Identidades busca qué SP pueden manejar las peticiones DST que afectan al tipo de perfil especificado en la petición entrante. Por ejemplo, si la petición de DST afecta a los perfiles del tipo um:banking:profile:data, el Proveedor de Identidades busca todos los bancos con los que el usuario tiene una suscripción. Esta información tiene que estar disponible para el Proveedor de Identidades que usualmente se establece por una etapa de federación de cuentas anterior.

En la etapa 1.7 de la Fig. 4, el Proveedor de Identidades redirige la petición al primer SP servidor (SP-B) que en primer lugar intenta resolver el seudónimo temporal a partir de la petición para una ID del usuario local. Esto identificará el perfil de usuario. El Proveedor de Identidades resuelve la ID temporal como está acostumbrado en los escenarios de IdM. Después de esto el SP-B está procesando la petición de DST y responde con una respuesta de DST de SAML incluyendo la respuesta a la petición de DST (etapa 1.11).

El Proveedor de Identidades repite este procedimiento para todos los SP disponibles y acumula las respuestas de cada uno de los SP servidores. Finalmente, (etapa 1.18) el Proveedor de Identidades devuelve una respuesta de DST de SAML que contiene todas las respuestas DST desde los SP servidores. Adicionalmente para cada una de las respuestas DST, incluye una ID para identificar al respondedor de DST respectivo, es decir, el SP servidor.

Durante todo el proceso, el Proveedor de Identidades puede denegar el acceso a la información del perfil específico o los SP servidores de acuerdo con las políticas de control de acceso definidas por el usuario. Además, cada uno de los SP servidores tiene un control total sobre el acceso y modificación de la información de perfiles que almacena. De este modo, se puede asegurar que cada uno de los SP solo puede acceder a un subconjunto limitado o ninguna información en absoluto.

Haciendo uso de los metadatos publicados por los SP - que es un concepto común en las soluciones IdM de la Alianza de Libertades - es posible para un Proveedor de Identidades o SP solicitante descubrir qué tipos de datos de perfiles soporta un SP. Un SP servidor solo tiene que especificar los tipos soportados de perfiles de usuarios dentro de los metadatos publicados. Los tipos de perfiles se pueden identificar simplemente por el espacio de nombres del esquema de perfil único que también se usa para identificar el tipo de perfil dentro de los mensajes DST de SAML.

La Fig. 5 muestra un diagrama de secuencia que ilustra flujos de mensajes de ejemplo para el caso de que el Proveedor de Identidades actúe como un servidor de descubrimiento para un proveedor de servicios solicitante para

descubrir posibles proveedores de servicio servidores. Como prerrequisito, el Proveedor de Identidades, el SP solicitante y el SP servidor de datos tienen una federación. Especialmente, el SP servidor de datos tiene un almacenamiento de la información de usuario - cuenta - y federó esa cuenta con el Proveedor de Identidades. Es decir, existe un identificador del mapeo de cuentas en el Proveedor de Identidades que puede usar el SP servidor de datos para identificar una cuenta de datos de usuario local.

En la etapa 1.0 de la Fig. 5, el SP Solicitante envía una petición de DST de SAML al Proveedor de Identidades incluyendo el seudónimo del usuario como tema. El Proveedor de Identidades puede comprobar las firmas para asegurarse de que la petición es válida (etapa 1.1), averigua qué tipo de perfil será el tema para el procesamiento de DST (etapa 1.2 y 1.3), encuentra los SP que pueden servir a esta clase de petición para este usuario específico (etapa 1.4 y 1.5) y crea un seudónimo temporal que se puede usar por los SP servidores para identificar el usuario. Esto se establecería por el mapeo del nameID.

El Proveedor de Identidades intercambia a continuación el tema del mensaje DST de SAML con el seudónimo temporal y firma el mensaje con su firma. Como el cambio de la petición invalida la firma del SP Solicitante, el Proveedor de Identidades envía una respuesta de DST de SAML al SP Solicitante que contiene la petición cambiada y los URL (Localizadores de Recursos Uniformes) de punto final de los SP servidores que pueden servir esa petición cambiada y que tienen un mapeo del nameID establecido para el seudónimo temporal (etapa 1.9). El Proveedor de Identidad podría tener políticas de acceso impuestas y por ejemplo tener ciertos SP excluidos de la lista de URL.

El SP Solicitante refirmaría a continuación la petición de DST de SAML (lo hace de este modo, porque confía en el Proveedor de Identidades) y envía la petición a uno o varios de los SP para los que el SP solicitante recuperó los URL de contacto. A continuación cada uno de los SP servidores es capaz de comprobar tanto la firma del Proveedor de Identidades como del SP Solicitante. Un SP servidor resolvería el seudónimo para una ID del usuario local, serviría la petición de DST y respondería con la respuesta de DST de SAML al SP Solicitante.

Por lo tanto, la carga del Proveedor de Identidades es menor y la conversación entre los SP es más directa. Por otra parte, saca el Proveedor de Identidades del bucle de mensajes y de este modo reduce sus capacidades de imponer derechos de acceso. Además, distribuyendo los URI del punto final de los SP de DST de SAML servidores, un SP solicitante es capaz de averiguar dónde tiene cuentas un usuario. Aunque el SP solicitante podría identificar a un usuario solo por un seudónimo, es decir no su identidad real, esto podría comprometer la privacidad del usuario.

Muchas modificaciones y otras realizaciones de la invención mostradas en este documento vendrán a la mente de los expertos en la técnica a la que pertenece la invención que tienen el beneficio de las enseñanzas presentadas en la descripción anterior y los dibujos asociados. Por lo tanto se entenderá que la invención no está limitada a las realizaciones específicas reveladas y que se intenta que las modificaciones y otras realizaciones estén incluidas dentro del alcance de las reivindicaciones adjuntas. Aunque se han empleado términos específicos en este documento, se usan solo en un sentido genérico y descriptivo y no para propósitos de limitación.

REIVINDICACIONES

1. Método para soportar la gestión y el intercambio de datos distribuidos de un usuario o una entidad, en particular datos de información de perfiles de usuarios,
en el que se proporciona un protocolo que emplea SAML (Lenguaje de Marcación de Afirmación de Seguridad), como protocolo de soporte en tal modo que los mensajes de SAML funcionan como contenedores para DST, (Plantilla de Servicios de Datos), para componer mensajes DST de SAML,
en el que dichos mensajes DST de SAML involucran mensajes de petición de DST de SAML o mensajes de respuesta de DST de SAML,
en el que un mensaje de petición de DST de SAML incluye una petición de DST que se contesta por una respuesta de DST que está incluida en un mensaje de respuesta de DST de SAML,
en el que, dichos mensajes de DST incluyen información de procesamiento de datos y
en el que, para dichos mensajes de DST se definen espacios de nombres de protocolo unificado como espacios de nombres específicos del protocolo,
en el que, dichas peticiones de DST incluyen una declaración de selección, en el que dicha declaración de selección mantiene una expresión XPATH para indicar qué parte de dichos datos distribuidos se tiene que procesar,
en el que dicha expresión XPATH se maneja sobre el receptor futuro de dichas peticiones de DST, y
en el que el espacio de nombres que se define en dichas peticiones de DST y que no es uno de dichos espacios de nombres específicos del protocolo se usa en el interior de dicha expresión XPATH para los elementos de referencia de dichos datos distribuidos.

2. El método de acuerdo con la reivindicación 1, en el que dichos mensajes DST de SAML incluyen un elemento que funciona como un contenedor - elemento contenedor - para transportar un único mensaje de DST.

3. El método de acuerdo con la reivindicación 1 o 2, en el que dichos mensajes de petición de DST de SAML incluyen un elemento que funciona como campo de tema para la identificación del usuario o la entidad cuyos datos están sujetos al procesamiento de DST especificado en el mensaje de DST contenido en dichos mensajes de petición de DST de SAML, y/o
en el que dichos mensajes de petición de DST de SAML incluyen un elemento que funciona como un campo del emisor para la identificación del originador de dichos mensajes de petición de DST de SAML, y/o
en el que dichos mensajes de petición de DST de SAML incluyen un elemento que funciona como un campo del receptor para enviar dichos mensajes de petición de DST de SAML a un destino específico, en particular a un servicio de datos específico.

4. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que cada uno de dichos mensajes de petición de DST de SAML incluye un elemento contenedor que constituye dicha petición de DST, o
en el que dichas peticiones de DST transportan información de procesamiento de datos con respecto a la creación, modificación, borrado o consulta de dichos datos distribuidos.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que la semántica de dichas peticiones de DST con respecto a dicho procesamiento de creación y/o borrado se construye de tal modo que el efecto de dichas peticiones se limita solamente a la creación y/o borrado de datos dentro de un registro de datos.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en el que dichos mensajes de respuesta de DST de SAML incluyen un elemento que funciona como campo de estado que indica el estado del mensaje de respuesta de DST de SALM, y/o
en el que dichos mensajes de respuesta de DST de SAML incluyen un elemento que funciona como un campo de reintento de tema para mantener la información acerca de un nombre de tema que se usará dentro de una petición de reintento.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, en el que cada uno de dichos mensajes de respuesta de DST de SAML incluyen uno o más elementos contenedores que incluyen dichas respuestas de DST.

8. El método de acuerdo con la reivindicación 7, en el que dicho uno o más elementos de contenedor incluidos por dichos mensajes de respuesta de DST de SAML incluyen un identificador que se usa para referirse al emisor de una respuesta de DST.

9. El método de acuerdo con cualquiera de las reivindicaciones 1 a 8, en el que dichos mensajes DST de SAML incluyen un elemento de firma que contiene el resultado de firmar dichos mensajes DST de SAML, y/o
en el que dichos mensajes DST de SAML se intercambian entre los proveedores de servicios solicitante y servidor para gestionar dichos datos distribuidos de dicho usuario o dicha entidad.

10. El método de acuerdo con cualquiera de las reivindicaciones 1 a 9, en el que está involucrado un Proveedor de Identidades en el intercambio de dichos mensajes DST de SAML entre los proveedores de servicios solicitante y servidor,
en el que dicho usuario o dicha entidad pueden acceder a un proveedor de servicios por un identificador de

seudónimo, en el que dicho Proveedor de Identidades se emplea por los proveedores de servicios para resolver dicho identificador de seudónimo y/o mapearlo a su cuenta de usuario local, y/o
en el que un proveedor de servicio solicitante puede enviar un mensaje de petición de DST de SAML incluyendo dicho identificador de seudónimo de dicho usuario o dicha entidad como tema y un mensaje de DST a dicho Proveedor de Identidades.

11. El método de acuerdo con la reivindicación 10, en el que dicho Proveedor de Identidades crea un identificador de seudónimo temporal que es válido tanto en dicho proveedor de servicio solicitante como dicho proveedor de servicio servidor.

12. El método de acuerdo con la reivindicación 11, en el que dicho Proveedor de Identidades responde a dicho proveedor de servicios solicitante con un mensaje de reintento de DST de SAML que indica dicho identificador de seudónimo temporal, y/o
en el que dicho Proveedor de Identidades sustituye dicho identificador de seudónimo por dicho identificador de seudónimo temporal dentro de dicho mensaje de DST de SAML, y/o
en el que dicho proveedor de servicios solicitante envía un nuevo mensaje de petición de DST de SAML que incluye dicho seudónimo temporal como tema y dicho mensaje de DST a dicho Proveedor de Identidades.

13. El método de acuerdo con cualquiera de las reivindicaciones 10 a 12, en el que dicho Proveedor de Identidades busca qué proveedores de servicios pueden servir dichas peticiones de DST que afectan al tipo de dichos datos distribuidos, en particular los datos de información de perfiles de usuarios, especificados en dichas peticiones de DST y redirige dicho mensaje de petición de DST de SAML a dichos proveedores de servicio servidores, y/o
en el que dichos proveedores de servicios servidores responden con mensajes de respuesta de DST de SAML a dicho Proveedor de Identidades, en el que dicho Proveedor de Identidades acumula dichas respuestas de DST incluidas en dichos mensajes de respuesta de DST de SAML de dichos proveedores de servicios servidores y devuelve un mensaje de respuesta de DST de SAML que contiene dichas respuestas de DST o similares a DST acumuladas a dicho proveedor de servicios solicitante.

14. El método de acuerdo con cualquiera de las reivindicaciones 10 a 13, en el que dicho Proveedor de Identidades se usa como servidor de descubrimiento para un proveedor de servicios solicitante para descubrir proveedores de servicio servidores,
en el que dicho Proveedor de Identidades comprueba la firma de un mensaje de petición de DST de SAML enviado desde dicho proveedor de servicios solicitante,
en el que dicho Proveedor de Identidades busca qué proveedores de servicios pueden servir dichas peticiones de DST que afectan al tipo de dichos datos distribuidos, en particular datos de información de perfiles de usuario, especificados en dichas peticiones de DST,
en el que dicho Proveedor de Identidades crea un identificador de seudónimo temporal,
en el que dicho Proveedor de Identidades sustituye el tema en dicho mensaje de petición de DST de SAML por dicho seudónimo temporal - petición cambiada -,
en el que dicho Proveedor de Identidades firma dicha petición cambiada, y
en el que dicho Proveedor de Identidades envía un mensaje de respuesta de DST de SAML que contiene dicha petición cambiada y los Identificadores de Recursos Uniformes de dichos proveedores de servicios servidores de búsqueda a dicho proveedor de servicios solicitante.

15. El método de acuerdo con la reivindicación 14, en el que dicho proveedor de servicios solicitante refirma dicha petición cambiada y envía dicha petición cambiada refirmada a dichos proveedores de servicios servidores buscados.

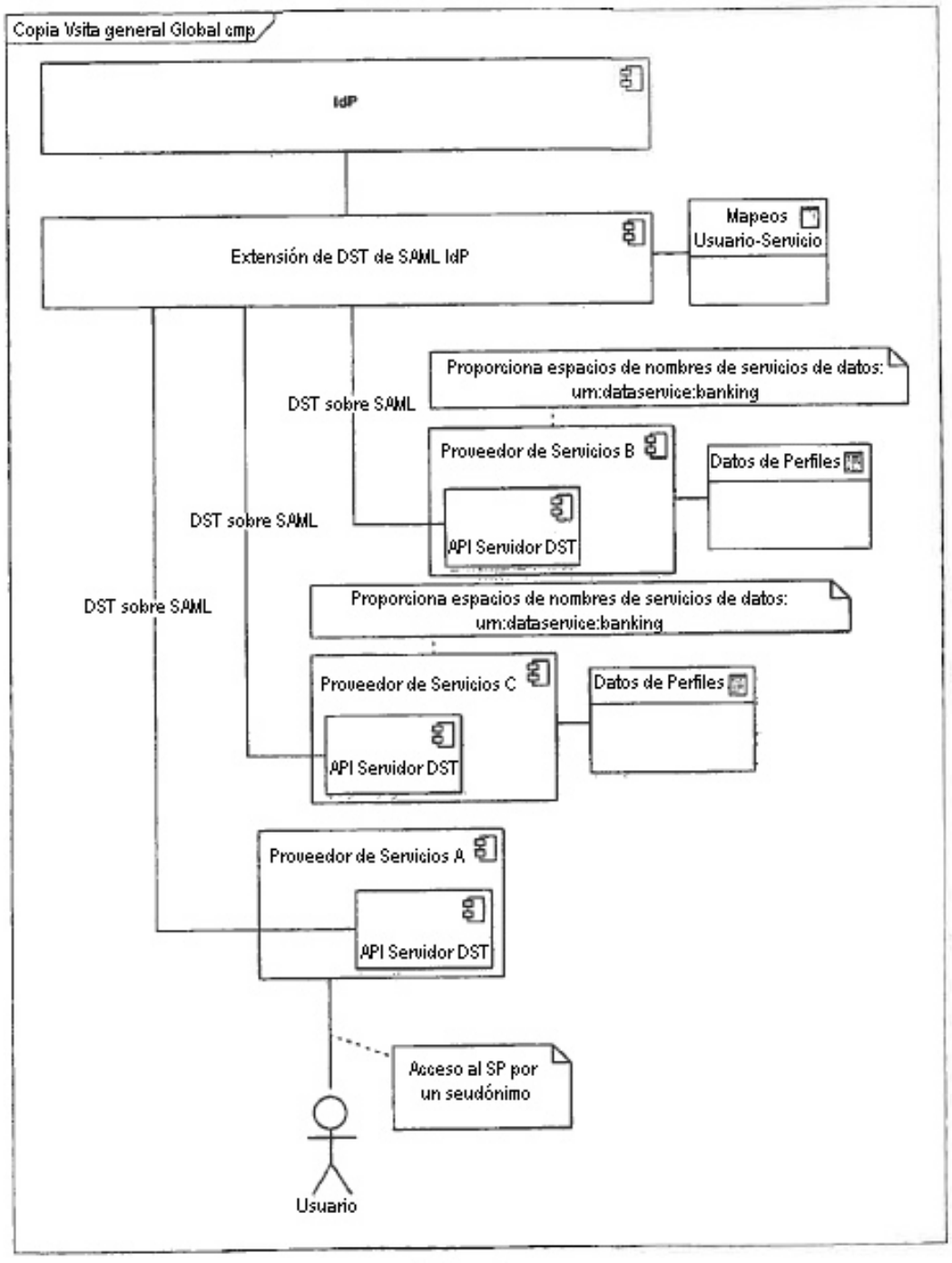
Copia Vsita general Global cmp
IdP
Extensión de DST de SAML IdP
Mapeos Usuario-Servicio
DST sobre SAML
Proporciona espacios de nombres de servicios de datos: um:dataservice:banking
Proveedor de Servicios B
Datos de Perfiles
API Servidor DST
DST sobre SAML
DST sobre SAML
Proporciona espacios de nombres de servicios de datos: um:dataservice:banking
Proveedor de Servicios C
Datos de Perfiles
API Servidor DST
Proveedor de Servicios A
API Servidor DST
Acceso al SP por un seudónimo
Usuario

Fig. 1

7

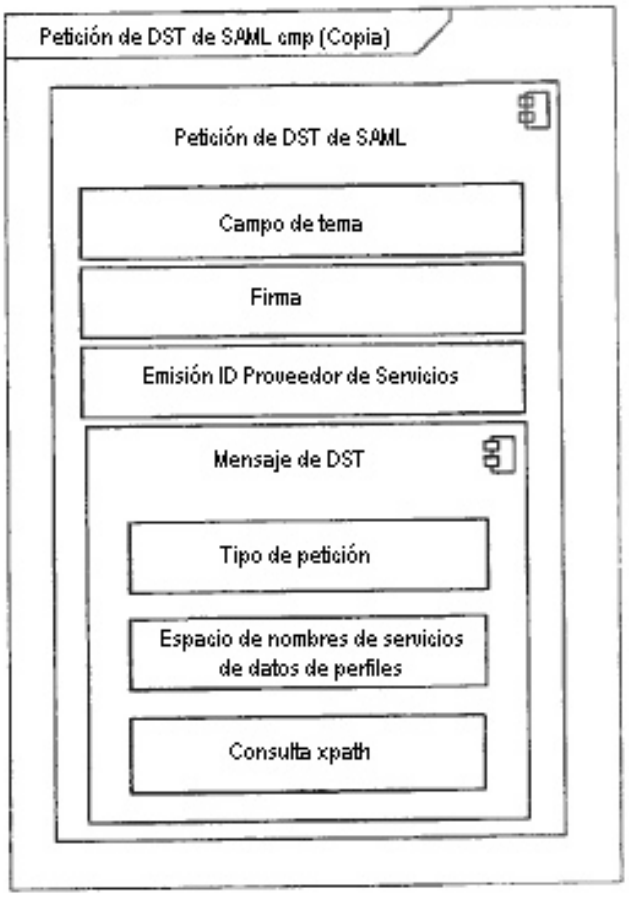
Petición de DST de SAML cmp (Copia)
Petición de DST de SAML
Campo de tema
Firma
Emisión ID Proveedor de Servicios
Mensaje de DST
Tipo de petición
Espacio de nombres de servicios de datos de perfiles
Consulta xpath

Fig. 2

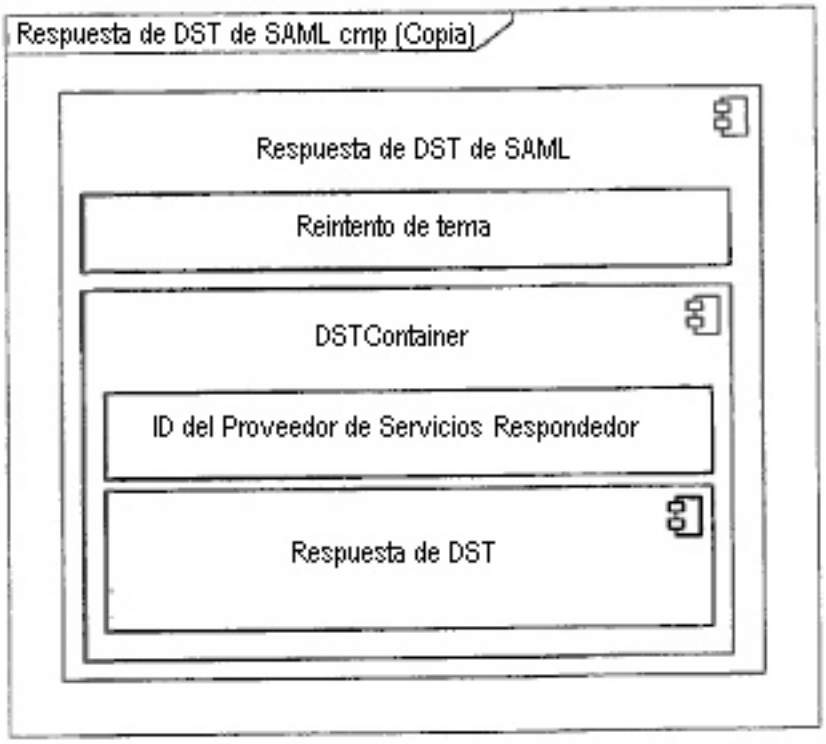
Respuesta de DST de SAML cmp (Copia)
Respuesta de DST de SAML
Reintento de terna
DSTContainer
ID del Proveedor de Servicios Respondedor
Respuesta de DST

Fig. 3

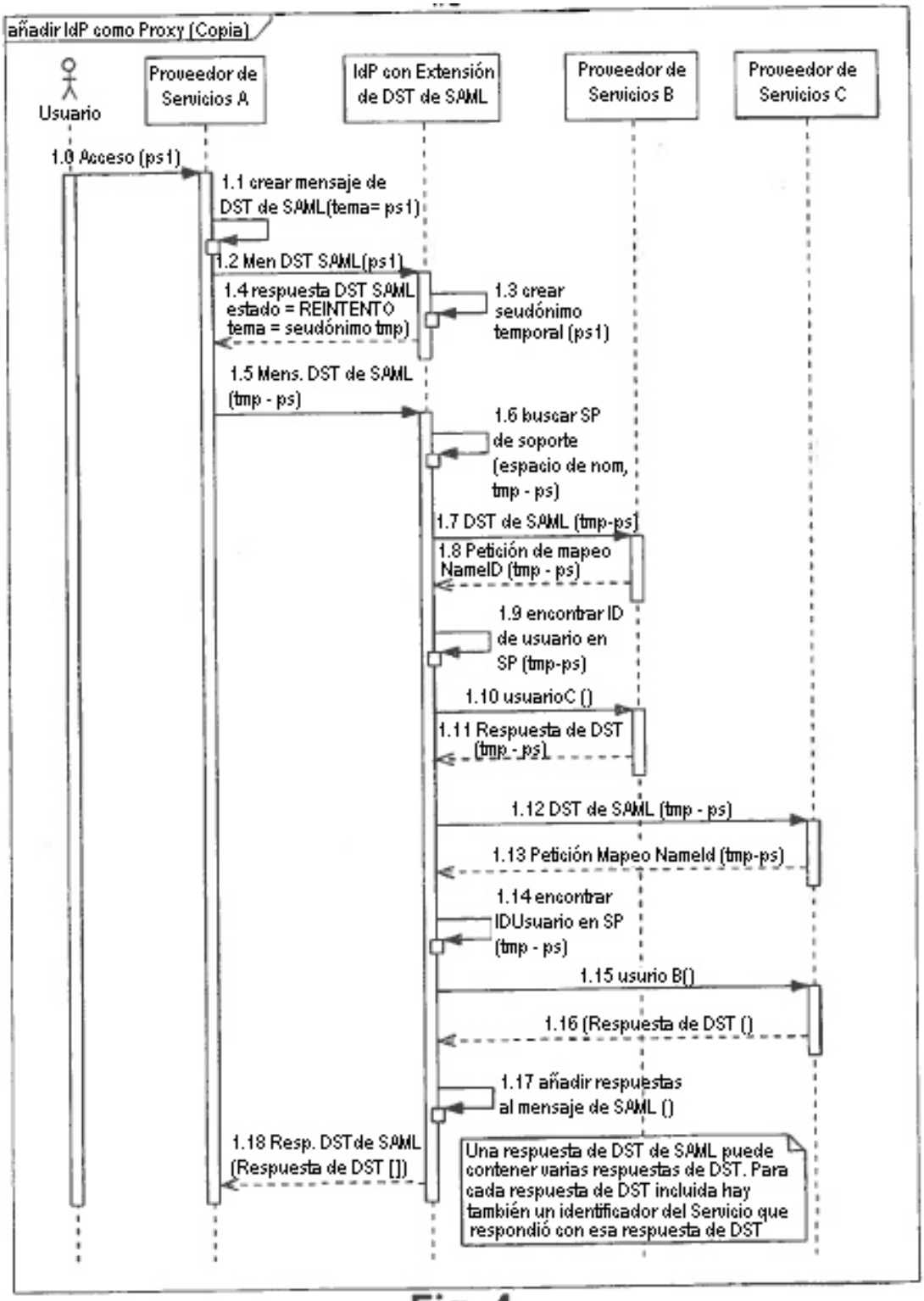
añadir IdP como Proxy (Copia)
Usuario
Proveedor de Servicios A
IdP con Extensión de DST de SAML
Proveedor de Servicios B
Proveedor de Servicios C
1.0 Acceso (ps1)
1.1 crear mensaje de DST de SAML(tema= ps1)
1.2 Men DST SAML(ps1)
1.4 respuesta DST SAML estado = REINTENTO tema = seudónimo tmp)
1.3 crear seudónimo temporal (ps1)
1.5 Mens. DST de SAML (tmp - ps)
1.6 buscar SP de soporte (espacio de nom, tmp - ps)
1.7 DST de SAML (tmp-ps)
1.8 Petición de mapeo NameID (tmp - ps)
1.9 encontrar ID de usuario en SP (tmp-ps)
1.10 usuarioC ()
1.11 Respuesta de DST (tmp - ps)
1.12 DST de SAML (tmp - ps)
1.13 Petición Mapeo NameId (tmp-ps)
1.14 encontrar IDUsuario en SP (tmp - ps)
1.15 usurio B()
1.16 (Respuesta de DST ()
1.17 añadir respuestas al mensaje de SAML ()
1.18 Resp. DSTde SAML (Respuesta de DST [])
Una respuesta de DST de SAML puede contener varias respuestas de DST. Para cada respuesta de DST incluida hay también un identificador del Servicio que respondió con esa respuesta de DST

Fig. 4

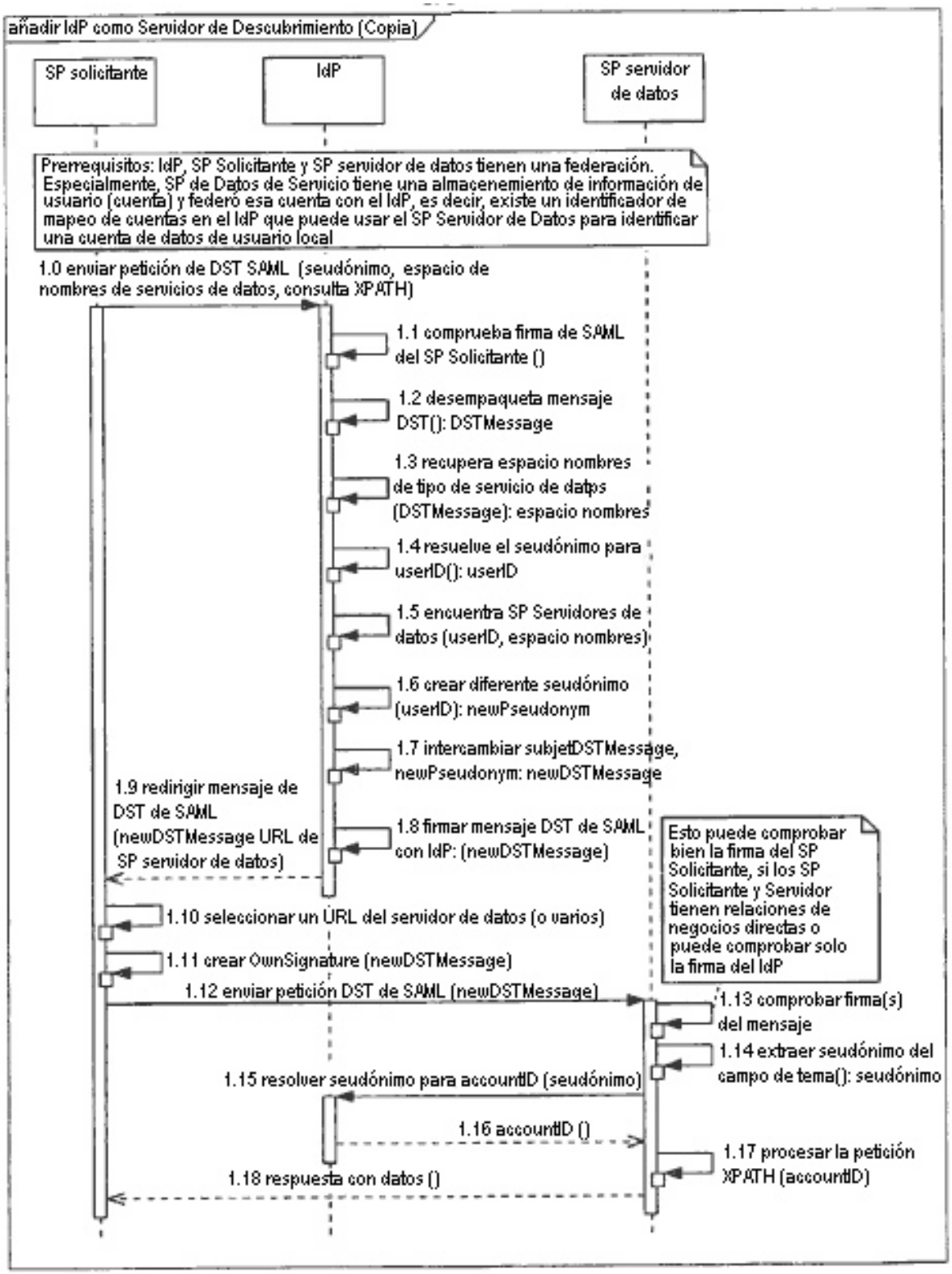
añadir IdP como Servidor de Descubrimiento (Copia)
SP solicitante
IdP
SP servidor de datos
Prerrequisitos: IdP, SP Solicitante y SP servidor de datos tienen una federación. Especialmente, SP de Datos de Servicio tiene una almacenemiento de información de usuario (cuenta) y federó esa cuenta con el IdP, es decir, existe un identificador de mapeo de cuentas en el IdP que puede usar el SP Servidor de Datos para identificar una cuenta de datos de usuario local
1.0 enviar petición de DST SAML (seudónimo, espacio de nombres de servicios de datos, consulta XPATH)
1.1 comprueba firma de SAML del SP Solicitante ()
1.2 desempaqueta mensaje DST(): DSTMessage
1.3 recupera espacio nombres de tipo de servicio de datps (DSTMessage): espacio nombres
1.4 resuelve el seudónimo para userID(): userID
1.5 encuentra SP Servidores de datos (userID, espacio nombres)
1.6 crear diferente seudónimo (userID): newPseudonym
1.7 intercambiar subjetDSTMessage, newPseudonym: newDSTMessage
1.8 firmar mensaje DST de SAML con IdP: (newDSTMessage)
1.9 redirigir mensaje de DST de SAML (newDSTMessage URL de SP servidor de datos)
Esto puede comprobar bien la firma del SP Solicitante, si los SP Solicitante y Servidor tienen relaciones de negocios directas o puede comprobar solo la firma del IdP
1.10 seleccionar un URL del servidor de datos (o varios)
1.11 crear OwnSignature (newDSTMessage)
1.12 enviar petición DST de SAML (newDSTMessage)
1.13 comprobar firma(s) del mensaje
1.14 extraer seudónimo del campo de tema(): seudónimo
1.15 resolver seudónimo para accountID (seudónimo)
1.16 accountID ()
1.17 procesar la petición XPATH (accountID)
1.18 respuesta con datos ()

Fig. 5