(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 624 841**

(51) Int. CI.:

G06F 17/22 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.12.2013 E 13382519 (0)**

(97) Fecha y número de publicación de la concesión europea: **15.02.2017 EP 2887608**

(54) Título: **Un método implementado por ordenador y sistema para una comunicación anónima y programa de ordenador para los mismos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.07.2017

(73) Titular/es:

TELEFONICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Vía, 28
28013 Madrid, ES

(72) Inventor/es:

GREENBERG-BARAK, MERAV y
NEYSTADT, JOHN (EUGENE)

(74) Agente/Representante:

ARIZTI ACHA, Monica

Un método implementado por ordenador y sistema para una comunicación anónima y programa de ordenador para los mismos

DESCRIPCIÓN

Campo de la invención

La presente invención se refiere en general al campo de los sistemas y métodos de comunicaciones de red, y más particularmente se refiere a un método implementado por ordenador, a un sistema y un programa de ordenador para los mismos para una comunicación anónima, es decir a través de WebRTC, VoIP, o cualquier otro sistema abierto

Antecedentes de la invención

La telefonía basada en Web (WebRTC) es una tecnología que permite compartir en tiempo real, datos, audio y video, entre navegadores. Como un conjunto de estándares, WebRTC proporciona a cualquier navegador la capacidad de compartir datos de aplicación y establecer teleconferencias, sin necesidad de instalar complementos software (plug in) o Software de terceras partes.

Los componentes de WebRTC se usan a través de interfaces de programación avanzadas en JavaScript (API). Actualmente, dichas API que fluyen a través de la red, representan los flujos de datos de audio y video, y la API de Conexión entre Pares, que permite a dos o más usuarios realizar una conexión de navegador a navegador. La API de Canal de Datos está también en desarrollo, permite la transmisión de otros tipos de datos para juegos en tiempo real, mensajería instantánea, transferencia de ficheros, y otros.

Actualmente, algunas áreas de aplicación en las que la WebRTC es importante es en la creación de números libres de tarificación (por ejemplo, los números 1-800- en los Estados Unidos), un número de teléfono especial que es gratis para el usuario llamante, y en cambio, el operador telefónico carga al usuario llamado el coste de la llamada, o en una llamada anónima a través de la Web.

El documento US 2012/124227 A1 divulga un sistema para proporcionar servicios VOIP basados en navegador. El sistema incluye un servidor web, un servidor de base de datos, un servidor de encuentro, y un servidor de medios de retransmisión. El servidor web está configurado para proporcionar una página web para un ordenador de usuario y un ordenador receptor para realizar una conexión de llamada en base a un enlace de llamada de ordenador a ordenador (CC) enviado desde el ordenador del usuario al ordenador receptor. El servidor de base de datos está acoplado al servidor web para proporcionar datos de usuario. Además, el servidor de encuentro está configurado para soportar un protocolo de flujo de medios en tiempo real (RTMFP) para permitir una comunicación directa entre iguales entre el ordenador de usuario y el ordenador receptor para establecer la conexión de llamada. El servidor de medios de retransmisión está configurado para soportar un protocolo de mensajería en tiempo real (RTMP), un RTMP tunelado (RTMPT), y un RTMP asegurado (RTMPS) y para ser un fallo para el servidor de encuentro. Además, el enlace de llamada CC se crea mediante el servidor web bajo una petición desde el ordenador de usuario y se envía al ordenador receptor.

Además, también es importante en el caso de que un negocio o un usuario quieran proporcionar un servicio a otras personas permitiendo a las últimas llamar a dicho negocio o usuario realizando únicamente un clic en un botón o hiperenlace (por ejemplo, desde la página Web del negocio). Sin embargo, no hay actualmente ninguna solución técnica en los servicios WebRTC (o en los servicios de Voz sobre IP (VoIP)) que permitan recibir dicha llamada después de que se ha realizado una autorización para dicha llamada manteniendo anónima la identidad del usuario llamado.

Sumario de la invención

Por lo tanto, un objeto de la presente invención es proporcionar un mecanismo que permita a un usuario o negocio a través de una página web recibir una comunicación autorizada tal como una llamada de audio, una llamada de video, un mensaje, etc. desde al menos otro usuario, esto es, no se tiene que proporcionar ninguna información con respecto a dicho otro usuario, protegiendo por lo tanto dicho usuario o negocio de un mal comportamiento, como comunicaciones de correos no deseados (spam) o acosos.

Para este fin, de acuerdo con un primer aspecto se proporciona un método implementado por ordenador para una comunicación anónima, incluyendo WebRTC, VoIP, u otros, en los que se proporciona una comunicación tal como una llamada de audio, una llamada de video, un mensaje de texto, un mensaje multimedia o un email entre un primer usuario que tiene un dispositivo de computación y al menos un segundo usuario que tiene un dispositivo de computación por medio del uso en al menos un servicio de comunicación accesible sobre una web. Al contrario de las propuestas conocidas, el método del primer aspecto comprende:

- autenticar, dicho servicio de comunicaciones, una vez que se realiza una petición por dicho primer usuario para registrarse en dicho servicio de comunicación, la información de credenciales de dicho primer usuario para autorizar dicha petición;
- solicitar, dicho primer usuario, a dicho servicio de comunicaciones generar un hiperenlace (es decir, un Localizador de Recursos uniforme, URL) que está asociado con la dirección de comunicación de dicho primer usuario;
- proporcionar, dicho primer usuario, dicho hiperenlace generado para al menos un segundo usuario:
- solicitar, dicho al menos un segundo usuario, iniciar una comunicación con dicho primer usuario haciendo clic directamente sobre dicho hiperenlace proporcionado, en el que la identidad de dicho al menos un segundo usuario se mantiene anónima y la identidad de dicho primer usuario se realiza en base a la información proporcionada en dicho hiperenlace; y
- autorizar, por un primer servidor en comunicación con dicho servicio de comunicación, dicha comunicación entre dicho al menos un segundo usuario y dicho primer usuario.

Por mantener anónima la identidad del segundo usuario tiene que entenderse que el segundo usuario no necesita proporcionar ninguna identificación o credencial tal como su número de teléfono, dirección IP, etc. para iniciar la comunicación con el primer usuario.

La petición de generar un hiperenlace incluye indicar si dicho hiperenlace a generar es privado o público.

De acuerdo con una realización, si se ha indicado que el hiperenlace es privado, este hiperenlace contendrá las condiciones de restricción de uso. En este caso la etapa de provisión se realizará enviando directamente dicho hiperenlace a través de un canal de comunicación tal como un email, un mensaje de texto, un mensaje multimedia o un mensaje instantáneo, por el primer usuario a dicho segundo usuario. Además, el servicio de comunicación usará el primer servidor para generar un token, que se incluirá en el hiperenlace a generar. De acuerdo con dicha realización, antes de dicha etapa de autorización, el token se valida por el primer servidor, comprobando dicho proceso de validación las condiciones de restricción de uso de dicho hiperenlace.

De acuerdo con una realización, si se ha indicado que el hiperenlace es público, este hiperenlace se publicará en una página web, tweet, email masivo, etc. En este caso y antes de que se realice dicha etapa de autorización, el servicio de comunicación requerirá a un segundo servidor la generación de un mecanismo de discriminación entre máquinas y humanos y de autorización tal como un mecanismo Captcha, o cualquier otro. A continuación, el servicio de comunicación enviará un desafío de discriminación entre máquinas y humanos y de autorización al segundo usuario y después de que este último resuelva dicho reto, el servicio de comunicación usará el primer servidor para generar una segunda URL incluyendo un token que contendrá las condiciones de restricciones de uso. En este punto, el servicio de comunicación, redirigirá el navegador del al menos un segundo usuario a dicha segunda URL generada, por medio de una redirección de HTTP, y ambos negociarán además una sesión para la comunicación. Finalmente, el primer servidor, validará el token comprobando que dicho hiperenlace está conforme con las condiciones de restricciones de uso.

Por medios de Captcha tiene que entenderse un tipo de prueba de reto - respuesta usada en computación para determinar si el usuario es o no una persona humana.

Las condiciones de restricción de uso preferiblemente limitan el número de intentos de comunicación en los cuales el hiperenlace es efectivo y/o el periodo de tiempo en el que el hiperenlace permanece válido.

De acuerdo con un segundo aspecto se proporciona un sistema de comunicaciones que comprende al menos un servicio de comunicación instalado sobre una Web para proporcionar una comunicación entre un primer usuario que tiene un dispositivo de computación y al menos un segundo usuario que tiene un dispositivo de computación. Al contrario de las propuestas conocidas, el servicio de comunicación incluye al menos: medios para la autenticación de la información de credenciales de usuario de dicho primer usuario; medios para la generación de un hiperenlace asociado con la dirección de comunicación de dicho primer usuario, y medios para la comunicación con un primer servidor, y dicho primer servidor incluye al menos medios para autorizar dicha comunicación entre dicho al menos un segundo usuario, y dicho primer usuario, una vez que el primer usuario ha proporcionado dicho hiperenlace generado a dicho segundo usuario y habiendo solicitado el último la iniciación de dicha comunicación haciendo clic directamente sobre dicho hiperenlace proporcionado.

De acuerdo con una realización, el sistema incluye además un segundo servidor configurado para generar un mecanismo de discriminación entre máquinas y humanos y de autorización.

Dicho medio para autorizar la comunicación, en una realización, incluye medios para validar un token comprobando las condiciones de restricciones de uso de dicho hiperenlace.

El sistema del segundo aspecto está adaptado para implementar el método del primer aspecto.

El tema objeto descrito en este documento se puede implementar en software en combinación con hardware y/o firmware, o cualquier combinación adecuada de los mismos. Por ejemplo, el tema objeto descrito en este documento se puede implementar en software ejecutado por un procesador.
De acuerdo con un tercer aspecto se proporciona un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta sobre un ordenador, un procesador de señales digitales, una red de puertas programables en campo, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador, o cualquier otra forma de hardware programable.

Breve Descripción de los Dibujos

Las anteriores y otras ventajas y características se harán más completamente entendibles a partir de la siguiente descripción detallada de las realizaciones, con referencia a los dibujos adjuntos que se deben considerar en un modo ilustrativo y no limitativo, en los que:

La Figura 1 ilustra una realización particular en la que el hiperenlace se indica que es privado.
La Figura 2 ilustra una realización particular en la que el hiperenlace se indica que es público.

Descripción Detallada de Varias Realizaciones

En referencia a la Fig. 1, un primer usuario 100 o Alice como se llama en dicha figura 1 se registra en un servicio de comunicaciones 300, una aplicación que proporciona capacidades de comunicación tales como la mensajería, llamadas de audio y video sobre la web y autenticación con sus credenciales (1). A continuación, el Servicio de comunicaciones 300 autentica dicho primer usuario 100. Si se requiere, se puede enviar un token de la autorización para indicar dicha autenticación.

A continuación, el primer usuario 100 solicita al servicio de comunicaciones 300 generar un hiperenlace o enlace click2call como se ilustra en la figura 1 que está asociado con la dirección de comunicación de dicho primer usuario 100. En el caso de que el primer usuario 100 haya recibido dicho token de autorización, este token también se puede proporcionar al servicio de comunicaciones 300 aumentando por lo tanto la seguridad. El primer usuario 100 de acuerdo con esta realización particular indicará que dicho hiperenlace es un hiperenlace privado que puede limitar opcionalmente el número de intentos de comunicaciones, por ejemplo, a cinco de acuerdo con esta realización, pero se podría limitar a cualquier otro número de intentos, con fecha de expiración (3). El número de intentos de comunicación restringe tanto el número de segundos usuarios 200 o las personas a las que más tarde el primer usuario 100 enviará el hiperenlace (8) como el número de intentos de comunicación que pueden hacerse con este hiperenlace.

A continuación, el servicio de comunicaciones accede a un primer servidor 400 o el Servidor del Click2Call para crear un token o token de acceso con los parámetros proporcionados por el primer usuario 100 (es decir, los intentos de comunicación y el tiempo de expiración (4)). El primer servidor 400 genera el token y mantiene el token con los parámetros (5). A continuación, el primer servidor 400 envía el token de acceso al Servicio de Comunicación 300 (6) incluyéndose dicho token de acceso además en dicho hiperenlace a generar (7). A continuación, el primer usuario 100 envía el hiperenlace a un segundo usuario 200 denominado como Bob en la figura (o a más personas) preferiblemente a través de un email, y mensaje instantáneo, u otro canal de comunicación (8).

A continuación, el segundo usuario 200 (o personas adicionales) hace clic en el hiperenlace para establecer un intento de comunicación (9). El Servicio de comunicaciones 300 solicita al primer servidor 400 validar el token de acceso (10). En este momento, el primer servidor 400 comprueba que dicho token de acceso existe realmente, esto es que el token de acceso no ha expirado y que el contador de tokens de acceso está por encima de cero, a continuación, el primer servidor 400 disminuye en 1 el contador (11). El primer servidor 400 en base a dicha comprobación autorizará la comunicación (19), de modo que el servicio de comunicaciones 300 establecerá una comunicación entre el primer usuario 100 y el segundo usuario 200 (13). Ahora ambos usuarios pueden mantener una comunicación anónima.

En referencia a la Fig. 2, ahora el primer usuario o Alice 100 indica que dicho hiperenlace es público. De acuerdo con esta realización, una vez que el primer usuario 100 ha solicitado la generación del hiperenlace al servicio de comunicación 300 (3) y habiéndose enviado el último de vuelta al primer usuario 100 (4), el primer usuario 100 proporciona el hiperenlace recibido publicándolo en una página Web, una página web privada o pública donde un botón clic2call o hiperenlace se puede publicar, tal como un blog, sitio de comercio electrónico, foro web, etc. (5). A continuación, el segundo usuario o Bob 200 accede a dicha página web (6) por ejemplo a través de su navegador 201 y hace clic sobre el hiperenlace recibido. Un intento de comunicación se realiza desde el segundo usuario 200 al servicio de comunicaciones 300 (7). El servicio de comunicaciones 300 solicita a un segundo servidor 500, por

ejemplo, un servidor Captcha, que genere un reto Captcha (8-9) permitiendo por lo tanto el bloqueo de la comunicación de correo basura por un sistema automatizado. A continuación, el servicio de comunicación envía el reto Captcha al segundo usuario por medio de dicho navegador del segundo usuario 201 (10). El segundo usuario 200 resuelve el reto Captcha (11).

En este momento, el servicio de comunicación 300 usa el primer servidor 400 para generar una segunda URL que incluye el token de acceso que encierra dichas condiciones de restricción de uso (es decir, intentos de comunicación y tiempo de expiración) (12, 13, 14). A continuación, el servicio de comunicación redirige, por medio de una redirección de HTTP, dicho segundo navegador de usuario 201 a dicha segunda URL generada que incluye el token de acceso, que a continuación solicita al servicio de comunicación 300, de forma transparente al segundo usuario 200, esto es sin proporcionar la identidad del segundo usuario 200, negociar una sesión de comunicaciones (15-16).

A continuación, el servicio de comunicación 300 solicita al primer servidor 400 que valide dicho token de acceso comprobando las condiciones de restricciones de uso del hiperenlace, por ejemplo, si no ha expirado y a continuación el primer servidor 400 disminuye el contador en 1 (18). Finalmente, el primer servidor 400 en base a dicha comprobación autorizará la comunicación (19), de modo que el servicio de comunicación 300 establecerá una comunicación entre el primer usuario 100 y el segundo usuario 200.

Se ha observado que dependiendo de qué realización se considere, la Fig. 1 o la Fig. 2, el token creada por el primer servidor 100 (o token de acceso) se crea en una etapa diferente dependiendo de que el hiperenlace generado sea privado o público.

La presente invención posibilita a un primer usuario 100 o cualquier otro negocio para recibir llamadas autorizadas gratuitas creando un hiperenlace limitado en tiempo y cantidad o una URL, y proporcionándolo por un envío directo o por una publicación en la página web, al usuario correspondiente que puede usar dicho hiperenlace para establecer una comunicación, por ejemplo, una llamada de audio sin revelar la identificación del usuario tal como el número de teléfono real.

Además, la invención limita además el número de intentos de comunicaciones y el periodo de tiempo durante el cual se puede realizar dicha comunicación anónima usando dicho hiperenlace.

La invención incluso permite a una página web comercial proporcionar clic2call autorizadas y protegidas.

El alcance de la presente invención se define en el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Un método implementado por ordenador para una comunicación anónima, en el que se proporciona una comunicación entre un primer usuario (100) que tiene un dispositivo de computación y al menos un segundo usuario (200) que tiene un dispositivo de computación por medio del uso de al menos un servicio de comunicación (300) accesible sobre una web, comprendiendo dicho método:

- autenticar, mediante dicho servicio de comunicación (300), una vez que se ha recibido una petición desde dicho primer usuario (100) para registrarse en dicho servicio de comunicaciones (300), información de credenciales de usuario de dicho primer usuario (100) para autorizar dicha petición;
- solicitar, mediante dicho primer usuario (100), a dicho servicio de comunicaciones (300) generar un hiperenlace que está asociado con la dirección de comunicación de dicho primer usuario (100);
- proporcionar, mediante dicho primer usuario (100), a través de un canal de comunicación o una página web de dicha web, dicho hiperenlace generado a al menos un segundo usuario (200);
- solicitar, mediante dicho al menos un segundo usuario (200), iniciar dicha comunicación con dicho primer usuario (100) haciendo clic directamente sobre dicho hiperenlace proporcionado, en el que la identidad de dicho primer usuario (100) se realiza en base a la información proporcionada sobre dicho hiperenlace; y
- autorizar, por un primer servidor (400) en comunicación con dicho servicio de comunicación (300), dicha comunicación entre dicho al menos un segundo usuario (200) y dicho primer usuario (100),

caracterizado porque:

dicha petición para generar un hiperenlace comprende indicar que dicho hiperenlace que se genera es público;
en dicha etapa de petición para iniciar la comunicación con el primer usuario (100), el segundo usuario (200) no proporciona ninguna información de identificación o de credencial del segundo usuario (200), de manera que su identidad se mantiene anónima; y **por que** el método comprende antes de realizar dicha etapa de autorización:

- solicitar, mediante el servicio de comunicación (300), la generación de un control humano y un mecanismo de autorización a un segundo servidor (500);
- solucionar, el al menos segundo usuario (200), al recibir un desafío para dicho control humano y mecanismo de autorización desde el servicio de comunicación (300), dicho desafío; y
- usar, mediante el servicio de comunicación (300), dicho primer servidor (400) para generar una segunda URL que incluye un token que encierra condiciones de restricción de uso de dicho hiperenlace generado.

2. Un método implementado por ordenador de acuerdo con la reivindicación 1, que comprende, además:

- redirigir, por el servicio de comunicación (300), dicho al menos un segundo usuario (200), en respuesta a dicha resolución del reto, a dicha segunda URL generada, incluyendo dicho token;
- negociar, por el servicio de comunicación (300) y el al menos un segundo usuario (200), una sesión para la comunicación; y
- validar, por el primer servidor (400), dicho token, comprendiendo dicho proceso de validación la comprobación de dichas condiciones de restricciones de uso.

3. Un método implementado por ordenador de acuerdo con la reivindicación 1, en el que dicho mecanismo de discriminación entre máquinas y humanos y de autorización comprende al menos un mecanismo Captcha.

4. Un método implementado por ordenador de acuerdo con las reivindicaciones anteriores, en el que dichas condiciones de restricciones de uso limitan al menos el número de intentos de comunicación en los que dicho hiperenlace es efectivo y/o el periodo de tiempo en el que dicho hiperenlace permanece válido.

5. Un método implementado por ordenador de acuerdo con las reivindicaciones anteriores, en el que dicha comunicación comprende al menos una llamada de audio, una llamada de video, un mensaje de texto, un mensaje multimedia, o un email.

6. Un sistema de comunicaciones, que comprende:

- un servicio de comunicación (300) instalado en una web para proporcionar una comunicación anónima entre un primer usuario (100) que tiene un dispositivo de comunicación y al menos un segundo usuario (200) que tiene un dispositivo de computación, comprendiendo dicho servicio de comunicación (300) comprende al menos:

- medios para autenticar la información de credenciales de usuario de dicho primer usuario (100);
- medios para generar un hiperenlace asociado con la dirección de comunicación de dicho primer usuario (100); y
- medios para comunicar con un primer servidor (400); y

- dicho primer servidor (400) comprende al menos medios para autorizar dicha comunicación entre dicho el segundo usuario (200) y dicho primer usuario (100),

caracterizado porque:

- el sistema de comunicación también comprende un segundo servidor (500) configurado para generar un control humano y mecanismo de autorización al recibir una petición desde el servicio de comunicación (300);
- dichos medios para autorizar dicha comunicación incluye medios para validar un token que encierra condiciones de restricción de uso de dicho hiperenlace generado; y **por que**
- el sistema de comunicación está adaptado para implementar el método de acuerdo con la reivindicación 1.

7. Un programa de ordenador que comprende medios de código del programa de ordenador adaptado para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta sobre un ordenador, un procesador de señal digital, una red de puertas programables en campo, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

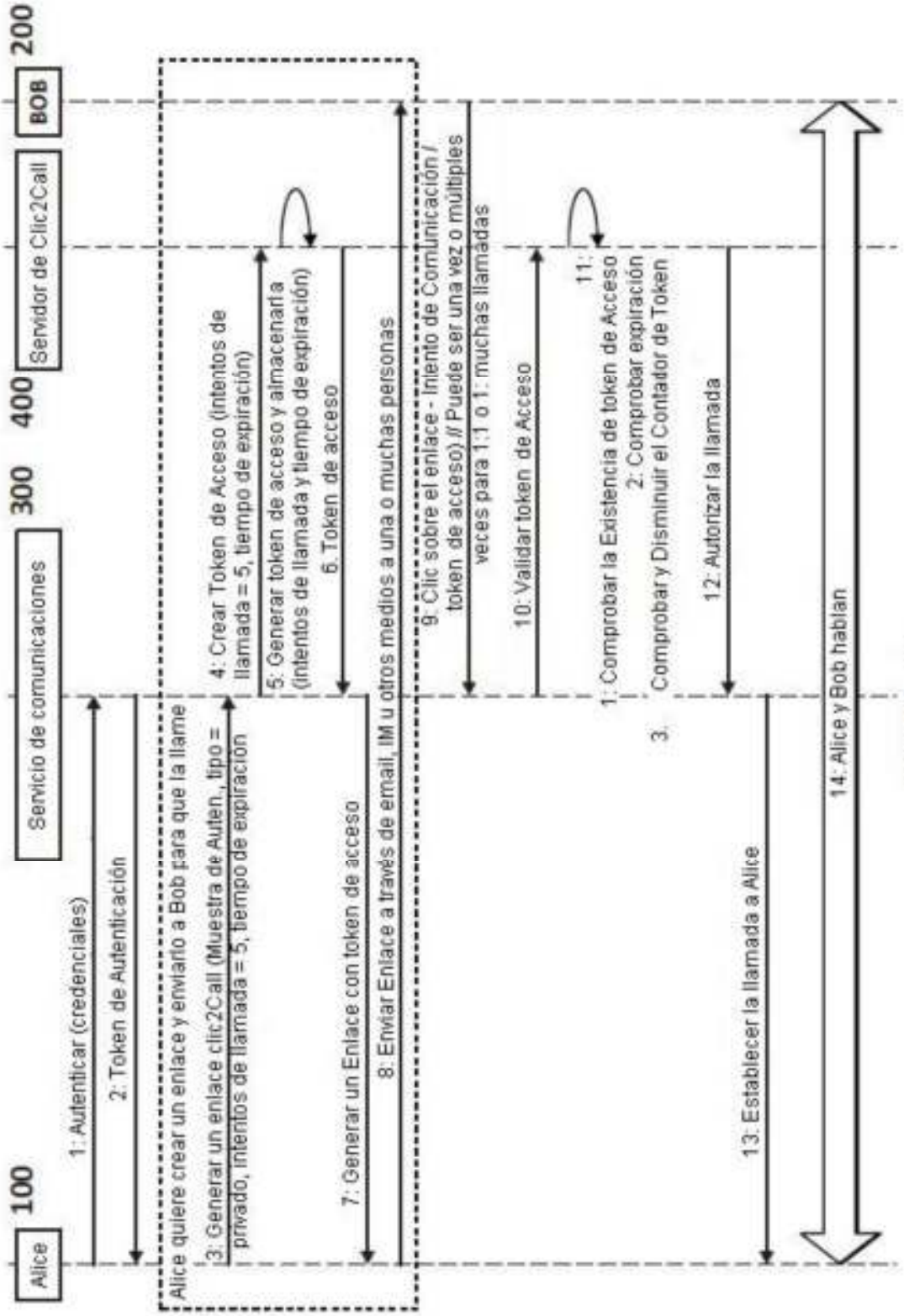
Alice
100
Servicio de comunicaciones
300
Servidor de Clic2Call
400
BOB
200
1: Autenticar (credenciales)
2: Token de Autenticación
Alice quiere crear un enlace y enviarlo a Bob para que la llame
3: Generar un enlace clic2Call (Muestra de Auten., tipo = privado, intentos de llamada = 5, tiempo de expiración
4: Crear Token de Acceso (intentos de llamada = 5, tiempo de expiración)
5: Generar token de acceso y almacenarla (intentos de llamada y tiempo de expiración)
6. Token de acceso
7: Generar un Enlace con token de acceso
8: Enviar Enlace a través de email, IM u otros medios a una o muchas personas
9: Clic sobre el enlace - Inicio de Comunicación / token de acceso) // Puede ser una vez o múltiples veces para 1:1 o 1: muchas llamadas
10: Validar token de Acceso
11:
1: Comprobar la Existencia de token de Acceso
2: Comprobar expiración
3.
Comprobar y Disminuir el Contador de Token
12: Autorizar la llamada
13: Establecer la llamada a Alice
14: Alice y Bob hablan

FIG. 1

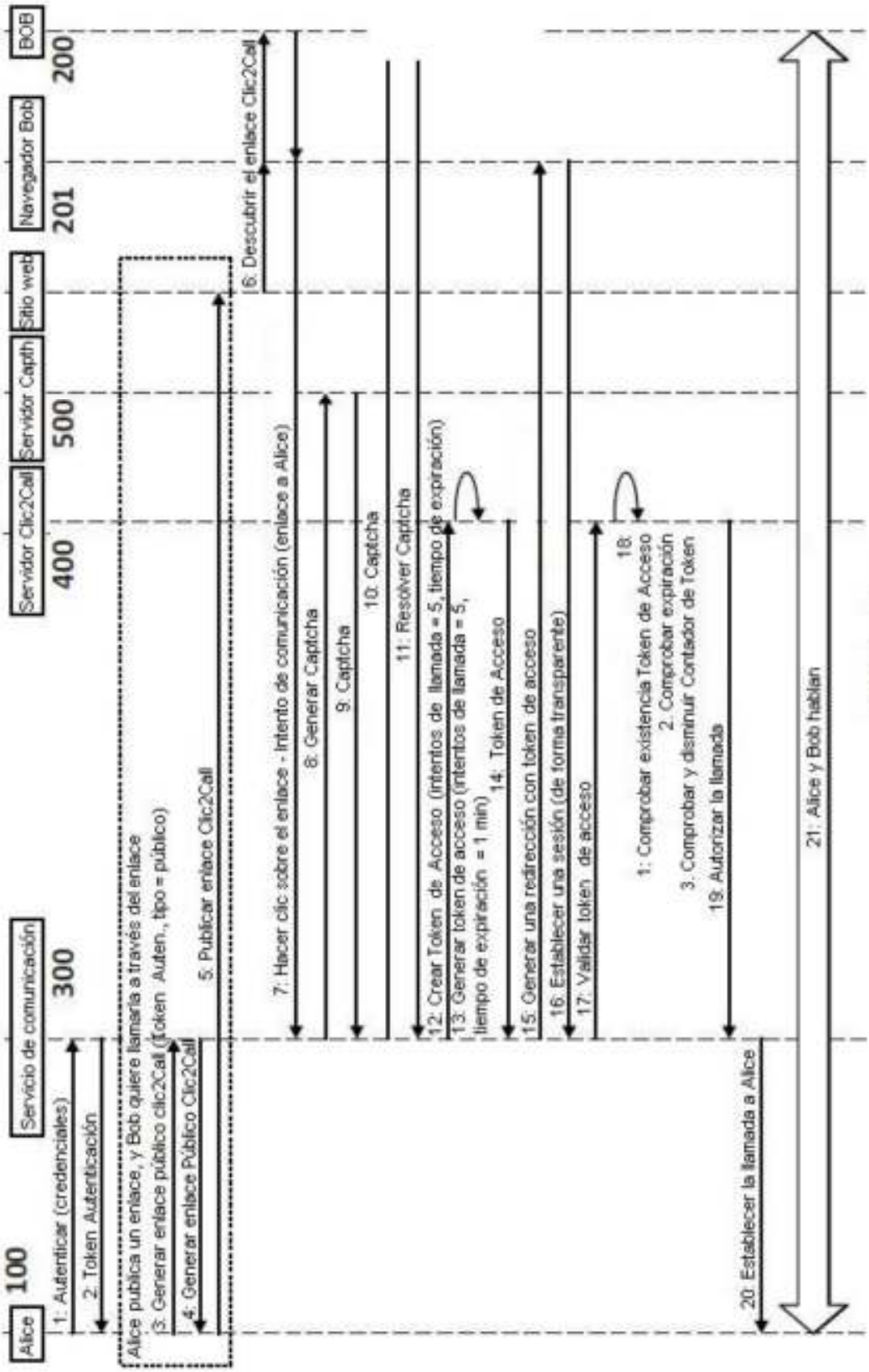
Alice
100
Servicio de comunicación
300
Servidor Clic2Call
400
Servidor Capth
500
Sitio web
Navegador Bob
201
BOB
200
1: Autenticar (credenciales)
2: Token Autenticación
Alice publica un enlace, y Bob quiere llamaría a través del enlace
3: Generar enlace público clic2Call (Token Auten., tipo = público)
4: Generar enlace Público Clic2Call
5: Publicar enlace Clic2Call
6: Descubrir el enlace Clic2Call
7: Hacer clic sobre el enlace - Intento de comunicación (enlace a Alice)
8: Generar Captcha
9: Captcha
10: Captcha
11: Resolver Captcha
12: Crear Token de Acceso (intentos de llamada = 5, tiempo de expiración)
13: Generar token de acceso (intentos de llamada = 5, tiempo de expiración = 1 min)
14: Token de Acceso
15: Generar una redirección con token de acceso
16: Establecer una sesión (de forma transparente)
17: Validar token de acceso
18:
1: Comprobar existencia Token de Acceso
2. Comprobar expiración
3. Comprobar y disminuir Contador de Token
19: Autorizar la llamada
20: Establecer la llamada a Alice
21: Alice y Bob hablan

FIG. 2