(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 601 009**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/30 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.10.2011 PCT/EP2011/068513**

(87) Fecha y número de publicación internacional: **31.05.2012 WO12069263**

(96) Fecha de presentación y número de la solicitud europea: **24.10.2011 E 11773463 (2)**

(97) Fecha y número de publicación de la concesión europea: **10.08.2016 EP 2643955**

(54) Título: **Procedimientos para autorizar el acceso a contenido protegido**

(30) Prioridad:

24.11.2010 US 416901 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.02.2017

(73) Titular/es:

TELEFÓNICA, S.A. (100.0%)
Gran Vía, 28
28013 Madrid, ES

(72) Inventor/es:

GONZÁLEZ MARTÍNEZ, DIEGO;
LOZANO LLANOS, DAVID;
MUNUERA ANDREO, JORGE;
VÉLEZ TARILONTE, ENRIQUE y
GUILLÉN NAVARRO, JORGE

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimientos para autorizar el acceso a contenido protegido

Campo de la invención

La presente invención se refiere en general a un procedimiento de autentificación para un usuario de un sistema de telecomunicaciones y, específicamente, a la autorización de terceros para acceder a un servidor en nombre del usuario sin necesidad de utilizar sus credenciales, siendo dicho usuario un propietario de contenido protegido. La invención se basa en el SMS como un canal especial para ser utilizado en entornos de telecomunicaciones para la transmisión de información relacionada con la autorización.

Antecedentes de la invención

Con el creciente uso de los servicios web distribuidos y computación en la nube, las aplicaciones de terceros requieren acceso a recursos alojados por el servidor. La mayor parte de estos recursos suelen estar protegidos y requieren la autorización explícita del usuario, después de la autentificación de usuario con éxito utilizando las credenciales de los propietarios de los recursos (por lo general, un nombre de usuario y contraseña). En el modelo tradicional de autentificación de cliente-servidor, un cliente que accede a un recurso protegido en un servidor presenta credenciales de los propietarios de los recursos con el fin de autentificar y obtener acceso.

El problema es que, para que estas aplicaciones puedan acceder a los datos del usuario en otros sitios, piden nombres de usuario y/o contraseñas. Esto no solo requiere la exposición de las contraseñas de usuario a otra persona, a menudo las mismas contraseñas utilizadas para banca en línea y otros sitios, sino que también proporciona a estas aplicaciones un acceso ilimitado para hacer lo que quieran, pudiendo hacer cualquier cosa, incluyendo el cambio de las contraseñas de los usuarios y bloquearlos.

Esto significa que la solución debe proporcionar al usuario no solo la confidencialidad de sus credenciales, sino también la posibilidad de restringir el acceso a un subconjunto limitado de los recursos que controlan, o limitar la duración de acceso, o limitar el acceso a los procedimientos de HTTP soportados por estos recursos. El protocolo OAuth 1.0, definido en "*RFC 5849 - El Protocolo OAuth 1.0*" proporciona una solución de este tipo, en base a un modelo de 3 vías y redirecciones web.

OAuth 1.0 es un protocolo abierto para permitir la autorización API segura en un procedimiento simple y estándar de las aplicaciones de escritorio y web, disponible tanto para los consumidores de confianza como los que no son de confianza (clientes). OAuth, tal como se especifica, es directamente aplicable para permitir el acceso a los recursos en los servicios REST, pero también se puede utilizar, por ejemplo, en los servicios web basados en SOAP.

Para que el cliente acceda a los recursos, primero tiene que obtener el permiso del propietario del recurso a través de la API OAuth. Este permiso se expresa en forma de un token y un secreto compartido correspondiente. El propósito de el token es, como ya se ha explicado, que sea innecesario que el propietario del recurso comparta sus credenciales con el cliente. A diferencia de las credenciales de dueños de recursos, los tokens pueden emitirse con un ámbito de aplicación restringido y limitado de por vida, y revocadas de forma independiente.

En resumen, el objetivo principal del protocolo OAuth es proporcionar los medios para que el consumidor pueda obtener un token de acceso válido como consecuencia de las interacciones que se resumen en la figura 1, que muestra el escenario de acceso de 3 vías.

En este modo de acceso de 3 vías, hay dos tokens con funciones cruciales:

En primer lugar, el token de solicitud se utiliza como una referencia dentro de los procedimientos de autorización delegados. Más concretamente, los tokens de solicitud son utilizados por el cliente para pedir al usuario que autorice el acceso a los recursos protegidos. Para ello, el usuario es redirigido a un portal en el que se haya autentificado el usuario y el usuario autoriza el acceso a los recursos protegidos de su propiedad. A continuación, el cliente recibe un código de verificación e intercambia este código y el token de solicitud autorizada por el usuario, que se recomienda que tenga una vida útil limitada, por un token de acceso.

Por último, este token de acceso es utilizado por el cliente para acceder a las API en nombre del usuario, en lugar de utilizar las credenciales del usuario (usuario y contraseña). Los tokens de acceso pueden limitar el acceso a determinadas API o incluso recursos dentro de una API determinada.

Por lo tanto, etapa a etapa, la figura 1 implica que el cliente 2 envía una solicitud de un token de solicitud 4 al servidor 3. Las etapas 5 y 6 proporcionan el token de solicitud al cliente e informan al usuario acerca de la acción 1, y en las etapas 7 y 8 el usuario informa al servidor que el cliente está autorizado. Luego se redirige 9 al cliente y el cliente obtiene un token de acceso en las etapas 10 y 11, y así se completa la autentificación 12. Las etapas 13, 14, 15 y 16 vienen después de la autentificación; el acceso de los clientes a los datos en el servidor en nombre del usuario.

Hay otros procedimientos de autentificación que hacen uso de diferentes mecanismos. Además, el servicio de mensajes cortos (SMS) ya se ha utilizado en conjunto con otras técnicas para enviar al usuario final las credenciales necesarias para acceder a los recursos. El documento "9.0 Uso de la API de la invitación" que se puede encontrar en la guía del desarrollador de la página web de Location Labs, divulgó un procedimiento para aquellas aplicaciones que no encajan de forma natural en un proceso de autorización basado-redirigido OAuth. Por ejemplo, las aplicaciones basadas en SMS no tienen forma natural para enviar una redirección. Para estas situaciones, se ofrece un procedimiento en el que el usuario final responde afirmativamente a una invitación de SMS para conceder permiso para ser localizado.

El usuario puede enviar un SMS de respuesta para conceder el permiso, y también registrarse al mismo tiempo, si no está ya registrado; o el usuario puede negarse, ya sea declinando la invitación en particular o mediante la solicitud de un bloque en todas las futuras invitaciones de SMS.

También hay un mecanismo de SMS iniciado por el usuario, separado de la API de invitación: una aplicación se puede configurar con una palabra clave única y en cuyo caso el usuario puede conceder permiso sin requerir ninguna acción por parte de la aplicación. O, por ejemplo, la solicitud de patente US 2010/0100725 A1 divulga un procedimiento para proporcionar la autentificación de usuario. Cuando un usuario de un sitio web o un sistema de servidor de empresa desea acceder a cierta información o realizar ciertas transacciones en el sitio web/servidor, se les pide que introduzcan un nombre de usuario y una contraseña en una interfaz de usuario (UI). El uso de una contraseña asociada con un nombre de usuario particular puede proporcionar autentificación del usuario, por ejemplo, porque la contraseña es conocida normalmente solo para el usuario que está registrado en el sitio web/servidor. Sin embargo, la seguridad para el acceso remoto a los sitios web y servidores puede verse comprometida si las contraseñas son utilizadas por aquellos que no sean el usuario registrado (por ejemplo, por los ladrones de identidades).

Las técnicas actuales de autentificación de factores múltiples incluyen la utilización de teléfonos o dispositivos móviles como un segundo factor de autentificación. A modo de ejemplo, cuando un usuario del sitio web intenta comprar un artículo en línea, el sitio web anfitrión puede enviar un mensaje de servicio de mensajes cortos (SMS) (por ejemplo, un mensaje de texto) al dispositivo móvil del usuario (por ejemplo, teléfono, móvil). En este ejemplo, después de recibir el mensaje SMS, el usuario puede responder con una clave de autentificación proporcionada por el sitio web. De esta manera, por ejemplo, un ladrón de identidades necesitaría el nombre de usuario, la contraseña y el dispositivo móvil designado del usuario con el fin de completar la autentificación.

El principal problema, como se ha dicho anteriormente, es que el protocolo OAuth se basa en cambios de dirección web (procedimientos HTTP). Esto significa que OAuth es apropiado para aplicaciones web y en general para entornos de uso, donde redirigir al usuario a una página web para la autentificación y la autorización es una experiencia de usuario apropiada. Para otros entornos o aplicaciones, como las aplicaciones no basadas en web instaladas en un teléfono móvil, las redirecciones web no proporcionan una experiencia de usuario adecuada, especialmente la etapa en el que el usuario tiene que introducir sus credenciales en una web como procedimiento de autentificación. Además, para aplicaciones de teléfonos móviles nativas que no sean web, la redirección web implica que la solicitud pierda el control del flujo de usuarios.

Sumario de la invención

La presente invención se refiere a un procedimiento de autentificación y autorización, que incluye un modo basado en interacciones de SMS.

El objetivo del procedimiento propuesto es extender el protocolo OAuth mediante la sustitución de las redirecciones web con SMS interacciones. Esto cambia la experiencia del usuario y permite nuevos escenarios de uso mediante la definición, en un primer aspecto de la invención, de un procedimiento para autorizar el acceso a una aplicación de terceros, denominada cliente, a un contenido protegido propiedad de un usuario y alojado en un servidor; el procedimiento comprende:

- el cliente es utilizado por el usuario que pide un token de solicitud al servidor;

- además de responder al cliente con dicho token de solicitud, el envío de un primer mensaje SMS al usuario por parte del servidor, proporcionando dicho primer SMS medios para autentificar al usuario;

- después de la autentificación del usuario y la posterior autorización para que el cliente acceda a los recursos protegidos, el envío de un segundo SMS al dispositivo del usuario, por parte del servidor, incluyendo un código de verificación necesario para obtener un token de acceso;

- el cliente recibe el código de verificación;

- el cliente obtiene el token de acceso del código de verificación.

- el cliente accede a recursos protegidos utilizando el token de acceso.

Un segundo aspecto de la invención se refiere a un procedimiento para autorizar el acceso a una aplicación de terceros, denominada cliente, a un contenido protegido propiedad de un usuario y alojado en un servidor; el procedimiento comprende:

- el cliente es utilizado por el usuario que pide un token de solicitud al servidor;

- además de responder al cliente con dicho token de solicitud, el envío de un primer mensaje SMS al usuario por parte del servidor, proporcionando dicho primer SMS medios para autentificar al usuario;

- después de la autentificación del usuario y la posterior autorización para que el cliente acceda a los recursos protegidos, el envío de un segundo SMS al dispositivo del usuario por parte del servidor, incluyendo un token de acceso;

- el cliente recibe el token de acceso;

- el cliente accede a recursos protegidos utilizando el token de acceso.

Un modo de realización preferido de la invención comprende la definición de un primer parámetro en el cliente para indicar quién es el usuario y dónde enviar el primer SMS.
Los medios del primer SMS para autentificar al usuario pueden ser una URL que lleva un token de SMS y una indicación para que el usuario haga clic en la URL, o los medios del primer SMS para autentificar al usuario pueden ser un token de SMS e indicaciones para que el usuario envíe un SMS con el token de SMS a un número designado.

El código de verificación incluido en el segundo SMS, según un modo de realización de la invención, puede darlo el usuario al cliente; o puede incluirse en el segundo SMS, siendo el segundo SMS un SMS binario enviado a un puerto indicado de la terminal del usuario en el que el cliente obtiene el código de verificación/autorización de forma automática. Alternativamente, el token de acceso puede incluirse directamente en el segundo SMS que el usuario da al cliente, o el token de acceso puede incluirse directamente en el segundo SMS, siendo el segundo SMS un SMS binario enviado a un puerto indicado del terminal del usuario en el que el cliente obtiene el token de acceso de forma automática.

Según otro modo de realización, un segundo parámetro se define en el cliente para indicar que un SMS o un binario-SMS tiene que enviarse al usuario después de la autentificación y autorización de usuario.

La presente invención puede utilizar el protocolo OAuth para realizar las etapas del procedimiento. La extensibilidad de los parámetros en dicho protocolo permite definir un parámetro adicional no especificado en el protocolo OAuth como primer parámetro. El segundo parámetro también puede ser el parámetro del protocolo OAuth descrito como una redirección URI a la que el servidor de autorización volverá a redirigir al agente de usuario una vez que se haya obtenido (o rechazado) la autorización. Este parámetro se denomina devolución de llamada OAuth en OAuth 1.0. En este documento se hará referencia al mismo como "URL de devolución de llamada".

Estos y otros aspectos de la invención se esclarecerán con referencia a los modos de realización descritos a continuación.

Breve descripción de los dibujos

Para completar la descripción y con el fin de proporcionar una mejor comprensión de la invención, se proporciona un conjunto de dibujos. Dichos dibujos forman parte integral de la descripción e ilustran modos de realización preferidos de la invención, lo cual no debe interpretarse como una restricción del alcance de la invención, sino solo como ejemplos de cómo la invención se puede realizar. Los dibujos comprenden las siguientes figuras:

La figura 1 ilustra una visión general del escenario de acceso de 3 vías. Técnica anterior

La figura 2 muestra las interacciones entre las entidades del protocolo OAuth.

La figura 3 muestra un diagrama de secuencia para acceso OAuth.

La figura 4 muestra un diagrama de secuencia de un modo de realización de la invención.

Descripción detallada de los modos de realización preferidos

Ahora se hará referencia en detalle a un modo de realización preferido de la presente invención. El escenario propuesto tiene el soporte de protocolos anteriores que están siendo masivamente adoptados como OAuth 1.0. Este procedimiento considera un modelo de 3 vías en el que tres diferentes entidades (o vías) están directamente involucradas en los procedimientos para acceder a los interfaces de programa de aplicación, también denominados API:

- El proveedor de APIs o servidor de recursos

- El consumidor o cliente

- El usuario final o propietario del recurso.

Las interacciones entre estas entidades se resumen en la figura 2. El usuario realiza la solicitud original 21 para recurso al cliente. El cliente "redirige" 22 de la solicitud al servidor para autorización. La respuesta es del dominio del servidor pidiendo 23 al usuario autentificación. A continuación, el usuario autoriza 24 al cliente. El cliente obtiene 25 el token que le proporciona acceso. Y, finalmente, el cliente confirma 26 el acceso.

Los procedimientos actuales más importantes proporcionan a un cliente que no es de confianza acceso a las API en nombre del usuario final. Para permitir esto, el usuario final debe interactuar directamente mediante un acceso a la web con el proveedor de API con el fin de autentificar y autorizar expresamente al cliente para acceder a las API en su nombre. De esta manera, el usuario no tiene que compartir sus credenciales con los clientes que no sean de confianza y él / ella puede controlar las acciones permitidas para el cliente; por lo tanto, el cliente actúa bajo la responsabilidad del usuario final.

La invención propuesta define un flujo alternativo al definido en el OAuth 1.0 RFC con el fin de evitar las redirecciones web y sustituirlas por las interacciones de SMS con el teléfono del usuario. Se consideran diferentes variaciones:

1. La primera parte del procedimiento consiste en el envío de un SMS de autentificación al teléfono del usuario final. El SMS incluye un token no conocido por el consumidor que no sea de confianza que será utilizada para autentificar al usuario. A partir de aquí, este tokene se denomina "token de SMS". Dependiendo de las características de los teléfonos y de la conectividad disponible, dos alternativas pueden ser utilizadas por el usuario final:

a. El SMS puede incluir un enlace que lleva el token de SMS y el usuario puede hacer clic en el enlace. Ya sea mediante WAP o acceso a la web, el usuario será autentificado. A pesar de que el teléfono de usuario utiliza un navegador, no es necesario que el usuario incluya sus credenciales en una web. En este procedimiento, el usuario tendrá que utilizar el navegador abierto para autorizar el consumidor (por ejemplo: Haga clic en "Acepto").

b. El SMS puede incluir directamente el token de SMS y el usuario puede responder a los SMS con otro SMS que lleva el token de SMS. Mediante este acceso de SMS, el usuario será autentificado y el token de solicitud (asociado a el token de SMS) será autorizado. Esta segunda alternativa permite el procedimiento en teléfonos sin un navegador, o donde no se recomiende el uso de un navegador.

En este procedimiento, el SMS dará suficiente información al usuario acerca de qué acceso y a qué consumidor se va a autorizar.

2. La segunda parte del procedimiento también tiene dos alternativas:

a. En la primera alternativa, se envía un SMS binario a un puerto indicado en el teléfono del usuario. El SMS lleva el código de verificación OAuth. La aplicación del cliente en el teléfono obtiene de forma automática, sin intervención del usuario, el código de verificación del SMS y lo utiliza para obtener el token de acceso. Esta segunda parte se debe utilizar teniendo en cuenta el riesgo de SMS binario en ciertos sistemas operativos del teléfono, ya que pueden existir riesgos de seguridad. También hay que tener en cuenta que para esta alternativa de SMS binario, el cliente tiene que estar utilizando el dispositivo del usuario que recibe los SMS.

b. En la segunda alternativa, otro SMS se envía al teléfono del usuario incluyendo el código de verificación OAuth. El usuario deberá copiar el código de verificación y lo dará al cliente con el fin de obtener el token de acceso. En esta segunda alternativa, el teléfono de usuario donde se recibe el SMS no tiene por qué ser el dispositivo en el que se ejecuta el cliente.

Las dos partes del procedimiento son independientes, es decir: en el mecanismo propuesto es posible aplicar solo la primera parte del procedimiento, solo la segunda parte del procedimiento o ambas. La primera parte del procedimiento sustituye a la primera redirección de OAuth y la segunda parte del procedimiento sustituye a la segunda redirección de OAuth o al proceso de OAuth alternativo de mostrar el código de verificación en el navegador web para que el usuario lo copie.

La invención propuesta hace un uso inteligente de los parámetros de OAuth, y utiliza los nuevos parámetros que integrados en el protocolo OAuth indican que se solicita SMS de OAuth y cuáles de las nuevas soluciones basadas en SMS se están solicitando.

Como se ha explicado antes, se consideran dos modos diferentes, a saber, "acceso OAuth" y "acceso a SMS de OAuth". El primer modo permite el proceso mediante el uso de redirecciones web, y el segundo modo permite que el proceso mediante la sustitución de las redirecciones web por las interacciones de SMS. En un intento de introducir el segundo modo, es importante entender el flujo de trabajo existente que se inicia con la ejecución del primer modo, "acceso de OAuth". La figura 3 muestra el funcionamiento básico de "acceso de OAuth" en la técnica anterior.

Como se puede ver en la figura 3, el proceso de obtener un token de acceso se divide en tres etapas diferentes:

1. Obtención de un token de solicitud no autorizado, a través de una "operación de obtención de token de solicitud de HTTP".

- Las etapas 32, 33, 34, 35 y 36 representan la solicitud de acceso desde el usuario hasta el cliente, la respuesta del cliente, la solicitud de un token de solicitud al servidor y la respuesta del servidor.

2. Delegación web: es la etapa intermedia en la que se autentifica el usuario y se autoriza al cliente a acceder a las APIs. Como resultado se autoriza el token de solicitud obtenido previamente.

- Etapa 37: redirección a una entidad de autentificación-autorización (o entidad AA) 31

- Etapa 38: autentificación de usuario y autorización de cliente

- Etapa 39: redirección al cliente

3. Obtención del token de acceso, a través de una "operación de obtención de token de acceso de HTTP"

- Las etapas 391 y 392 representan al cliente pidiendo un token de acceso al servidor y la respuesta correspondiente del servidor.

El nuevo modo del protocolo introduce algunas variaciones, como se muestra en la figura 4.

Como se puede ver en la figura 4, el proceso de obtener un token de acceso en OAuth 1.0 se divide en las siguientes etapas diferentes:

1. Obtención de un token de solicitud no autorizado 61, a través de una "operación de obtención de token de solicitud de HTTP".

Si se solicita la primera parte del procedimiento propuesto para ser ejecutado como alternativa a OAuth normal:

a. El cliente incluye un parámetro para indicar quién es el usuario y para saber dónde enviar el SMS. Esto se logra mediante el uso de un parámetro adicional no definido en el protocolo OAuth, pero también se puede lograr mediante la reutilización o un uso especial de un parámetro existente en el protocolo OAuth. La extensibilidad de los parámetros en el protocolo permite definir un nuevo parámetro. Este nuevo parámetro se puede utilizar como la indicación de que se solicita SMS-OAuth para ser utilizado, o también puede utilizarse un parámetro específico diferente. b. El cliente incluye opcionalmente un parámetro para indicar si el primer SMS debe ser enviado:

I. Incluyendo una URL que lleva un token de SMS, normalmente como un parámetro de consulta, y una indicación de que el usuario haga clic en la URL.

II. O el token de SMS junto con la información de autorización e indicaciones para el usuario para enviar un SMS con el token de solicitud a un número designado.

Ambos hacen que el usuario se autentique a sí mismo, autorizando de este modo al cliente, y se envía un token de autorización 55 al servidor.

Alternativamente, el usuario tal vez solo tenga que simplemente responder al SMS recibido.

Si no se incluye este parámetro, se puede aplicar un comportamiento por defecto de los dos descritos

a. y b. pueden realizarse mediante otras combinaciones de uso de parámetros. Por ejemplo, un solo parámetro puede utilizarse para indicar cualquiera de las diferentes combinaciones.

Si se solicita la segunda parte del procedimiento propuesto para ser ejecutada como una alternativa a OAuth normal:

c. El consumidor indica por medio de diferentes ajustes de parámetro de URL de devolución de llamada qué modo de procedimiento de acceso de SMS se está utilizando para la segunda interacción.

I. SMS para el usuario final

II. SMS binario a un puerto indicado con el fin de activar una aplicación en el terminal. El puerto donde enviar el SMS binario puede ser indicada por el cliente o puede ser un puerto conocido predefinido.

Alternativamente a la etapa c), la URL de devolución de llamada puede establecerse con un valor específico (por ejemplo: "Fuera de banda") y un nuevo parámetro puede indicar el modo de SMS binario o SMS / navegador.

El nuevo parámetro que lleva la identidad del usuario (por ejemplo: el MSISDN o un apodo) activa la primera parte del procedimiento propuesto.

El uso especial de la URL de devolución de llamada (por ejemplo: no incluye una URL, sino la información necesaria, como el puerto de la aplicación en modo binario-SMS o una secuencia específica en modo de SMS) activa la segunda parte del procedimiento propuesto. Por lo tanto, la primera parte, la segunda parte o ambas partes del procedimiento pueden ser activadas por el cliente.

La combinación de parámetros descrita en los párrafos anteriores es un ejemplo, pero pueden utilizarse otras combinaciones que hacen uso de los parámetros de OAuth existentes y la definición de nuevos parámetros para activar una o más partes del procedimiento.

2-a. Si se ha activado la primera parte del procedimiento, el servidor envía un SMS al usuario de que el cliente indica en la solicitud de token de solicitud. Dependiendo de la etapa 1-b:

i. El SMS incluye una URL 51 que señala a una entidad de autorización y autentificación (AA). La URL incluye el token de SMS, normalmente como un parámetro de consulta. De esta manera, el usuario utiliza esta URL para autentificarse a sí mismo, debido a que el SMS fue enviado a su teléfono. El usuario da autorización para el cliente en el navegador web abierto, pero no hay necesidad de que el usuario incluya sus credenciales.

ii. El SMS incluye directamente el token de SMS 52, información sobre la autorización, y solicita al usuario que responda con otro SMS incluyendo el token de solicitud. De esta manera, el usuario utiliza esta respuesta por SMS para autorizar al consumidor haciendo clic en la URL 53 proporcionada o respondiendo al número indicado con otro SMS que lleva el token de SMS 54. El usuario también se autentifica porque el SMS fue enviado a su teléfono.

2-b La entidad de AA solicita la autorización de token de SMS y obtiene un código de verificación 56. Si se ha activado la segunda parte del procedimiento, en función de si "Obtener token de solicitud" en la etapa 1-c indicaba si debe utilizarse SMS al usuario final o SMS binario:

a. La entidad AA envía 57 un SMS con el código de verificación al terminal del usuario. El usuario da 59 este código de verificación al cliente. b. La entidad de AA envía 58 un SMS binario al puerto indicado en "Obtención de token de solicitud" y llevando el código de verificación o el token de acceso. La aplicación en el teléfono del usuario, sin intervención del usuario, obtiene 60 el código de verificación o el token de acceso.

El token de SMS no es conocido por el cliente que no es de confianza, pero existe una asociación en el Proveedor del Servicio entre el token de SMS y el token de solicitud.

3. La obtención del token de acceso en las etapas 391, 392, a través de una "operación de obtención de token de acceso de HTTP", excepto en el caso en que el token de acceso ya fue enviado en SMS binario como se describe en 2-bb.

En resumen, la invención propuesta extiende el protocolo OAuth mediante la sustitución de las redirecciones web con interacciones de SMS. Esto cambia la experiencia del usuario y permite nuevos escenarios de uso, como los siguientes:

- Eliminación de la necesidad de que el usuario proporcione sus credenciales (por ejemplo: usuario y contraseña) en una web como mecanismo de autentificación.

- El uso de OAuth en aquellos dispositivos que no permiten el uso de navegadores.

- El uso de OAuth cuando la aplicación es una aplicación nativa que no sea de red en un teléfono móvil, en el que el uso de un navegador puede romper la interfaz de usuario de la aplicación.

- El uso de OAuth cuando la aplicación no sea capaz de recibir redirecciones HTTP, por cualquier motivo (por ejemplo: Una aplicación del lado del cliente en el teléfono móvil)

Como se ha indicado antes, las dos partes son independientes: es posible aplicar solo la primera parte del procedimiento, solo la segunda parte del procedimiento o ambas. La primera parte del procedimiento sustituye a la primera redirección OAuth y la segunda parte de la procedimiento sustituye a la segunda redirección OAuth o al proceso alternativo de OAuth de mostrar el código de verificación en el navegador web para que el usuario lo copie.

El procedimiento propuesto hace un uso inteligente de los parámetros de OAuth, y utiliza los nuevos parámetros que integrados en la API de OAuth indican que se solicita un SMS de OAuth y cuáles de las nuevas soluciones basadas en SMS se están solicitando.

La invención propuesta presenta varias ventajas con respecto al protocolo OAuth actual desarrollado por IETF.

- Compatibilidad retrospectiva con OAuth existente: es completamente compatible con el estándar. También permite al consumidor indicar y al servidor detectar la necesidad de enviar un SMS al usuario final o al aplicar el procedimiento OAuth existente.

- Aumento de la cantidad de potenciales usuarios: el procedimiento propuesto ofrece a muchos usuarios acceso a varios recursos que no podrían ser utilizados debido a sus restricciones de dispositivos móviles. El mercado de nuevos servicios aumenta en una enorme cantidad de potenciales usuarios.
- Experiencia del usuario mejorada en aplicaciones no basadas en web: El procedimiento propuesto mejora la experiencia del usuario cuando la aplicación de los consumidores no está basada en el navegador.

Para estos tipos de aplicaciones, el usuario tal vez encuentre las redirecciones web más invasivas, ya que una aplicación no web requiere iniciar el navegador y requiere que el usuario dé sus credenciales. La percepción dada al usuario también puede ser de menos seguridad.

El uso de interacciones de SMS, especialmente en teléfonos móviles, puede ser mejor percibida por los usuarios finales. Incluso cuando el primer SMS lleva una URL, es el usuario el que hace clic manualmente en la URL para iniciar el navegador. Esto da al usuario una percepción de más seguridad.

- Un enfoque más apropiado para aplicaciones nativas no basadas en Web: El mecanismo definido es más apropiado para aplicaciones nativas en teléfonos móviles. Para estas aplicaciones, la invocación de un navegador implica perder el control del flujo de usuario.
- Aplicación en dispositivos que no sean de navegador: La invención no excluye que las aplicaciones tengan acceso a los recursos protegidos en aquellos casos en los que el navegador no está soportado por el terminal. La respuesta de SMS puede ser mejor percibida por el usuario, en contraste con la invocación del navegador para la autentificación de usuario.
- Aplicabilidad de OAuth en aplicaciones que no soportan redirecciones HTTP y, por lo tanto, no podrán funcionar con OAuth, que requiere redirecciones HTTP. Diferentes opciones de implementación dentro de la misma solución: El nuevo mecanismo, basado en interacciones de SMS, ofrece diferentes variaciones. Estas variaciones pueden seleccionarse dependiendo de las características de los clientes, las características de la aplicación (ordenador, móvil, web).

Tiene que entenderse que la anterior descripción es una ejemplificación de los principios de la invención y no limita la invención a los modos de realización descritos.

La invención está definida por las reivindicaciones siguientes.

REIVINDICACIONES

1. Procedimiento para autorizar el acceso a una aplicación de terceros, llamada cliente (2), para recursos protegidos propiedad de un usuario (1) y alojados en un servidor (3), comprendiendo el procedimiento:

- el cliente pide un token temporal al servidor;

- además de la respuesta al cliente con dicho token temporal, el servidor envía un primer SMS (51, 52) al usuario, con dicho primer SMS proporcionando medios para autentificar al usuario (53,54);

- autentificar al usuario por los medios previstos en las dos etapas anteriores;

- el usuario autoriza al cliente (55);

estando el procedimiento **caracterizado por que** comprende:

- después de la autentificación del usuario y de la autorización del cliente por el usuario, el servidor envía un segundo SMS al usuario incluyendo un código de verificación necesario para obtener un token de acceso;

- el cliente recibe (59, 60) el código de verificación;

- el cliente obtiene el token de acceso del código de verificación;

- el cliente accede a recursos protegidos utilizando el token de acceso.

2. Procedimiento para autorizar el acceso a una aplicación de terceros, llamada cliente (2), para recursos protegidos propiedad de un usuario (1) y alojados en un servidor (3), comprendiendo el procedimiento:

- el cliente pide un token temporal al servidor;

- además de la respuesta al cliente con dicho token temporal, el servidor envía un primer SMS (51, 52) al usuario, con dicho primer SMS proporcionando medios para autentificar al usuario (53,54);

- el usuario se autentifica por los medios previstos en las dos etapas anteriores;

- el usuario autoriza al cliente (55);

estando el procedimiento **caracterizado por que** comprende

- después de la autentificación del usuario y la autorización del cliente por el usuario, el servidor envía un segundo SMS, que incluye un token de acceso;

- el cliente recibe (59, 60) el token de acceso;

- el cliente accede a recursos protegidos utilizando el token de acceso.

3. El procedimiento según una cualquiera de las reivindicaciones anteriores, que comprende además la definición o el uso de un primer parámetro en el cliente para indicar quién es el usuario y dónde enviar el primer SMS.

4. El procedimiento según una cualquiera de las reivindicaciones anteriores, en el que los medios para autentificar al usuario, incluidos en el primer SMS, son una URL que lleva un token no conocido para el cliente y una indicación para que el usuario haga clic en la URL.

5. El procedimiento según una cualquiera de las reivindicaciones 1-3, en el que los medios incluidos en el primer SMS para autentificar al usuario, son un token no conocido para el cliente y las indicaciones para el usuario para enviar un SMS con el token a un número designado.

6. El procedimiento según una cualquiera de las reivindicaciones 1, 2, que comprende además la definición o el uso de un segundo parámetro en el cliente para indicar que un SMS o un SMS binario tiene que ser enviado al usuario después de la autentificación y la autorización del usuario.

7. El procedimiento según la reivindicación 1, en el que el usuario da el código de verificación incluido en el segundo SMS al cliente (59).

8. El procedimiento según la reivindicación 1, en el que el segundo SMS es un SMS binario enviado a un puerto indicado de un teléfono del usuario desde el cual el cliente obtiene (60) el código de verificación directamente.

9. El procedimiento según la reivindicación 2, en el que el usuario da el token de acceso al cliente.

10. El procedimiento según la reivindicación 2, en el que el segundo SMS es un SMS binario enviado a un puerto indicado de un teléfono del usuario, en el que el cliente obtiene el token de acceso directamente.

11. El procedimiento según la reivindicación 3, en el que el primer parámetro se define mediante el uso de un parámetro adicional no definido en el protocolo OAuth.

12. El procedimiento según la reivindicación 3, en el que el primer parámetro se define mediante la reutilización de un parámetro definido en el protocolo OAuth.

13. El procedimiento según la reivindicación 6, en el que el segundo parámetro se define mediante el uso de un parámetro adicional no definido en el protocolo OAuth.

14. El procedimiento según 6, en el que el segundo parámetro es el parámetro de URL de devolución de llamada del protocolo OAuth.

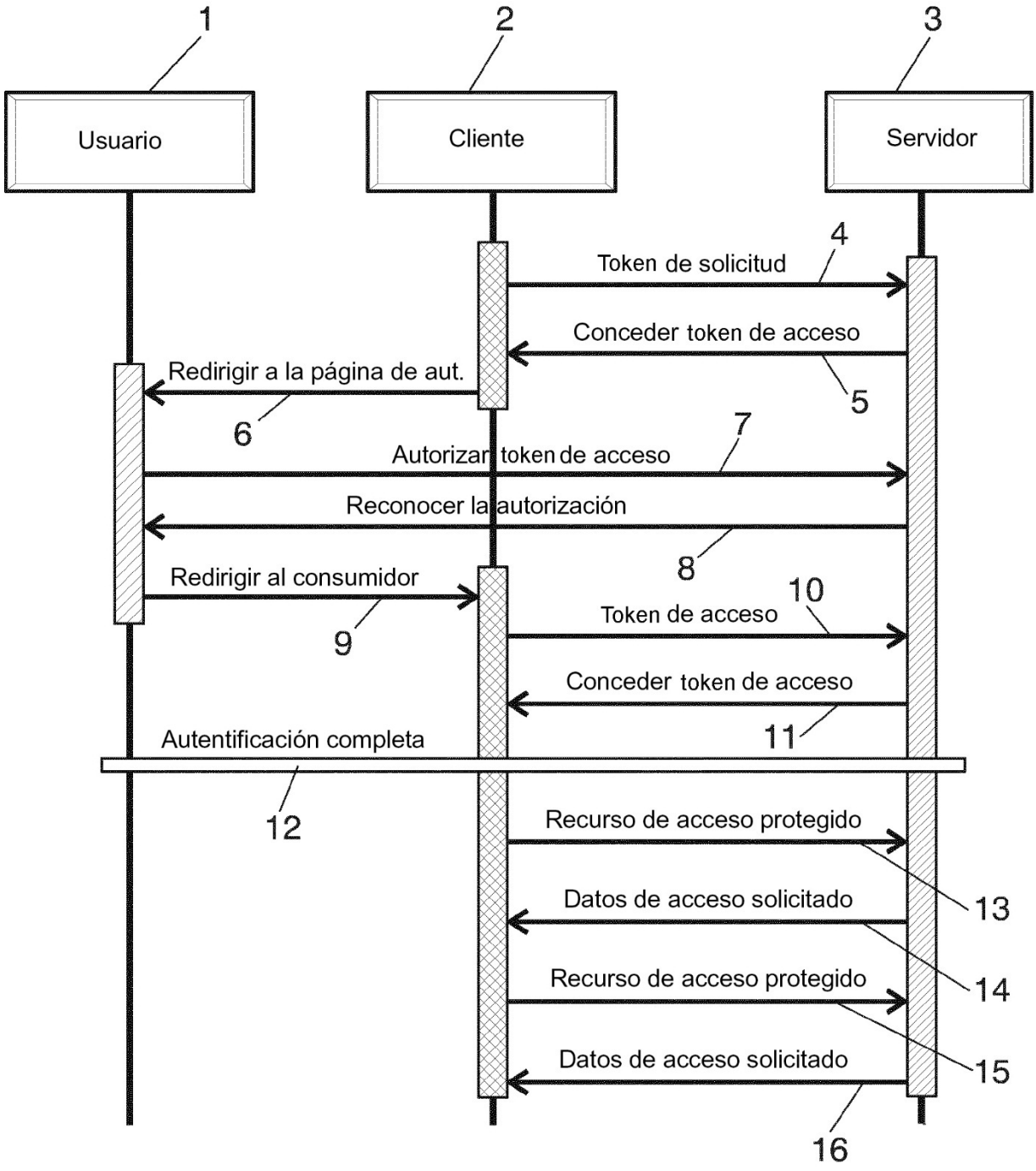
1
2
3
Usuario
Cliente
Servidor
4
Token de solicitud
Conceder token de acceso
5
Redirigir a la página de aut.
6
7
Autorizar token de acceso
Reconocer la autorización
8
Redirigir al consumidor
9
10
Token de acceso
Conceder token de acceso
11
Autentificación completa
12
Recurso de acceso protegido
13
Datos de acceso solicitado
14
Recurso de acceso protegido
15
Datos de acceso solicitado
16

FIG. 1

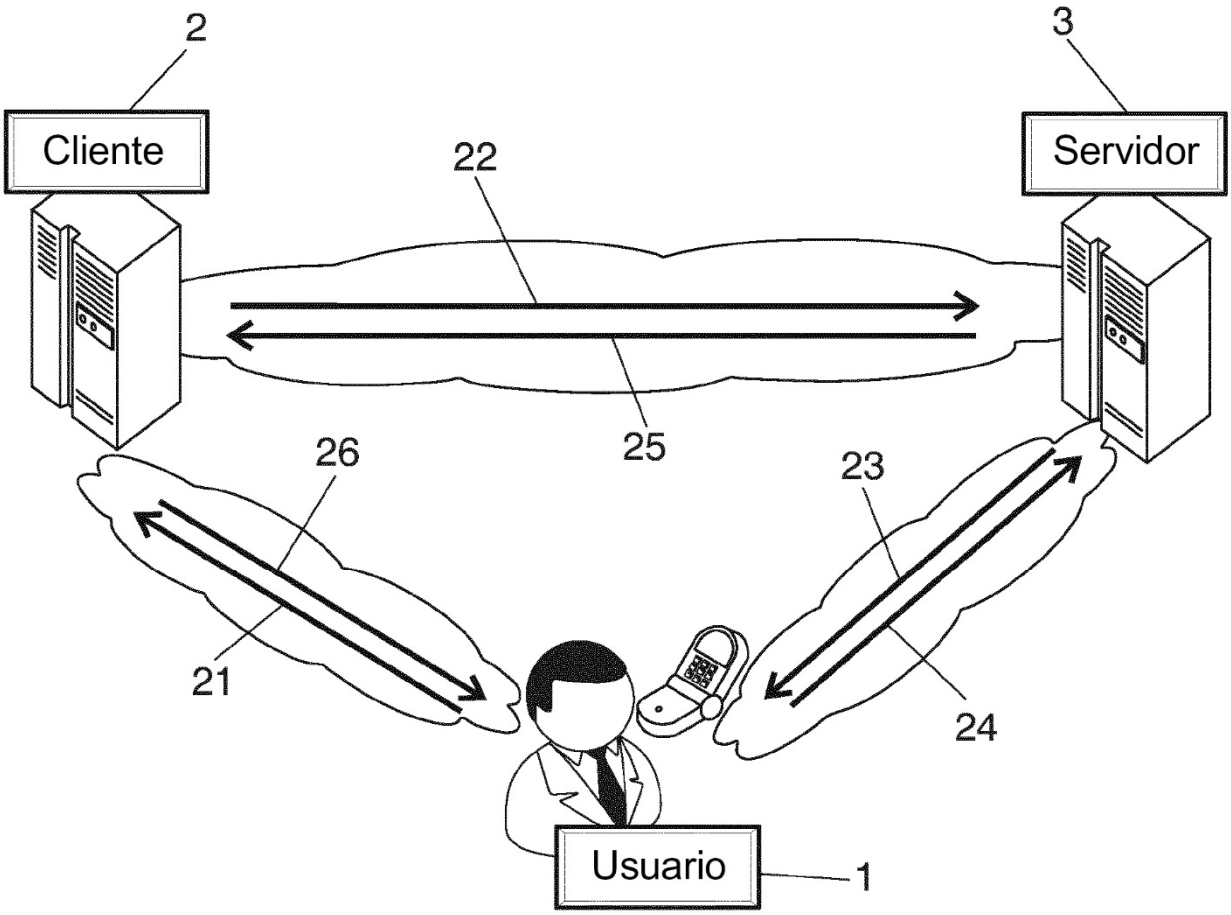

FIG. 2

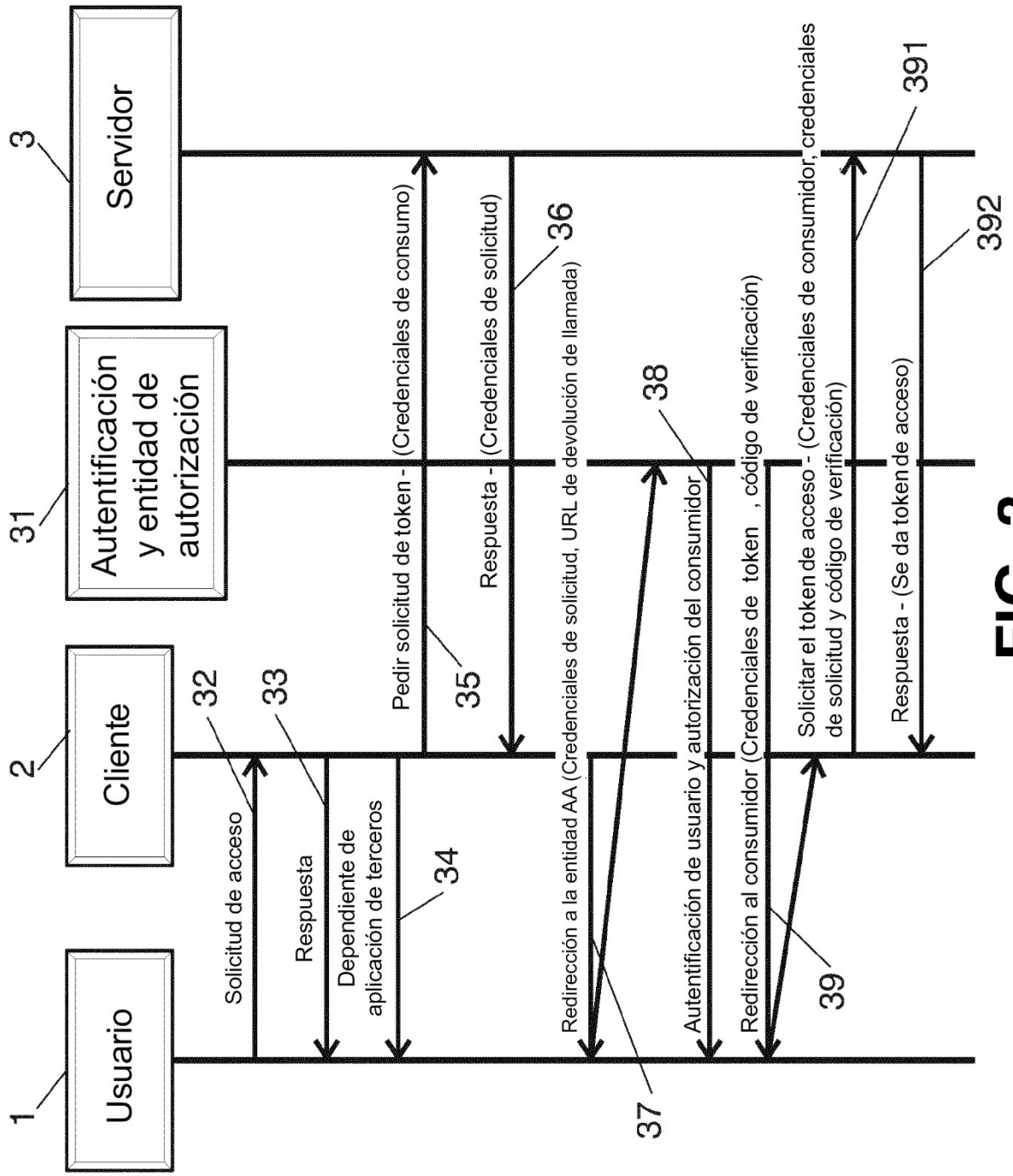
1
Usuario
2
Cliente
31
Autentificación y entidad de autorización
3
Servidor
Solicitud de acceso
32
Respuesta
33
Dependiente de aplicación de terceros
34
Pedir solicitud de token - (Credenciales de consumo)
35
Respuesta - (Credenciales de solicitud)
36
Redirección a la entidad AA (Credenciales de solicitud, URL de devolución de llamada)
37
Autentificación de usuario y autorización del consumidor
38
Redirección al consumidor (Credenciales de token , código de verificación)
39
Solicitar el token de acceso - (Credenciales de consumidor, credenciales de solicitud y código de verificación)
391
Respuesta - (Se da token de acceso)
392

FIG. 3

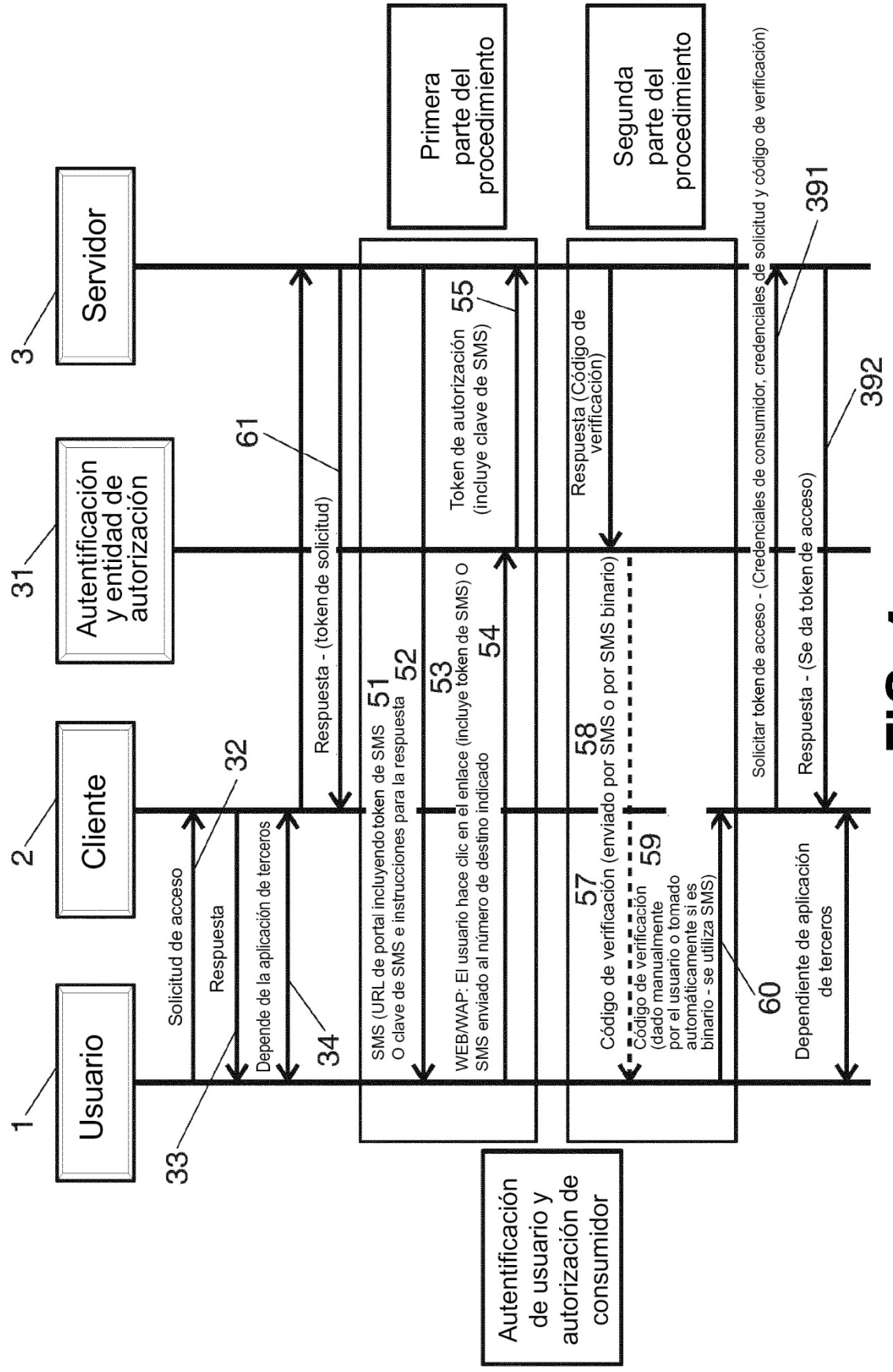
1
Usuario
2
Cliente
31
Autentificación y entidad de autorización
3
Servidor
Primera parte del procedimiento
Segunda parte del procedimiento
Autentificación de usuario y autorización de consumidor
Solicitud de acceso
32
Respuesta
33
Depende de la aplicación de terceros
34
Respuesta - (token de solicitud)
61
SMS (URL de portal incluyendo token de SMS O clave de SMS e instrucciones para la respuesta
51
52
WEB/WAP: El usuario hace clic en el enlace (incluye token de SMS) O SMS enviado al número de destino indicado
53
54
Token de autorización (incluye clave de SMS)
55
Código de verificación (enviado por SMS o por SMS binario)
57
58
Código de verificación (dado manualmente por el usuario o tomado automáticamente si es binario - se utiliza SMS)
59
Respuesta (Código de verificación)
Solicitar token de acceso - (Credenciales de consumidor, credenciales de solicitud y código de verificación)
391
Respuesta - (Se da token de acceso)
392
60
Dependiente de aplicación de terceros

FIG. 4