(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 427 249**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.03.2011 E 11275058 (3)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2013 EP 2375688**

(54) Título: **Gestión del inicio de sesión automático a recursos objetivo de Internet**

(30) Prioridad:

29.03.2010 ES 201030471

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.10.2013

(73) Titular/es:

VODAFONE GROUP PLC (50.0%)
Group Legal (Patents), The Connection Newbury Berkshire RG14 2FN, GB y
VODAFONE ESPAÑA, S.A.U. (50.0%)

(72) Inventor/es:

CAJIGAS BRINGAS, GUILLERMO;
TOUSET RÍOS, MIGUEL ÁNGEL;
VALVERDE FUSTER, JUAN JOSÉ;
OLIVER RIERA, MIQUEL y
ZUIDWEG ADEMA, JOHAN

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Gestión del inicio de sesión automático a recursos objetivo de Internet

Campo de la invención

La presente invención se incluye en el campo de la tecnología de la información, y más específicamente en el acceso automático de sitios web de Internet que requieren inicio de sesión.

Antecedentes de la invención

Actualmente, una de las frustraciones importantes de los usuarios de Internet es la necesidad de gestionar diferentes identidades de Internet para servicios en línea diferentes, lo cual en la práctica significa recordar muchos nombres de usuario, contraseñas y códigos pin diferentes. El número creciente de aplicaciones y servicios disponibles a partir de dispositivos tanto fijos como móviles demanda una solución para gestionar toda esta información sensible.

Existen soluciones y arquitecturas relacionadas con el uso de identidades, que tratan el Intercambio de identidades en Internet, como las herramientas OpenID, CardSpace, .NET Passport, Sibboleth y Liberty Alliance. Todas ellas se pueden usar únicamente con sitios web y servicios en línea que sean compatibles con estos sistemas. Son herramientas complejas, las cuales se describen detalladamente más adelante, y no están diseñadas para ser usadas con un conjunto telefónico móvil de mano.

Existen dos planteamientos para mejorar la gestión de identidades en Internet: sistemas de *inicio de sesión único* (SSO) y *meta-sistemas de identidades*.

Un sistema de *inicio de sesión único* proporciona a los usuarios una única identidad en Internet que ofrece acceso a múltiples sitios web y servicios en línea. Un *meta-sistema de identidades* permite que un usuario gestione sus múltiples identidades de Internet existentes, y que seleccione la identidad apropiada de acuerdo con el sitio web o servicio solicitado. Shibboleth, OpenID, Liberty y .NET Password son sistemas de *inicio de sesión único*, mientras que Windows CardSpace es un meta-sistema de identidades.

Shibboleth es un sistema de *inicio de sesión único* de código abierto, basado en el Lenguaje de Marcado de Aserción de Seguridad (SAML), una normativa que describe un formato y protocolo XML para intercambiar aserciones de autenticación y autorización entre servidores. La Figura 1 muestra cómo funciona Shibboleth, el flujo de información de Shibboleth.

El procedimiento de inicio de sesión de Shibboleth consta de las siguientes etapas:

S1. El usuario accede a un recurso protegido (denominado Proveedor de Servicios), y solicita una página web.

S2. El Proveedor de Servicios redirecciona al usuario al servicio Where Are You From (WAYF), de manera que pueda seleccionar su organización local (denominada Proveedor de Identidades).

S3. El servicio WAYF redirecciona al usuario a su Proveedor de Identidades.

S4. El usuario se autentica, mediante cualquiera que sea el procedimiento de autenticación que requiera su Proveedor de Identidades.

S5. Después de una autenticación satisfactoria, el Proveedor de Identidades genera un puntero (*handle*) único o identificador de sesión para esta sesión, y redirecciona al usuario al Proveedor de Servicios.

S6. El recurso puede utilizar el puntero para solicitar información de atributos para este usuario, del Proveedor de Identidades (opcional).

S7. El Proveedor de Identidades proporciona o deniega la información de atributos solicitada.

S8. Basándose en la información de autenticación y la información de atributos que se ha puesto a disposición, el Proveedor de Servicios proporciona o deniega al usuario, acceso al recurso solicitado.

En la actualidad, Shibboleth se usa principalmente entre instituciones académicas y centros de investigación. Obsérvese que en Shibboleth, un usuario debe pertenecer a una organización que pueda aseverar su identidad. Una de las características de Shibboleth es que permite una autenticación más fuerte o más débil, en función de los atributos intercambiados entre el Proveedor de Servicios y el Proveedor de Identidades.

OpenID es un sistema de *inicio de sesión único* que permite a usuarios de Internet acceder a sitios web con un único "OpenID". OpenID es un sistema distribuido abierto cuyo uso es gratuito. En principio, cualquier usuario u organización puede convertirse en un Proveedor de OpenID, y un usuario puede seleccionar cualquier Proveedor de OpenID que se adecue a sus necesidades. De hecho, un usuario puede cambiar muy fácilmente de Proveedores de OpenID sin perder su OpenID.

La Figura 2 muestra cómo funciona OpenID. El procedimiento de inicio de sesión de OpenID consta de las siguientes etapas:

S1'. El usuario accede a un sitio web habilitado para OpenID (denominado *Consumidor* en la terminología de OpenID), y el sitio proporciona un formulario que solicita la identidad OpenID del usuario.

S2'. El usuario introduce su OpenID, por ejemplo johan.vodafone-id.com, y presenta el formulario al Consumidor OpenID.

S3'. El Consumidor OpenID convierte el OpenID (por ejemplo, johan.vodafone-id.com) en el formulario normal URI (por ejemplo, http://johan.vodafone-id.com) y efectúa un HTTP GET para este URI.

S4'. El sitio devuelve un documento HTML a partir del cual el Consumidor puede obtener la ubicación del Proveedor de OpenID (obsérvese que, en este ejemplo, son iguales).

S5'. El Consumidor envía un HTTP POST al Proveedor de OpenID con una solicitud asociada. Esto establece un secreto compartido entre el Proveedor y el Consumidor, utilizando el algoritmo Diffie-Hellman.

S6'. El Proveedor de OpenID devuelve un puntero de asociación (con una fecha y hora de expiración fijadas) para ser usado en solicitudes futuras.

S7'. El Consumidor de OpenID redirecciona a continuación al usuario al Proveedor de OpenID para el inicio de sesión.

S8'. El usuario autentica su identidad con el Proveedor de OpenID.

S9'. El Proveedor de OpenID redirecciona al usuario de vuelta al sitio web del Consumidor, proporcionando la verificación de autenticación necesaria en una cadena de consulta.

Aunque el flujo de información de OpenID recuerda al de Shibboleth, existen dos diferencias importantes:

- En OpenID, el usuario asevera su propia identidad, mientras que en Shibboleth es la organización del usuario (el Proveedor de Identidades) la que "es propietaria" de la identidad del usuario.

- Los OpenIDs son persistentes e independientes del Proveedor de OpenID en el que un usuario elige registrarse. En Shibboleth, la identidad de un usuario está vinculada con su organización (que actúa como Proveedor de Identidades).

Esto significa que OpenID tiene ciertas ventajas en términos de apertura y universalidad. Aunque el uso del *inicio de sesión único* en Internet aún no se ha extendido ampliamente, parece como si OpenID estuviera ganando una rápida aceptación. Algunos sitios que aceptan OpenID, o que lo harán en el futuro próximo, incluyen AOL, Yahoo, Flickr, Blogger, Orange, Sun, Novell y Oxfam.

Los críticos argumentan que la implementación actual de OpenID presenta defectos de seguridad. OpenID no ofrece protección contra suplantación de identidades ni contra ataques del tipo hombre en el medio, puesto que la cadena de consulta usada para el inicio de sesión de un usuario en el sitio web del Consumidor se firma con el secreto compartido entre el Consumidor y el Proveedor. No obstante, sigue siendo posible que un Consumidor malintencionado suplante páginas de autenticación del proveedor de OpenID, y que obtenga así la contraseña y las credenciales OpenID de un usuario.

El usuario puede protegerse contra este tipo de ataques registrándose en un proveedor de OpenID seguro que utilice certificados de confianza para acreditar su identidad. Sin embargo, desafortunadamente, el usuario medio en general no tiene conocimiento de cómo funcionan los certificados ni de cómo confiar en (o desconfiar de) ellos.

Liberty Alliance es una arquitectura de gestión completa de identidades que ofrece no solamente un *inicio de sesión único* sino también un cierre de sesión único, federación de identidades y especificaciones de servicios web para construir aplicaciones de identidades con capacidad de interfuncionamiento. Igual que Shibboleth y OpenID, los protocolos de Liberty también se basan en SAML.

Como muestra la Figura 3, el procedimiento de *inicio de sesión único* de Liberty es similar al de Shibboleth y OpenID. El procedimiento de inicio de sesión de Liberty consta de las siguientes etapas:

- S1*. El usuario accede al sitio web de un Proveedor de Servicios que está habilitado para Liberty.

- S2*. El Proveedor de Servicios determina el Proveedor de Identidades del usuario a partir de la solicitud HTTP.

- S3* y S4*. El Proveedor de Servicios redirecciona al usuario al Proveedor de Identidades. El Proveedor de Identidades autentica al usuario.

- S6* y S7*. El Proveedor de Identidades redirecciona al usuario al Proveedor de Servicios con la aserción de su identidad.

- S8* y S9*. El Proveedor de Servicios y el Proveedor de Identidades intercambian punteros.

- S10*. El Proveedor de Servicios asevera el proceso.

- S11*. El Proveedor de Servicios proporciona acceso al usuario.

Liberty Alliance es una iniciativa de la industria a gran escala que se remonta a 1999. Los miembros de Liberty Alliance incluyen proveedores de IT y de telecomunicaciones, bancos y compañías de tarjetas de crédito, y operadores de telecomunicaciones. Entre muchos otros, Vodafone, France Télécom y NTT DoCoMo son miembros de Liberty Alliance.

A pesar de su amplio respaldo industrial y político, el uso de Liberty todavía no se ha extendido de forma amplia en Internet. Liberty parece haber sido aceptada mayormente por grandes organizaciones y organismos gubernamentales, pero no ha penetrado en servicios en línea de tamaño medio y más pequeños, que en la actualidad constituyen la mayor parte de Internet. Los críticos de Liberty Alliance argumentan que esto es debido a la complejidad de la arquitectura y los mecanismos de federación de Liberty. Aunque Liberty sí proporciona efectivamente una arquitectura completa para la gestión de identidades, esto parece ser excesivo para la mayoría de sitios web "comunes" que desean ofrecer un *inicio de sesión único*.

".NET Passport" es el sistema de *inicio de sesión único* de Microsoft. .NET Passport entrega al usuario una "*Windows Live Id*" que puede utilizarse en todos los servicios de Microsoft así como en algunos otros sitios. Igual que OpenID, .NET Passport solamente autentica identidades de usuario, no autoriza el acceso de usuarios a páginas web.

En la actualidad, .NET Passport y Windows Live Ids parecen usarse mayormente para servicios relacionados con Microsoft. Aunque algunos otros sitios web ofrecen autenticación basada en .NET Passport, el uso de Windows Live Id no se ha extendido ampliamente más allá de sitios web y servicios en línea de Microsoft.

La forma de funcionar de .NET Passport es similar a cómo funciona OpenID, tal como se ilustra en la Figura 4: cuando el usuario inicia una sesión en una página que está habilitada para Passport, su navegador es redireccionado a un sitio de .NET Passport que autenticará al usuario. Si el usuario se autentica satisfactoriamente, el sitio de .NET Passport envía la información de autenticación de vuelta al navegador del usuario en forma de una cadena de consulta cifrada y *cookies*; a continuación, el navegador del usuario reenvía esta información al sitio original para su autorización. Tal como se muestra en la Figura 4, el procedimiento de .NET Passport consta de las siguientes etapas:

- S1". El navegador del usuario envía una solicitud de página inicial al sitio participante.

- S2". Redireccionamiento para su autenticación.

- S3". El navegador del usuario envía una solicitud de página de inicio de sesión al sitio *passport*.

- S4". El navegador del usuario obtiene la página de inicio de sesión a partir del sitio *passport*.

- S5". Enviar credenciales de usuario al sitio *passport*.

- S6". Actualizar *cookies* de passport.com del navegador del usuario y redireccionamiento al sitio participante.

- S7". Enviar cadena de consulta de autenticación cifrada al sitio participante.

- S8". El navegador del usuario recibe *cookies* del sitio y la página solicitada a partir del sitio participante.

.NET Passport difiere con respecto OpenID en la manera que se gestionan los punteros a la página solicitada. En .NET existe principalmente un proveedor de identidades (Microsoft), de modo que resulta innecesario establecer un secreto compartido y asociar punteros como parte del flujo de inicio de sesión. En .NET Passport toda la comunicación pasa a través del navegador del usuario.

Sin embargo, la diferencia más importante reside en el hecho de que OpenID es un sistema abierto que soporta una gestión distribuida de identidades, mientras que los *Windows Live Ids* son gestionados principalmente por Microsoft.

La mayoría de los *meta-sistemas de identidades*, y muy especialmente Windows CardSpace, se basan en variaciones del concepto de *tarjeta de información*. Una *tarjeta de información* es un contenedor para la identidad de un usuario de Internet, emitida por un tercero de confianza, que puede presentarse a un sitio web o servicio en línea que solicite autenticación. Se representa gráficamente en el ordenador del usuario como una Tarjeta de identidad. Una tarjeta de información puede ser configurada por el propio usuario, aunque también puede proporcionar un certificado digital emitido por uno de los terceros de confianza con el que tenga relación el usuario.

Obsérvese que la tarjeta de información solamente sirve como selector de identidad, no es en sí misma un sistema de *inicio de sesión único* como OpenID, Liberty Alliance o .NET Passport.

El documento EP1919156 constituye además técnica anterior.

La presente invención soluciona los problemas comentados sobre los sistemas anteriores proporcionando un sistema y un método que habilitan el uso de un conjunto telefónico móvil de mano para iniciar fácilmente una sesión en un sitio web de Internet y no tener que recordar un número elevado de tuplas de nombre de usuario-contraseña. El objetivo del presente sistema, Dial Your Identity (Marca Tu Identidad; en adelante, DYI), es permitir que usuarios gestionen y usen las identidades que necesitan en su navegación regular en Internet con sus teléfonos móviles, ampliando el uso del teléfono móvil para proporcionar servicios más allá de comunicaciones básicas. Por lo tanto, el sistema propuesto en la presente invención proporciona a un usuario una manera sencilla de gestionar y utilizar sus identidades de Internet (pares de nombre de usuario-contraseña) utilizando su conjunto telefónico móvil de mano, de manera que se ofrece una forma muy fácil de iniciar sesión en sitios web de Internet.

Descripción de la invención

La invención se refiere a un sistema para gestionar el inicio de sesión automático en recursos objetivo de Internet según la reivindicación 1, y a un método correspondiente según la reivindicación 9. En las reivindicaciones dependientes se definen realizaciones preferidas del sistema y del método.

El sistema comprende:

- un teléfono móvil, provisto de un dispositivo de almacenamiento en el cual se almacenan identidades privadas de usuario;

- un servidor de identificación;

- un ordenador provisto de un navegador de cliente con un complemento (*plug-in*) de navegador, estando configurado el complemento de navegador para, al producirse la recepción de información que contiene un formulario de inicio de sesión enviado por un recurso objetivo al cual está accediendo un usuario del navegador de cliente:

  • detectar el formulario de inicio de sesión contenido en la información recibida;

  • solicitar el usuario, y por consiguiente obtener, un identificador de usuario;

  • enviar una solicitud de identidad destinada a llegar al servidor de identificación, incluyendo dicha solicitud de identidad por lo menos el identificador de usuario;

El servidor de identificación está configurado, al producirse la recepción del identificador de usuario, para:

  • obtener un número de teléfono móvil asociado a dicho identificador de usuario;

  • enviar un mensaje de identidad destinado al teléfono móvil, conteniendo el mensaje de identidad un identificador del recurso objetivo;

El teléfono móvil está provisto de una aplicación de cliente configurada para, al producirse la recepción de un mensaje de identidad:

  • buscar las identidades privadas de usuario asociadas al recurso objetivo en el dispositivo de almacenamiento;

  • si se halla por lo menos una identidad privada de usuario asociada, solicitar al teléfono móvil, confirmación de usuario para iniciar automáticamente una sesión en el recurso objetivo utilizando una identidad privada de usuario seleccionada a partir de dicha por lo menos una identidad privada de usuario asociada;

  • si se produce una confirmación para el inicio de sesión automático, enviar dicha confirmación y la identidad privada de usuario seleccionada al servidor de identificación;

El servidor de identificación está configurado además, si se recibe la confirmación para el inicio de sesión automático, para enviar la identidad privada de usuario seleccionada al navegador de cliente; el complemento de navegador está configurado además para, al producirse la recepción de la identidad privada de usuario seleccionada, iniciar sesión en el recurso objetivo usando dicha identidad privada de usuario seleccionada.

En una realización preferida, la solicitud de identidad incluye además un identificador del recurso objetivo al que se está accediendo, y el complemento de navegador está configurado para enviar la solicitud de identidad directamente al servidor de identificación.

El recurso objetivo puede estar habilitado para OpenID. En ese caso, el complemento de navegador está configurado preferentemente para enviar la solicitud de identidad destinada a llegar al servidor de identificación a través del recurso objetivo.

La aplicación de cliente puede estar configurada además para, en caso de que se halle una pluralidad de identidades privadas de usuario asociadas al recurso objetivo, solicitar al usuario que seleccione una identidad privada de usuario a enviar al servidor de identificación.

La aplicación de cliente está asociada preferentemente a por lo menos un puerto del teléfono móvil, y el teléfono móvil puede estar configurado para, al producirse la recepción de un mensaje de identidad recibido en un puerto predeterminado asociado a la aplicación de cliente, ejecutar la aplicación de cliente, si es que no se está ejecutando todavía.

Cada comunicación que se origina en el servidor de identificación y que está destinada al teléfono móvil se lleva a cabo preferentemente a través del envío de por lo menos un mensaje SMS.

En una realización preferida el teléfono móvil tiene capacidad de acceso inalámbrico a Internet, y cada comunicación que se origina desde el teléfono móvil y está destinada al servidor de identificación se lleva a cabo a través del envío de por lo menos un mensaje HTTP.

Cada comunicación entre el ordenador y el servidor de identificación, en ambas direcciones, se lleva a cabo preferentemente a través de por lo menos un mensaje HTTP.

Según otro aspecto de la presente invención, se proporciona un método para gestionar el inicio de sesión automático en recursos objetivo de Internet, cuando un ordenador provisto de un navegador de cliente accede a un recurso objetivo que requiere inicio de sesión.

El método comprende:

- detectar, al producirse la recepción de información que contiene un formulario de inicio de sesión enviado por el recurso objetivo al cual un usuario del navegador de cliente está accediendo, el formulario de inicio de sesión contenido en la información recibida;

- solicitar el usuario, y por consiguiente obtener, un identificador de usuario;

- enviar una solicitud de identidad destinada a llegar a un servidor de identificación, incluyendo dicha solicitud de identidad por lo menos el identificador de usuario;

- obtener, al producirse la recepción del identificador de usuario, un número de teléfono móvil asociado a dicho identificador de usuario;

- enviar un mensaje de identidad destinado al teléfono móvil con dicho número de teléfono móvil, conteniendo el mensaje de identidad un identificador del recurso objetivo;

- buscar, al producirse la recepción del mensaje de identidad, las identidades privadas de usuario asociadas al recurso objetivo en un dispositivo de almacenamiento del teléfono móvil;

- si se halla por lo menos una identidad privada de usuario asociada, solicitar al teléfono móvil una confirmación de usuario para iniciar una sesión de manera automática en el recurso objetivo utilizando una identidad privada de usuario seleccionada a partir de dicha por lo menos una identidad privada de usuario asociada;

- si se produce una confirmación para el inicio de sesión automático, enviar dicha confirmación y la identidad privada de usuario seleccionada al servidor de identificación;

- si el servidor de identificación recibe confirmación para el inicio de sesión automático, enviar la identidad privada de usuario seleccionada al navegador de cliente;

- iniciar sesión, al producirse la recepción de la identidad privada de usuario seleccionada, en el recurso objetivo usando dicha identidad privada de usuario seleccionada.

El método puede comprender además, en caso de que se halle una pluralidad de identidades privadas de usuario asociadas al recurso objetivo, solicitar al usuario que seleccione una identidad privada de usuario a enviar al servidor de identificación.

Breve descripción de los dibujos

A continuación se describe de forma muy breve una serie de dibujos que ayudan a entender mejor la invención y que están expresamente relacionados con una realización de dicha invención, presentada como ejemplo no limitativo de la misma.

La Figura 1 muestra el flujo de información del sistema de inicio de sesión Shibboleth, según la técnica anterior.

La Figura 2 muestra el flujo de información del sistema de inicio de sesión OpenID, según la técnica anterior.

La Figura 3 muestra el flujo de información del sistema de inicio de sesión Liberty, según la técnica anterior.

La Figura 4 muestra el procedimiento de autenticación del sistema de inicio de sesión .NET Passport, según la técnica anterior.

La Figura 5 representa de manera esquemática el sistema según la presente invención.

La Figura 6 muestra de manera esquemática los componentes lógicos del sistema.

Las Figuras 7 y 8 muestran el flujo de inicio de sesión automático llevado a cabo por el complemento de navegador.

La Figura 9 representa gráficamente el flujo de gestión de identidades de Internet.

La Figura 10 muestra el funcionamiento de la invención como sistema de *inicio de sesión único*, utilizando OpenID.

Descripción de una realización preferida de la invención

Según un aspecto de la presente invención, se proporciona un sistema para gestionar diferentes identidades privadas del usuario para servicios de Internet, al que se denominará de aquí en adelante sistema DYI (Dial Your Identity). El sistema comprende los siguientes componentes, tal como se ilustra en la Figura 5:

- Un ordenador 1 (normalmente un ordenador de cliente): un anfitrión en Internet con la capacidad de actuar como cliente HTTP. Idealmente, el usuario debería poder usar el DYI desde cualquier anfitrión en Internet, incluyendo PCs compartidos en cibercafés, áreas WiFi públicas, etcétera. Se supone que estos anfitriones tienen conexiones a Internet que no son de confianza.

- Un teléfono móvil 2: el teléfono móvil del usuario con una tarjeta SIM (Módulo de Identificación de Abonado). Cualquier terminal electrónico provisto de una tarjeta SIM o U/SIM y con conexión a la red de móviles se considera como teléfono móvil en la totalidad de la presente descripción. No existen restricciones sobre el teléfono aparte de que debe poder ejecutar la aplicación 20 de cliente representada en la Figura 6 (por ejemplo, aplicaciones J2ME -Java), y que debe poder conectarse a Internet. El requisito del teléfono móvil es que pueda ejecutar algún tipo de software que se pueda descargar en el mismo, por lo que el teléfono móvil debería disponer de funcionalidades mínimas de apertura con el fin de ejecutar software externo. La mayoría de teléfonos móviles actualmente dispone de mecanismos de plataforma de Dispositivo Móvil de Internet (MID) que soportan aplicaciones J2ME.

- Servidor 4 de identificación: un servidor o grupo que implemente el lado de la aplicación DYI correspondiente a la red.

El sistema interacciona con un recurso objetivo 3, el cual es cualquier recurso objetivo HTTP en Internet para el cual se requiere autenticación, típicamente un sitio web que requiere inicio de sesión.

Aunque la Figura 5 muestra el servidor 4 de identificación como un solo componente, el mismo se podría dividir ciertamente en varios sistemas físicos. El sistema en conjunto aloja múltiples funcionalidades:

• Servidor HTTP: Aloja un sistema para que el usuario gestione (cargue, edite, elimine, etcétera) su identidad. En el presente caso, pares de nombre de usuario/contraseña utilizados por el usuario en sus accesos regulares a servicios de Internet. El sistema no los almacena.

• Implementa la lógica del lado del servidor DYI - la lógica del lado de la red.

• Servidor de aplicación: El sistema permite que el usuario descargue software de cliente necesario para el teléfono y para el navegador de Internet.

• Proxy HTTP: en uno de los escenarios considerados, el servidor de identificación también actúa como un proxy HTTP.

En la Figura 6 se ilustra la arquitectura global de una realización preferida del sistema, y la misma tiene los siguientes componentes lógicos:

- El teléfono móvil 2 contiene una aplicación 20 de cliente, la cual accede a las identidades de usuario almacenadas en el dispositivo 21 de almacenamiento (por ejemplo, en la tarjeta SIM). El usuario deberá instalar la aplicación 20 de cliente (normalmente descargada de forma previa desde el operador de la red móvil) antes de usar el sistema DYI. Dicha descarga es sencilla, y consiste simplemente en descargar e instalar archivos (por ejemplo, archivos .jar/.jad) por vía aérea desde un URL público, por medio de Push WAP o desde un ordenador personal. Evidentemente, esto requiere que el teléfono móvil del cliente tenga la capacidad de ejecutar aplicaciones Java (más del 80% de teléfonos móviles disponibles en la actualidad soportan aplicaciones Java).

- El ordenador 1 contiene un navegador 10 de cliente HTTP convencional con una extensión o complemento 11 de navegador que recupera las identidades de usuario y lleva a cabo un inicio de sesión automático en recursos objetivo 3. El usuario deberá descargar e instalar el complemento 11 de navegador antes de usar el sistema DYI. No obstante,

dicho procedimiento de descarga es muy sencillo, e idéntico a la descarga e instalación de otros complementos (por ejemplo, un reproductor Flash o una barra de herramientas).

- El servidor 4 de identificación contiene un servidor HTTP 41 que gestiona solicitudes de gestión de identidades y una aplicación 40 de servidor. La aplicación de servidor tiene dos funciones principales: recuperar identidades de usuario desde el teléfono móvil de un usuario cuando se requiere un inicio de sesión automático y gestionar identidades de usuario en línea a través de HTTP.

El recurso objetivo 3, el cual no forma parte del sistema, comprende un servidor HTTP 31 y una base 30 de datos con información personalizada para la cual se requiere autenticación (por ejemplo, Facebook, un blog, correo electrónico, información de cuentas bancarias).

La Figura 6 también muestra las interfaces entre los componentes lógicos:

• I1: la interfaz, en la red móvil, entre la aplicación 20 de cliente y la aplicación 40 de servidor.

• I2: la interfaz entre el complemento 11 de navegador y la aplicación 40 de servidor, que usa el transporte TCP/IP convencional a través del servicio público de Internet.

• I3: la interfaz entre el navegador 10 de cliente y el servidor HTTP 41.

• I4: la interfaz entre el navegador 10 de cliente y el recurso objetivo 3.

Las interfaces I2, I3 e I4 utilizan el transporte TCP/IP convencional a través del servicio público de Internet. Estas interfaces transportan solicitudes y respuestas HTTP convencionales.

La interfaz I1 es la interfaz más compleja del sistema. Los mensajes provenientes de la aplicación de servidor que se ejecuta en el servidor 4 de identificación hacia la aplicación 20 de cliente en el teléfono móvil se transportan a través de SMS, mientras que los mensajes en la dirección opuesta se transportan preferentemente a través de TCP/IP por vía aérea (GPRS). Este mecanismo es similar a la forma de funcionamiento del Push WAP. Es necesario implementar esta interfaz de este modo, ya que el teléfono móvil solamente puede actuar como cliente HTTP y no puede prestar servicio a solicitudes HTTP. Los SMS no son solamente un mecanismo de texto entre teléfonos móviles sino también un mecanismo asíncrono de alerta de facto que es aceptado por todos los conjuntos telefónicos móviles de mano.

El sistema DYI tiene dos modos de funcionamiento:

1. Sistema de gestión de identidades: permite que el usuario inicie de manera automática una sesión en cualquier sitio web utilizando sus identidades de Internet existentes, utilizando el teléfono móvil como dispositivo de selección y gestión de identidades.

2. Sistema de *inicio de sesión único*: permite que el usuario inicie una sesión en sitios web habilitados para OpenID utilizando su OpenID, con lo cual el servidor de identificación del operador de la red móvil actúa como Proveedor de Identidades y el teléfono móvil se usa como dispositivo de autenticación. La presente invención también puede funcionar utilizando otros sistemas de inicio de sesión único, tales como .NET Passport, Shibboleth y Liberty.

1. Sistema de gestión de identidades

Los flujos de información entre los componentes de la arquitectura en caso de que el servicio de DYI funcione como un sistema de gestión de identidades son los siguientes (flujo para selección de identidad e inicio de sesión automático).

El complemento 11 de navegador en el ordenador 1 detecta de forma automática páginas de inicio de sesión, recupera la identidad de usuario relevante a partir del teléfono móvil del usuario, y a continuación efectúa automáticamente el inicio de sesión para el usuario en el recurso objetivo.

Este procedimiento es similar a la forma en la que navegadores convencionales tales como el Explorer de Windows y Firefox recuerdan de hecho nombres de usuario y contraseñas y los usan de manera automática para el inicio de sesión de un usuario. La diferencia principal es que en el caso del sistema DYI, las identidades del usuario se almacenan en el teléfono móvil del usuario y no en el navegador o un complemento (este último añade movilidad y elimina restricciones de acceso en la medida en que Firefox® y Explorer® de Windows solamente recuperan la contraseña que reside únicamente en el propio ordenador que están utilizando).

La Figura 7 muestra el flujo propuesto:

• Desde el ordenador 1, el usuario final solicita 100 (por ejemplo, a través de "HTTP GET recurso objetivo") conexión a (o información de) un recurso objetivo 3 que requiere inicio de sesión. El recurso objetivo 3 devuelve 101 un formulario de inicio de sesión (por ejemplo, a través de "200 OK [página de inicio de sesión]"). Esta es una solicitud-respuesta HTTP convencional.

• El complemento 11 de navegador en el ordenador 1 reconoce el formulario de inicio de sesión y solicita (102) un identificador de usuario (por ejemplo, identidad OpenID, número de teléfono móvil del usuario, etcétera) a través de una ventana emergente, véase la Figura 8. El complemento 11 de navegador en el ordenador 1 a continuación envía 103 una solicitud de identidad (por ejemplo, por medio de un mensaje “HTTP GET identidad [recurso objetivo, identificador de usuario]") al servidor 4 de identificación para que la identidad privada del usuario inicie sesión en el recurso objetivo 3. Esta es una solicitud HTTP convencional que transporta una identificación del recurso objetivo (el URL de la página de inicio de sesión) y el identificador de usuario.

• Con el identificador de usuario, el servidor 4 de identificación recupera el número de teléfono móvil del usuario (habitualmente buscando el número de teléfono almacenado en una base de datos, puesto que el servidor 4 de identificación forma parte preferentemente de la red de móviles; de hecho, el identificador de usuario podría ser el propio número de teléfono), y envía una solicitud 105 (por ejemplo, a través de un SMS:puerto x [recurso objetivo, identificador de usuario]) al teléfono móvil 2 del usuario para que la identidad privada de usuario que se requiere que inicie sesión en el recurso objetivo 3. Esta solicitud 105 se envía preferentemente en forma de SMS (en un puerto x predeterminado) que contiene una identificación del recurso objetivo 3 para el cual se requiere una identidad privada de usuario y una dirección de retrollamada (por ejemplo, un URL).

• Al producirse la recepción del SMS (en el puerto x predeterminado), el teléfono móvil detecta dicho mensaje en el puerto x y ejecuta la aplicación 20 de cliente (que está asociada al puerto x), si no se está ejecutando todavía. La aplicación 20 de cliente en el teléfono del usuario despliega 106 un artilugio (*widget*) que invita al usuario a seleccionar una identidad de usuario privada (si existen múltiples opciones, por ejemplo cuando se utiliza una pluralidad de cuentas de correo electrónico con diferentes nombres de usuario y contraseñas) y a confirmar el inicio de sesión automático en el recurso objetivo 3.

• Cuando el usuario ha seleccionado una identidad y ha confirmado que desea llevar a cabo el inicio de sesión automático, el cliente 20 de aplicación en el teléfono del usuario envía 108 la identidad de usuario particular al servidor 4 de identificación utilizando un mensaje HTTP POST (que incluye el nombre de usuario y la contraseña de la identidad privada de usuario asociada al recurso objetivo 3 solicitado). El cliente 20 de aplicación puede recuperar las identidades de usuario accediendo al dispositivo 21 de almacenamiento (SIM o memoria del teléfono) en el cual se almacenan las identidades.

• El servidor 4 de identificación reenvía 109 (por ejemplo, por medio de un mensaje HTTP "200 OK [nombre de usuario, contraseña]") la identidad privada de usuario (nombre de usuario y contraseña) al complemento 11 de navegador en el ordenador 1. Esta es una respuesta HTTP convencional a la solicitud 103 anterior.

• Utilizando la identidad privada de usuario recibida, el complemento 11 de navegador inicia sesión 110 de manera automática en el recurso objetivo 3. Este es el mismo mecanismo que usan los navegadores web convencionales para soportar el inicio de sesión automático (por medio de un mensaje "HTTP POST" que incluye nombre de usuario y contraseña, los cuales están contenidos en la identidad de usuario particular). El recurso objetivo 3 envía entonces el recurso protegido al ordenador 1 (por ejemplo, por medio de "200 OK [recurso protegido]").

El SMS transporta, en la etapa 105, la dirección de retrollamada, es decir el URL hacia el que debe efectuar un POST de su respuesta la aplicación 20 de cliente en el teléfono móvil 2 del usuario. Esto permite que el servidor de identificación correlacione la respuesta (SMS) con la solicitud (HTTP POST).

Si no existe ninguna identidad privada de usuario almacenada en el teléfono móvil 2 del usuario para un recurso objetivo 3 particular, entonces hay dos opciones alternativas de implementación:

- La aplicación 20 de cliente en el teléfono móvil 2 abre un artilugio para pedirle al usuario la identidad privada de usuario (típicamente, nombre de usuario y contraseña) para el recurso objetivo 3 en cuestión, la almacena en el dispositivo 21 de almacenamiento (por ejemplo, la tarjeta SIM) y la envía 108 de vuelta al servidor 4 de identificación.

- La aplicación 20 de cliente en el teléfono móvil 2 no despliega ningún artilugio, pero devuelve un mensaje que indica que no se ha hallado ninguna id de usuario particular para el recurso objetivo 3 en cuestión. Este mensaje es reenviado al complemento 11 de navegador en el ordenador 1, el cual informa al usuario que no es posible un inicio de sesión automático, e invita al usuario a efectuar un inicio de sesión manual. Cuando el usuario lleva a cabo un inicio de sesión manual, el complemento 11 de navegador registra la identidad de usuario y la envía al servidor 4 de identificación, el cual a su vez la reenvía al teléfono móvil 2 del usuario por medio de SMS de manera que se pueda almacenar en la tarjeta SIM (la Figura 7 no muestra este escenario).

Estas dos opciones alternativas de implementación también pueden combinarse en un escenario en el que el usuario puede introducir la identidad de usuario nueva o bien en su teléfono móvil (a través de un artilugio en el teléfono móvil 2) o bien a través de el ordenador 1.

La Figura 8 ilustra el proceso para inicio de sesión automático mostrando los elementos del sistema de manera similar a la Figura 5.

El sistema DYI también permite gestionar las identidades de Internet. En particular, un usuario debería poder añadir identidades de Internet, eliminarlas y editarlas.

Una premisa importante es que se espera que el sistema DYI almacene la identidad de Internet de un usuario en su tarjeta SIM o en la memoria interna del teléfono móvil.

El usuario podrá gestionar sus identidades de dos maneras diferentes:

- Directamente en el teléfono móvil. Esto requiere algo más que una simple aplicación J2ME en el teléfono que proporciona un artilugio a las identidades de Internet almacenadas en el SIM o en la memoria interna del teléfono móvil. Este primer escenario es una aplicación local en el teléfono y no conlleva ningún flujo de información entre los componentes de la arquitectura.

- Por medio de la web del servidor de identificación. Puesto que la pantalla y el teclado del teléfono móvil 2 son en ocasiones demasiado pequeños para introducir o editar datos, un usuario podría preferir gestionar sus identidades por medio de una interfaz web.

Puesto que las identidades del usuario están almacenadas localmente en el SIM o en la memoria del teléfono móvil, el segundo escenario no es trivial y requiere sincronización entre la web del servidor de identificación y el teléfono móvil del usuario. Puede que las identidades del usuario tengan que almacenarse de forma temporal en el servidor 4 de identificación durante el tiempo que dure la sesión de gestión. La Figura 9 muestra el flujo propuesto. Obsérvese que este flujo requiere inicio de sesión (descrito en el punto anterior 1.2) antes de la propia sesión de gestión de identidades.

• El usuario inicia sesión 300 en el servidor 4 de identificación, siguiendo el procedimiento antes descrito.

• El usuario hace clic en un enlace para solicitar 301 la página de gestión de identidades a partir del servidor.

• El servidor 4 de identificación solicita 302 las identidades de Internet del usuario, almacenadas en el teléfono móvil 2 del usuario. Esto es, esencialmente, una acción de sincronización que puede lograrse o bien mediante un protocolo de sincronización tal como el SYNCML, o bien de una manera más simple mediante un intercambio de mensajes cortos.

• El teléfono móvil 2 del usuario devuelve 303 las identidades de Internet del usuario, utilizando el protocolo de sincronización o el intercambio de mensajes cortos antes mencionado. Las identidades de Internet del usuario deberán cifrarse por seguridad. Se almacenan de forma temporal en el servidor 4 de identificación para permitir su edición en línea.

• El usuario a continuación edita 304 sus identidades de Internet a través de un intercambio HTTP normal (esto puede conllevar un procesado de JavaScript o de formularios).

• Cuando el usuario ha finalizado la edición, hace clic en un botón para actualizar las identidades en su teléfono móvil 2. Esta acción da como resultado que se envíe 305 un mensaje HTTP POST al servidor 4 de identificación.

• El servidor 4 de identificación envía 306 las identidades de Internet actualizadas al teléfono móvil 2, o bien mediante protocolo de sincronización o bien mediante un intercambio de mensajes cortos, tal como se ha indicado anteriormente.

• El teléfono móvil 2 confirma 307 la actualización (esto o bien forma parte del protocolo de sincronización, o bien es un mensaje corto explícito).

• Finalmente, el servidor 4 de identificación devuelve 308 una página de confirmación al usuario.

2. Inicio de sesión único basado en OpenID

La Figura 10 muestra el funcionamiento del servicio DYI como sistema de inicio de sesión único, que permite al usuario iniciar sesión en sitios web habilitados para OpenID utilizando su OpenID. Este flujo se ajusta al procedimiento de inicio de sesión OpenID convencional, con excepción de la autenticación de usuario, que en este caso se realiza por medio del teléfono móvil.

• El usuario accede 400 a un recurso objetivo 3 habilitado para OpenID (o sitio web objetivo, denominado consumidor en la terminología OpenID).

• El recurso objetivo 3 proporciona 401 un formulario solicitando la identidad OpenID del usuario.

• El usuario introduce su OpenID y presenta 402 el formulario al Consumidor de OpenID.

• El recurso objetivo 3 envía una solicitud asociada al servidor 4 de identificación y los dos intercambian 403 un secreto compartido utilizando el algoritmo Diffie-Hellman.

• El recurso objetivo 3 redirecciona 404 al usuario al servidor 4 de identificación para el inicio de sesión.

• El servidor 4 de identificación envía 405 un mensaje que abre un artilugio de autenticación en el teléfono móvil del usuario y solicita autenticación.

• El usuario se autentica 406 con el servidor 4 de identificación por medio de la conexión móvil.

• El servidor 4 de identificación redirecciona 407 al usuario de vuelta al sitio web objetivo 4, proporcionando las credenciales de autenticación necesarias en una cadena de consulta.

Todas las etapas, a excepción de las etapas 405 y 406, son interacciones OpenID convencionales, según especifica la normativa OpenID. OpenID no impone ningún mecanismo de autenticación específico, de manera que es posible autenticar un usuario a través del teléfono móvil sin violar la normativa OpenID.

Este escenario no introduce ningún requisito nuevo en sitios web, ni en ningún proveedor de OpenID. De esta manera un usuario podrá acceder a cualquier sitio web habilitado para OpenID sin ninguna modificación.

REIVINDICACIONES

1. Sistema para gestionar el inicio de sesión automático en recursos objetivo de Internet, caracterizado porque comprende:

- un teléfono móvil (2), provisto de un dispositivo (21) de almacenamiento en el cual están almacenadas identidades privadas de usuario;

- un servidor (4) de identificación;

- un ordenador (1) provisto de un navegador (10) de cliente con un complemento (11) de navegador, estando configurado el complemento de navegador para, al producirse la recepción (101, 401) de información que contiene un formulario de inicio de sesión enviado por un recurso objetivo (3) al cual está accediendo un usuario del navegador (10) de cliente:

  • detectar el formulario de inicio de sesión contenido en la información recibida;

  • solicitar (102) el usuario, y por consiguiente obtener, un identificador de usuario;

  • enviar (103, 402) una solicitud de identidad destinada a llegar al servidor (4) de identificación, incluyendo dicha solicitud (103, 402) de identidad por lo menos el identificador de usuario;

estando configurado el servidor (4) de identificación para, al producirse la recepción del identificador de usuario:

  • obtener un número de teléfono móvil asociado a dicho identificador de usuario;

  • enviar (105, 405) un mensaje de identidad destinado al teléfono móvil (2), conteniendo el mensaje de identidad un identificador del recurso objetivo (3);

estando provisto el teléfono móvil (2) de una aplicación (20) de cliente configurada para, al producirse la recepción de un mensaje de identidad:

  • buscar las identidades privadas de usuario asociadas al recurso objetivo (3) en el dispositivo (21) de almacenamiento;

  • si se halla por lo menos una identidad privada de usuario asociada, solicitar (106) al teléfono móvil una confirmación de usuario para el inicio de sesión automático en el recurso objetivo (3) utilizando una identidad privada de usuario seleccionada a partir de dicha por lo menos una identidad privada de usuario asociada;

  • si se produce una confirmación para el inicio de sesión automático, enviar (108, 406) dicha confirmación y la identidad privada de usuario seleccionada al servidor (4) de identificación;

estando configurado además el servidor (4) de identificación, si se recibe la confirmación para el inicio de sesión automático, para enviar (109) la identidad privada de usuario seleccionada al navegador (10) de cliente; estando configurado además el complemento (11) de navegador para, al producirse la recepción de la identidad privada de usuario seleccionada, iniciar sesión (110, 407) en el recurso objetivo (3) usando dicha identidad privada de usuario seleccionada.

2. Sistema según la reivindicación 1, en el que la solicitud de identidad incluye además un identificador del recurso objetivo (3) al que se está accediendo, y en donde el complemento (11) de navegador está configurado para enviar (103) la solicitud de identidad directamente al servidor (4) de identificación.

3. Sistema según la reivindicación 1, estando habilitado para OpenID el recurso objetivo, en donde el complemento (11) de navegador está configurado para enviar (402) la solicitud de identidad destinada a llegar al servidor (4) de identificación a través del recurso objetivo (3).

4. Sistema según cualquiera de las reivindicaciones 1 a 3, en el que la aplicación (20) de cliente está configurada además para, en caso de que se halle una pluralidad de identidades privadas de usuario asociadas al recurso objetivo (3), solicitar (106) al usuario que seleccione una identidad privada de usuario a enviar al servidor (4) de identificación.

5. Sistema según cualquiera de las reivindicaciones 1 a 4, en el que la aplicación (20) de cliente está asociada a por lo menos un puerto del teléfono móvil (2), y en donde el teléfono móvil (2) está configurado para, al producirse la recepción (105, 405) de un mensaje de identidad recibido en un puerto predeterminado asociado a la aplicación (20) de cliente, ejecutar la aplicación (20) de cliente, si todavía no se está ejecutando.

6. Sistema según cualquiera de las reivindicaciones 1 a 5, en el que cada comunicación (105, 405) que se origina desde el servidor (4) de identificación y que está destinada al teléfono móvil (2) se lleva a cabo a través del envío de por lo menos un mensaje SMS.

7. Sistema según cualquiera de las reivindicaciones 1 a 6, presentando el teléfono móvil capacidad de acceso inalámbrico a Internet, en donde cada comunicación (108, 406) que se origina desde el teléfono móvil y está destinada al servidor (4) de identificación se lleva a cabo a través del envío de por lo menos un mensaje HTTP.

8. Sistema según cualquiera de las reivindicaciones 1 a 7, en el que cada comunicación (103, 109) entre el ordenador (1) y el servidor (4) de identificación, en ambas direcciones, se lleva a cabo a través de por lo menos un mensaje HTTP.

9. Método para gestionar el inicio de sesión automático en recursos objetivo de Internet, cuando un ordenador (1) provisto de un navegador (10) de cliente accede (100) a un recurso objetivo (3) que requiere inicio de sesión, caracterizado porque comprende:

- detectar, al producirse la recepción (101, 401) de información que contiene un formulario de inicio de sesión enviado por el recurso objetivo (3) al cual está accediendo un usuario del navegador (10) de cliente, el formulario de inicio de sesión contenido en la información recibida;

- solicitar (102) al usuario, y por consiguiente obtener, un identificador de usuario;

- enviar (103, 402) una solicitud de identidad destinada a llegar a un servidor (4) de identificación, incluyendo dicha solicitud (103, 402) de identidad por lo menos el identificador de usuario;

- obtener, al producirse la recepción del identificador de usuario, un número de teléfono móvil asociado a dicho identificador de usuario;

- enviar (105, 405) un mensaje de identidad destinado al teléfono móvil (2) con dicho número de teléfono móvil, conteniendo el mensaje de identidad un identificador del recurso objetivo (3);

- buscar, al producirse la recepción del mensaje de identidad, las identidades privadas de usuario asociadas al recurso objetivo (3) en un dispositivo (21) de almacenamiento del teléfono móvil (2);

- si se halla por lo menos una identidad privada de usuario asociada, solicitar (106) al teléfono móvil una confirmación de usuario para el inicio de sesión automático en el recurso objetivo (3) utilizando una identidad privada de usuario seleccionada a partir de dicha por lo menos una identidad privada de usuario asociada;

- si se produce una confirmación para el inicio de sesión automático, enviar (108, 406) dicha confirmación y la identidad privada de usuario seleccionada al servidor (4) de identificación;

- si el servidor (4) de identificación recibe confirmación para el inicio de sesión automático, enviar (109) la identidad privada de usuario seleccionada al navegador (10) de cliente;

- iniciar sesión (110, 407), al producirse la recepción de la identidad privada de usuario seleccionada, en el recurso objetivo (3) utilizando dicha identidad privada de usuario seleccionada.

10. Método según la reivindicación 9, que comprende además, en caso de que se halle una pluralidad de identidades privadas de usuario asociadas al recurso objetivo (3), solicitar (106) al usuario que seleccione una identidad privada de usuario a enviar al servidor (4) de identificación.

11. Método según cualquiera de las reivindicaciones 9 a 10, en el que cada comunicación (105, 405) que se origina desde el servidor (4) de identificación y que está destinada al teléfono móvil (2) se lleva a cabo a través del envío de por lo menos un mensaje SMS.

12. Método según cualquiera de las reivindicaciones 9 a 11, en el que cada comunicación (108, 406) que se origina desde el teléfono móvil y que está destinada al servidor (4) de identificación se lleva a cabo a través del envío de por lo menos un mensaje HTTP.

13. Método según cualquiera de las reivindicaciones 9 a 12, en el que cada comunicación (103, 109) entre el ordenador (1) y el servidor (4) de identificación, en ambas direcciones, se lleva a cabo a través de por lo menos un mensaje HTTP.

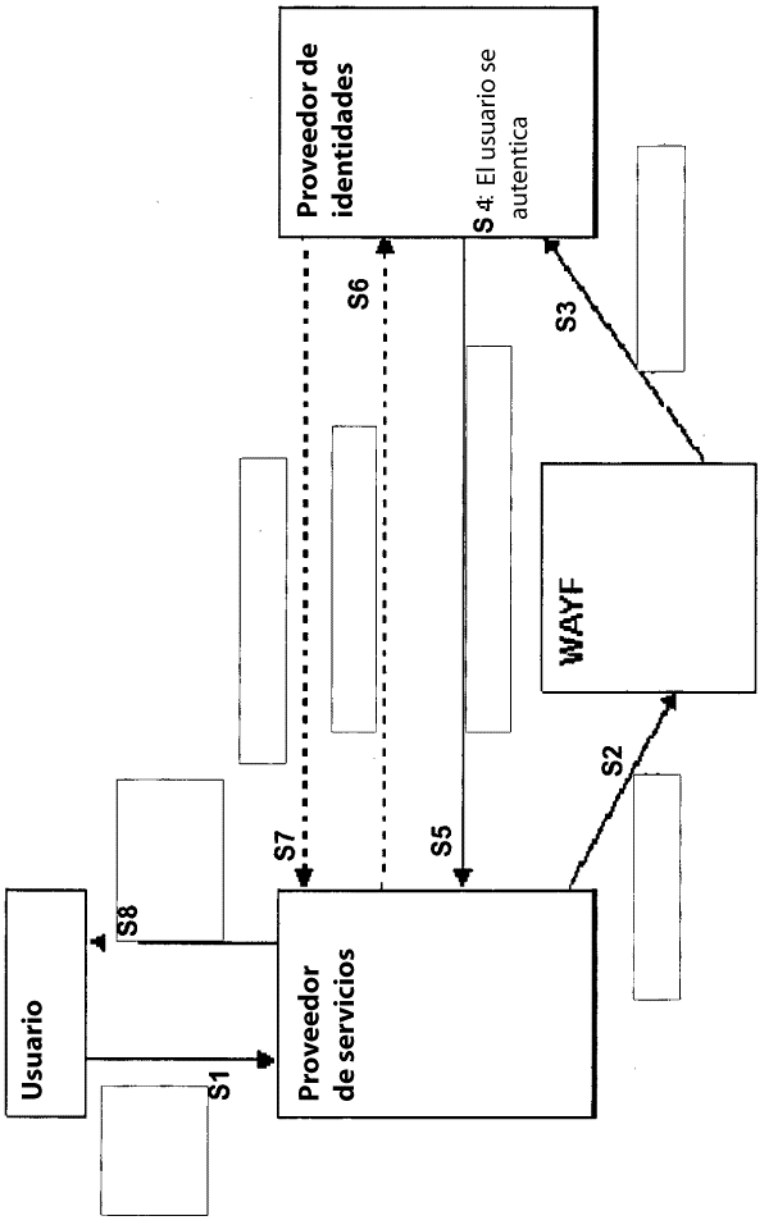
Proveedor de identidades
S 4: El usuario se autentica
S6
S3
WAYF
S2
S7
S5
S8
Usuario
Proveedor de servicios
S1

Fig. 1

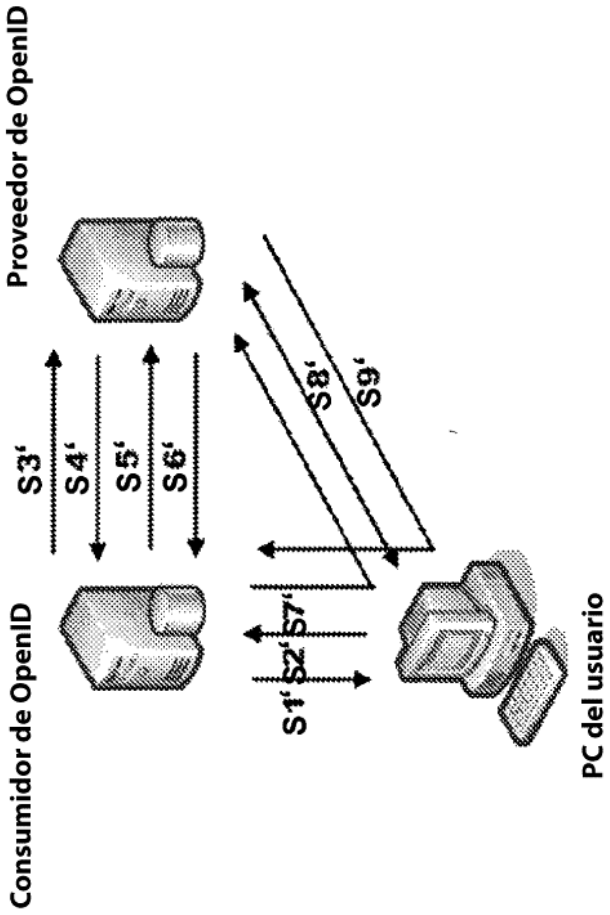
Proveedor de OpenID
Consumidor de OpenID
PC del usuario
S1'
S2'
S3'
S4'
S5'
S6'
S7'
S8'
S9'

Fig. 2

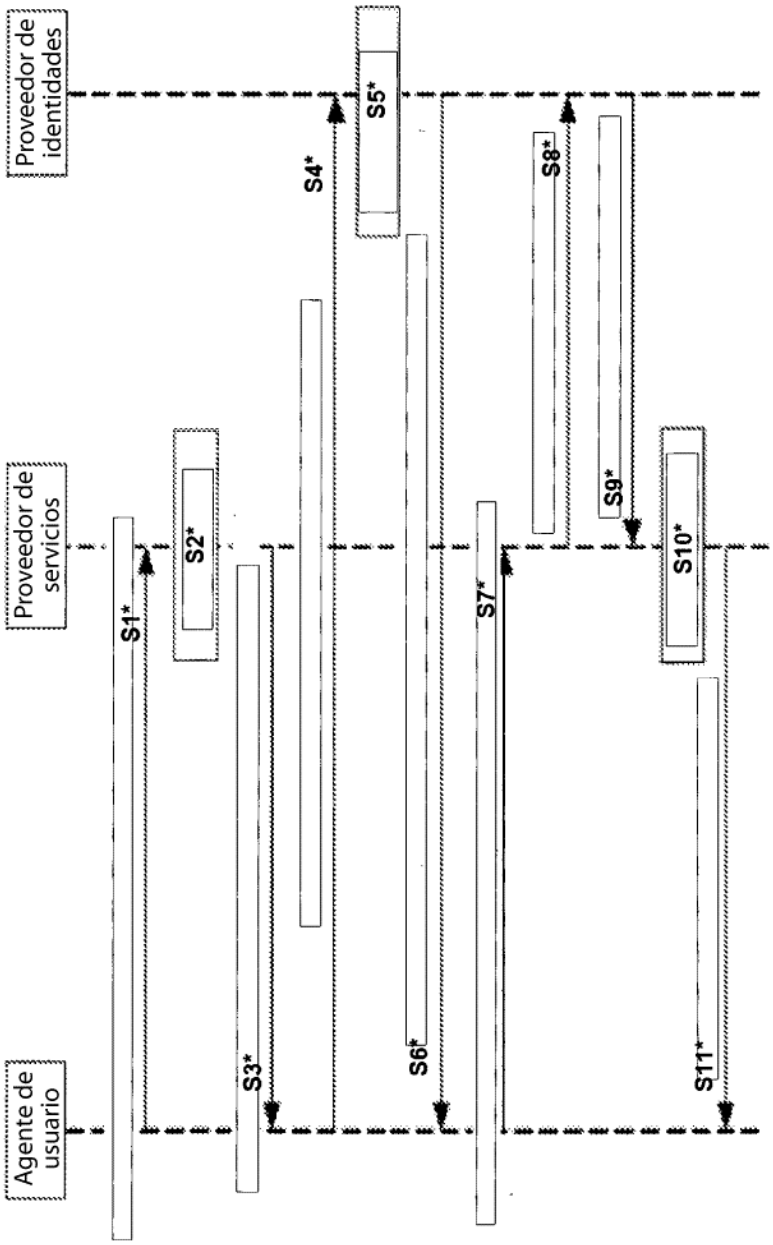
Proveedor de identidades
Proveedor de servicios
Agente de usuario
S1*
S2*
S3*
S4*
S5*
S6*
S7*
S8*
S9*
S10*
S11*

Fig. 3

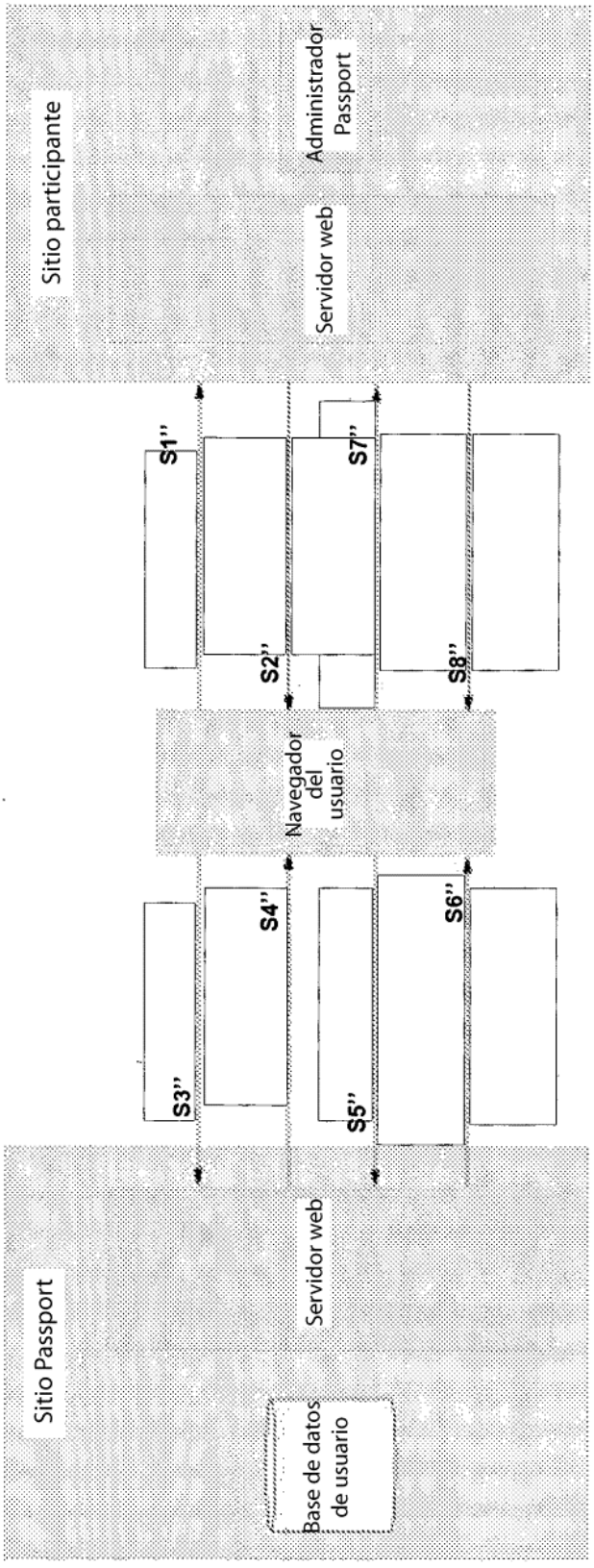
Sitio participante
Administrador Passport
Servidor web
S1''
S2''
S7''
S8''
Navegador del usuario
S3''
S4''
S5''
S6''
Sitio Passport
Servidor web
Base de datos de usuario

Fig. 4

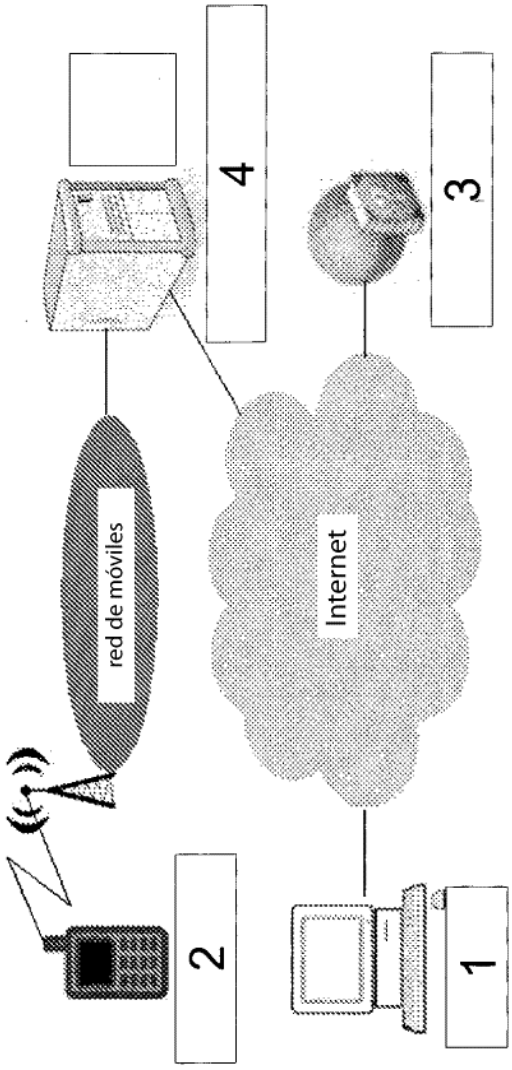

Fig. 5

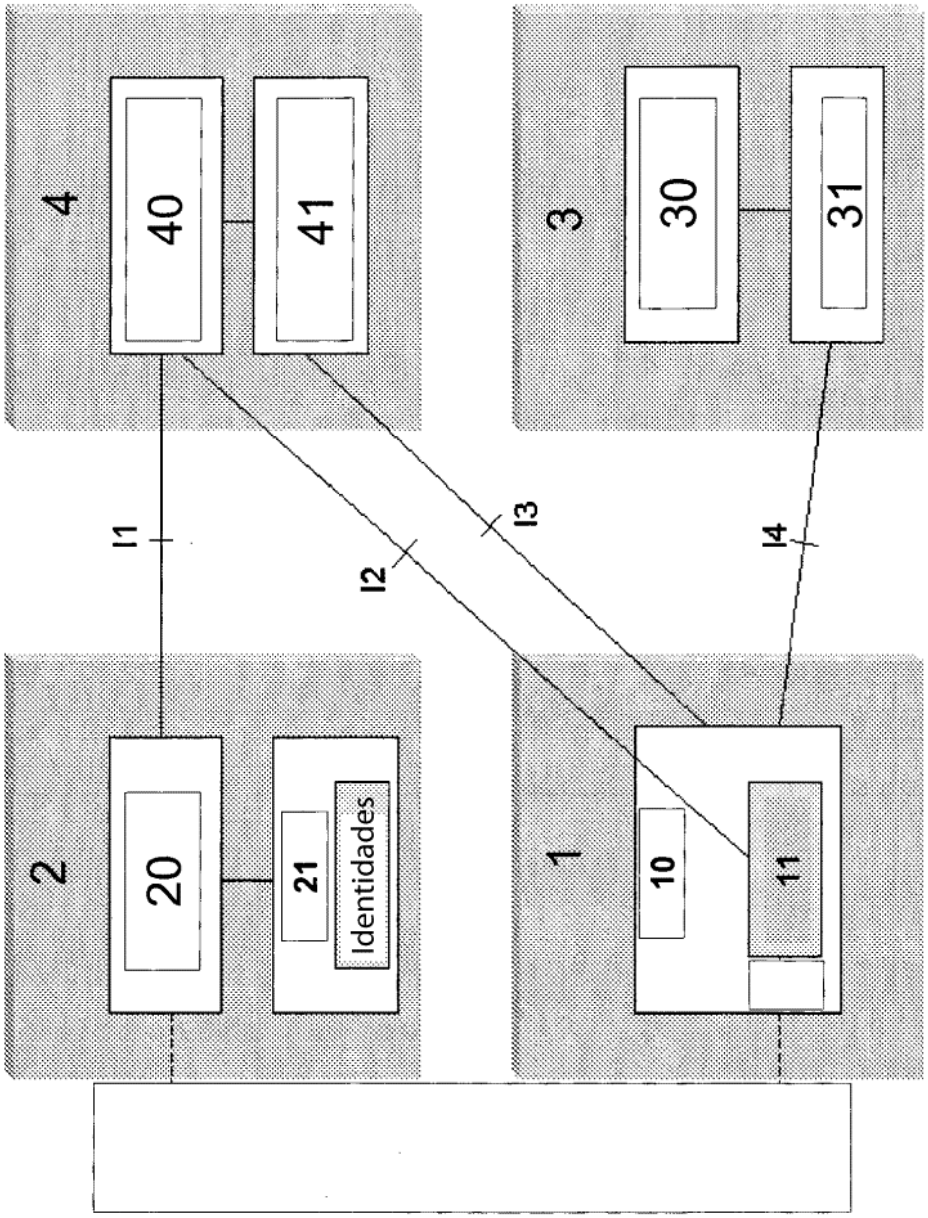

Fig. 6

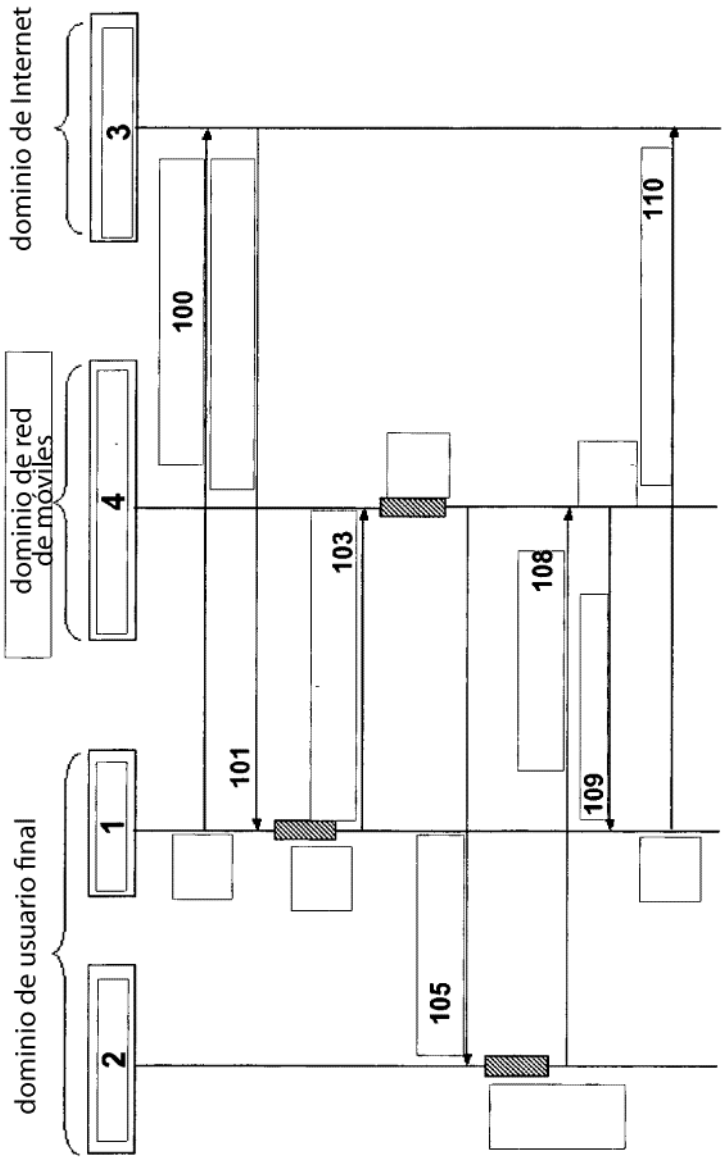
dominio de Internet
3
dominio de red de móviles
4
dominio de usuario final
1
2
100
101
103
105
108
109
110

Fig. 7

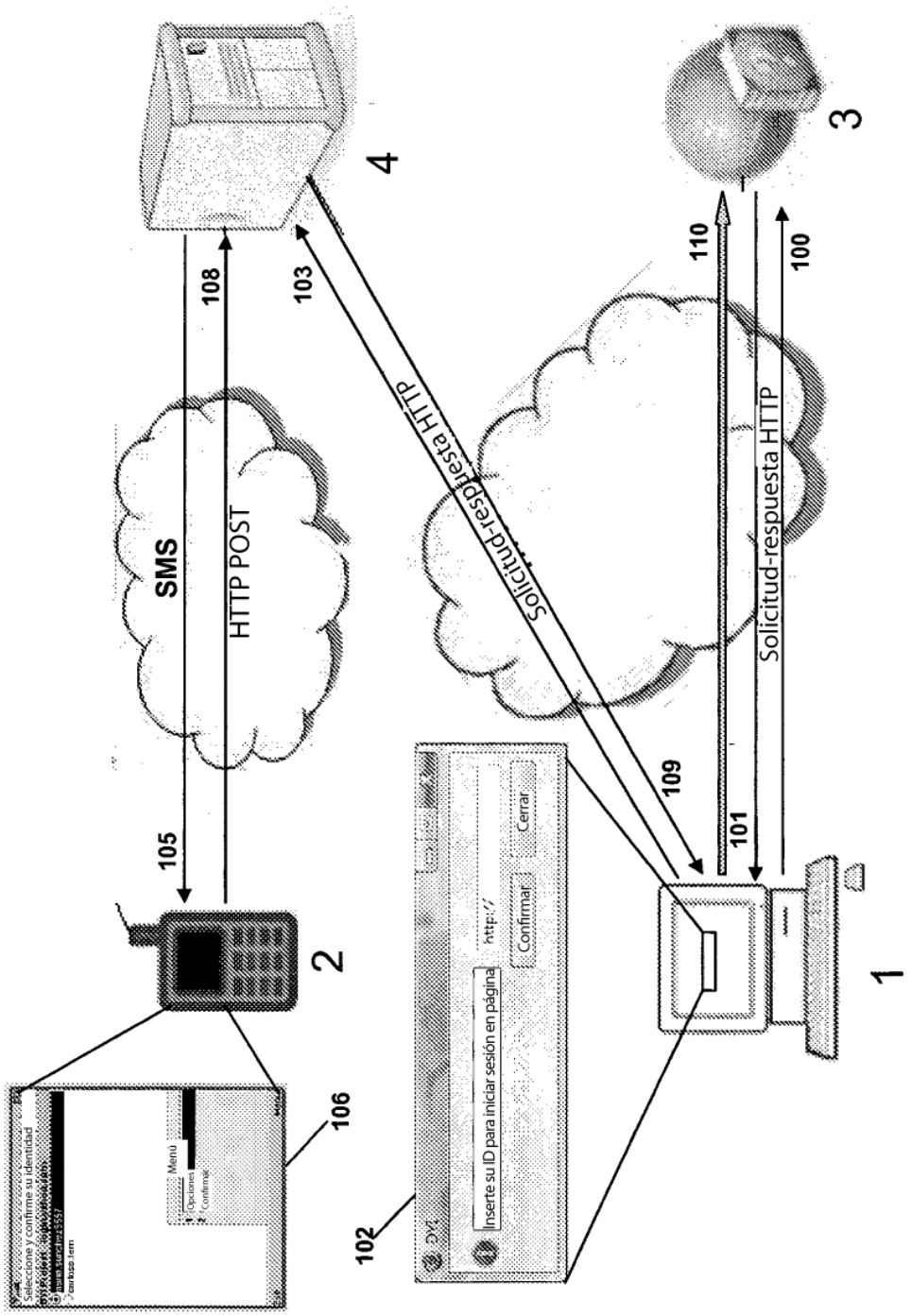
SMS
HTTP POST
Solicitud-respuesta HTTP
Solicitud-respuesta HTTP
Inserte su ID para iniciar sesión en página
Confirmar
Cerrar
Menu
Opciones
Confirmar
1
2
3
4
100
101
102
103
105
106
108
109
110

Fig. 8

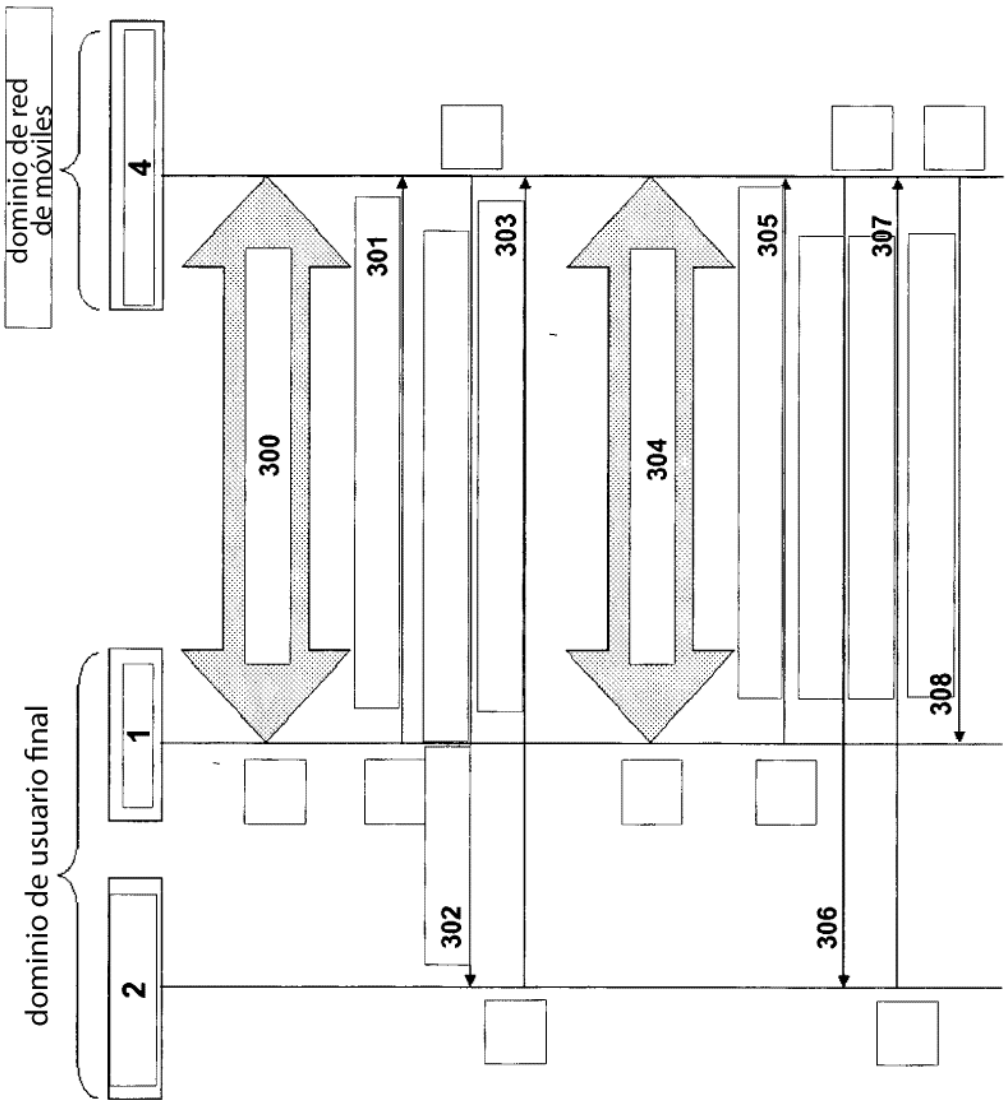
dominio de red de móviles
4
dominio de usuario final
1
2
300
301
302
303
304
305
306
307
308

Fig. 9

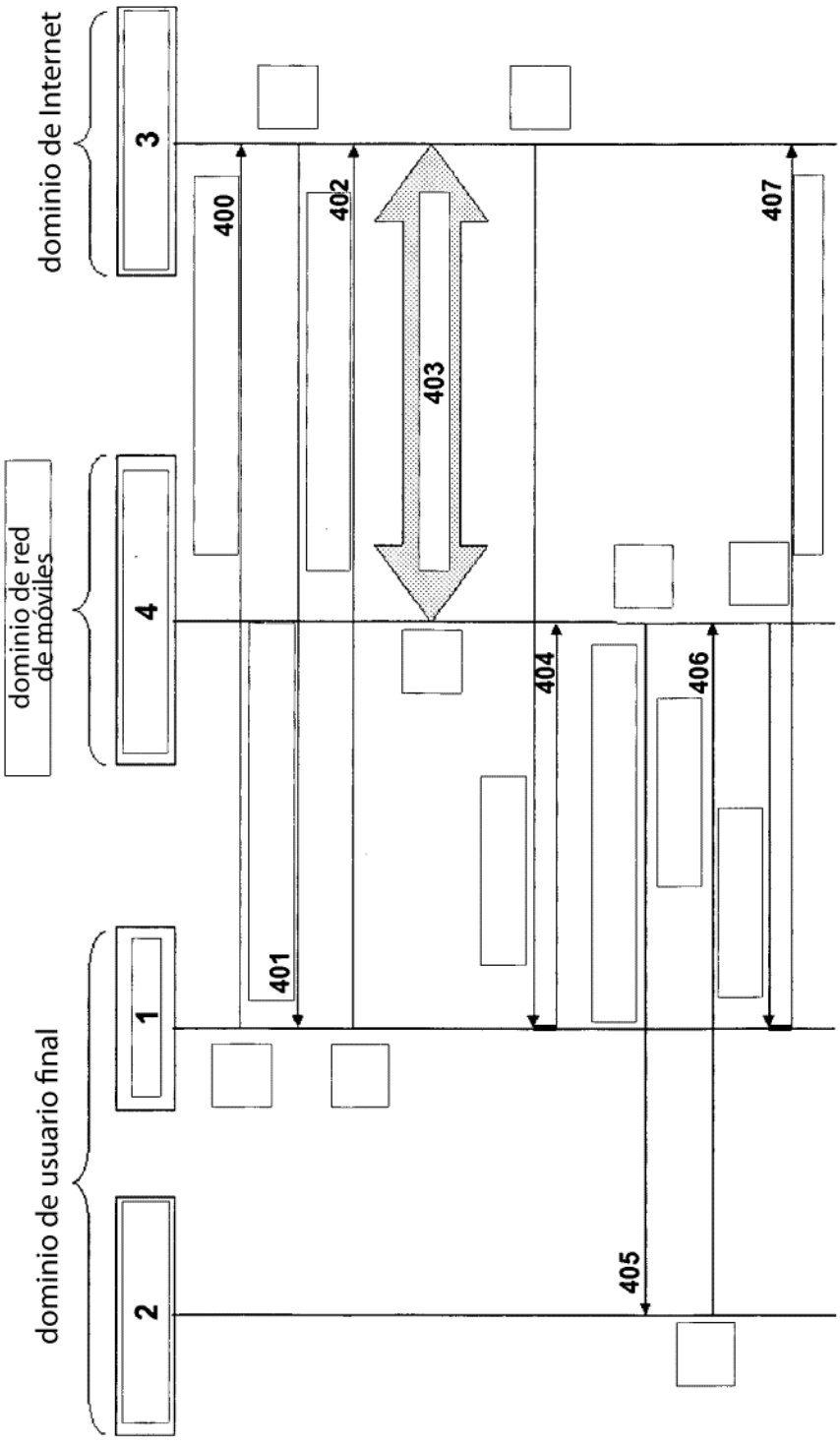
dominio de Internet
3
dominio de red de móviles
4
dominio de usuario final
1
2
400
401
402
403
404
405
406
407

Fig. 10