(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 481**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06Q 20/00 (2012.01)
G06Q 20/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.04.2018 E 18166874 (0)**

(97) Fecha y número de publicación de la concesión europea: **13.05.2020 EP 3553719**

(54) Título: **Sistema para acceder de forma fiable a un recurso protegido**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.01.2021

(73) Titular/es:

BARCLAYS EXECUTION SERVICES LIMITED (100.0%)
1 Churchill Place
London E14 5HP, GB

(72) Inventor/es:

HOLT, DICKON y
FORREST, MICHAEL

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Sistema para acceder de forma fiable a un recurso protegido

Campo técnico

[0001] Esta divulgación se refiere a un sistema, un método y un programa informático para acceder de forma fiable a un recurso protegido en un sistema cliente en nombre de un usuario.

Antecedentes

[0002] El marco de autorización OAuth ("Autorización abierta") 2.0 permite que una aplicación de terceros obtenga acceso limitado a un servicio HTTP, como el acceso a un recurso protegido. La aplicación de terceros puede obtener acceso al servicio HTTP en nombre del propietario del recurso al organizar una interacción de aprobación entre el propietario del recurso y el servicio HTTP. Alternativamente, la aplicación de terceros puede obtener acceso al servicio HTTP en su propio nombre.

[0003] La Fig. 1 ilustra una visión general del flujo del protocolo OAuth 2.0, que involucra las siguientes cuatro entidades: un propietario de recursos 1, un cliente 3, un servidor de autorización 5 y un servidor de recursos 7. El propietario de recursos 1 es una entidad que es capaz de otorgar acceso a un recurso protegido. El propietario del recurso 1 puede ser una persona, denominada usuario que opera un dispositivo de usuario. El cliente 3 es una entidad, o una aplicación, que puede realizar una solicitud de acceso al recurso protegido en nombre del propietario del recurso 1, cuando lo autoriza el propietario del recurso 1. El servidor de autorización 5 es una entidad que otorga y emite tokens de acceso para el cliente después de autenticar con éxito el propietario del recurso y obtener la autorización. El servidor de recursos 7 es una entidad que aloja el recurso protegido y es capaz de aceptar y responder a las solicitudes del recurso protegido mediante tokens de acceso.

[0004] Los tokens de acceso, como los emitidos por el servidor de autorización 5, son credenciales utilizadas para acceder a recursos protegidos. Un token de acceso es una cadena que representa una autorización emitida al cliente. La cadena suele ser opaca para el cliente. Los tokens representan ámbitos específicos y duraciones de acceso, otorgadas por el propietario del recurso, y aplicadas por el servidor de recursos y el servidor de autorización.

[0005] Un token de acceso puede denotar un identificador utilizado para recuperar la información de autorización o puede contener la información de autorización de manera verificable (es decir, una cadena de token que consta de algunos datos y una firma). Los tokens de acceso pueden tener diferentes formatos, estructuras y métodos de utilización (p. ej., propiedades criptográficas) según los requisitos de seguridad del servidor de recursos.

[0006] Se puede usar un token de acceso para identificar a un cliente. Cuando se utiliza un token de acceso en este contexto, puede denominarse en este documento como un token de concesión, en lugar de un token de acceso. Sin embargo, un token de concesión podría describirse igualmente como un token de acceso.

[0007] El servidor de autorización 5 puede emitir tokens de actualización, que son credenciales utilizadas para obtener tokens de acceso. El servidor de autorización emite tokens de actualización para el cliente y se utilizan para obtener un nuevo token de acceso cuando el token de acceso actual deja de ser válido o caduca, o para obtener tokens de acceso adicionales con una vida útil idéntica o más limitada y menos permisos que los autorizados por el propietario del recurso). La emisión de un token de actualización es opcional a discreción del servidor de autorización. Si el servidor de autorización emite un token de actualización, se incluye al emitir un token de acceso.

[0008] Un token de actualización es una cadena que representa la autorización otorgada al cliente por el propietario del recurso. La cadena suele ser opaca para el cliente. El token denota un identificador utilizado para recuperar la información de autorización.

[0009] En el paso 11, el cliente 3 solicita autorización del propietario del recurso 1 para acceder al recurso protegido. La solicitud de autorización se puede hacer directamente al propietario del recurso 1, o indirectamente a través del servidor de autorización 5 como intermediario.

[0010] En el paso 12, el cliente 3 recibe una concesión de autorización, que es una credencial que representa la autorización proporcionada por el propietario del recurso 1. Esta autorización puede expresarse usando uno de una pluralidad de "tipos de concesión" descritos en el Marco de Autorización. El tipo de concesión de autorización depende de los métodos utilizados por el cliente 3 para solicitar autorización y los tipos admitidos por el servidor de autorización 5.

[0011] En el paso 13, el cliente 3 solicita un token de acceso mediante la autenticación con el servidor de autorización 5 y la presentación de la concesión de autorización. La autenticación puede expresarse usando uno de una pluralidad de "tipos de autenticación" para autenticar la identificación del cliente 3 en el servidor de autorización 5. El tipo de

autenticación depende del (de los) método(s) utilizado(s) por el cliente 3 para autenticarse y el (los) tipo(s) soportado(s) por el servidor de autorización 5.

[0012] En el paso 14, el servidor de autorización 5 autentica al cliente 3 y valida la concesión de autorización, y si es válido, emite un token de acceso.

[0013] En el paso 15, el cliente 3 solicita el recurso protegido del servidor de recursos 7 y se autentica en el servidor de recursos 7 presentando el token de acceso.

[0014] En el paso 16, el servidor de recursos 7 valida el token de acceso. Si el token de acceso es válido, el servidor de recursos 7 atiende la solicitud transmitiendo el recurso protegido al cliente 3.

[0015] Como se explicó anteriormente, el servidor de autorización 5 puede soportar diferentes tipos de método de concesión y diferentes tipos de método de autenticación. En los sistemas convencionales, el cliente 3 está preconfigurado para usar un tipo de método de concesión y un tipo de método de autenticación para comunicarse con el servidor de autorización 5 para obtener el token de acceso. En estos sistemas convencionales, si el tipo de método de concesión o el tipo de método de autenticación que admite el servidor de autorización 5 cambia a un tipo de método diferente, el cliente 3 usaría el método de concesión o autenticación incorrecto para comunicarse con el servidor de autorización 5. Por lo tanto, el cliente 3 sería incapaz de obtener el token de acceso.

[0016] Existe la necesidad de un sistema flexible y más confiable que sea resistente a los cambios en los tipos de métodos de concesión y autenticación soportados por un servidor de autorización 5, para que un cliente pueda acceder de manera confiable a los recursos protegidos.

Resumen

[0017] En un aspecto de la invención, se proporciona un método implementado por computadora para obtener un token de acceso para proporcionar acceso a un recurso protegido almacenado en un sistema de recursos, comprendiendo el método: almacenar, en un sistema cliente: una pluralidad de porciones de código del método de concesiones, cada una de las cuales es ejecutable para obtener acceso al token de acceso usando uno de una pluralidad de tipos de método de concesión, en donde cada tipo respectivo de método de concesión es diferente a los otros tipos de método de concesión; y una pluralidad de porciones de código del método de autenticación, cada una ejecutable para autenticar el sistema cliente usando un método de autenticación diferente, en donde cada tipo respectivo de método de autenticación es diferente a los otros tipos de método de autenticación; almacenar, en el sistema cliente, una base de datos configurable que comprende una pluralidad de identificadores del sistema de autorización, cada uno indicativo de un sistema de autorización respectivo, en donde cada uno de la pluralidad de identificadores del sistema de autorización está asociado con uno o más de la pluralidad de tipos de métodos de concesión que son soportados por el sistema de autorización respectivo, y cada uno de la pluralidad de identificadores del sistema de autorización está asociado con uno o más de la pluralidad de tipos de métodos de autenticación soportados por el sistema de autorización respectivo; recibir, en el sistema cliente, desde un dispositivo de usuario una solicitud de acceso que comprende una instrucción para que el sistema cliente acceda a un recurso protegido, comprendiendo la instrucción un identificador de solicitud indicativo de un sistema de autorización para autorizar el acceso al recurso protegido; identificar, en la base de datos configurable, un tipo de método de concesión seleccionado de uno o más de los tipos de métodos de concesión asociados con un identificador del sistema de autorización correspondiente al identificador de solicitud; identificar, en la base de datos configurable, un tipo de método de autenticación seleccionado, de uno o más de los tipos de métodos de autenticación asociados con el identificador del sistema de autorización correspondiente al identificador de solicitud; ejecutar, en el sistema del cliente, la parte del código del método de concesión correspondiente al tipo de método de concesión seleccionado para solicitar el token de acceso para acceder al recurso protegido; ejecutar, en el sistema del cliente, la parte del código del método de autenticación correspondiente al tipo de método de autenticación seleccionado para autenticar el sistema del cliente en el sistema de autorización; y recibir el token de acceso en el sistema del cliente desde el servidor de autorización, en respuesta a la ejecución de la parte del código del método de concesión y la parte del código del método de autenticación.

[0018] En el método, el sistema cliente mantiene una base de datos configurable que indica los tipos de método de autenticación y concesión que son compatibles con cada sistema de autorización con el que el sistema cliente puede comunicarse para obtener un token de acceso para acceder al recurso protegido. Además, el sistema del cliente almacena una pluralidad de porciones de código, cada ejecutable para realizar cualquiera de los métodos de concesión o autenticación admitidos. Por lo tanto, cuando el sistema cliente solicita el token de acceso, el sistema cliente puede determinar los métodos correctos de concesión y autenticación y ejecutar estos métodos en consecuencia para recibir el token de acceso. Por lo tanto, el sistema del cliente puede adaptarse a una variedad de diferentes métodos de autenticación y concesión que pueden ser compatibles en diferentes momentos por una variedad de servidores de autorización, lo que proporciona una mayor flexibilidad y resistencia.

Breve descripción de los dibujos

[0019] Se describirán realizaciones de la invención, a modo de ejemplo, con referencia a los siguientes dibujos, en los que:

Fig. 1 ilustra un diagrama de secuencia de protocolo del marco OAuth 2.0;

Fig. 2 ilustra la arquitectura general de un sistema para acceder a un recurso protegido;

Figs. 3 y 4 ilustran un diagrama de secuencia de protocolo de una invención implementada en computadora para acceder a un recurso protegido;

Fig. 5 ilustra un diagrama de flujo de un método implementado por computadora en donde un sistema cliente está configurado para ejecutar un método de autenticación seleccionado y un método de concesión para obtener un token de acceso utilizado para acceder a un recurso protegido;

Fig. 6 ilustra un diagrama de flujo de un método implementado por computadora en donde un sistema cliente actualiza un token de concesión en función de su tiempo de vencimiento;

Fig. 7 ilustra un diagrama de flujo del método implementado por computadora para administrar y almacenar tokens de acceso válidos e inválidos;

Fig. 8 ilustra un diagrama esquemático de un sistema cliente; y

Fig. 9 ilustra un diagrama esquemático de un dispositivo de ejemplo en el sistema.

Descripción detallada

[0020] Con referencia a la Fig. 2, hay un sistema 100 para gestionar el acceso a los recursos protegidos. El sistema 100 comprende uno o más dispositivos de usuario 101, un sistema de cliente 103 y un sistema externo 104, que comprende un sistema de autorización 105 y un sistema de recursos 107.

[0021] El dispositivo de usuario 101 puede considerarse como el propietario de recursos 1, el sistema cliente 103 puede considerarse como el cliente 3, el sistema de autorización 105 puede considerarse como el servidor de autorización 5, y el sistema de recursos 107 puede considerarse como el servidor de recursos 7 al considerar los métodos y sistemas descritos en este documento en términos del protocolo OAuth 2.0.

[0022] El sistema externo 104 está configurado para almacenar datos asociados con usuarios de dispositivos, tales como el dispositivo de usuario 101. Los datos almacenados en el sistema externo 104 pueden comprender recursos protegidos, tales como uno o más elementos de datos seguros.

[0023] Cada uno de los recursos protegidos puede ser indicativo de información privada relacionada con un usuario del sistema externo 104. En un ejemplo específico, cada elemento de datos almacenado en el sistema externo 104 comprende datos financieros relacionados con el usuario, tales como detalles que permiten al usuario realizar pagos o los detalles de transacciones financieras anteriores realizadas por el usuario.

[0024] Los siguientes sistemas y métodos se describen en el contexto de la gestión del acceso a los datos financieros en términos del protocolo OAuth 2.0. Sin embargo, estos sistemas y métodos podrían usarse para administrar el acceso a cualquier tipo de recurso protegido para el cual el acceso por parte de terceros no autorizados se restringirá utilizando otro protocolo adecuado, como SAML, OpenID y similares.

[0025] El sistema cliente 103 está configurado para acceder a recursos protegidos almacenados en el sistema externo 104, a petición de un usuario.

[0026] El sistema externo 104 puede comprender una pluralidad de subsistemas, *p. ej.*, una pluralidad de servidores. En el ejemplo descrito aquí, el sistema externo 104 comprende el sistema de autorización 105 y el sistema de recursos 107. El servidor de autorización 105 está configurado para autorizar solicitudes de acceso a recursos protegidos que están almacenados en el sistema de recursos 107. Alternativamente, el sistema externo 104 puede comprender un único servidor para realizar estas funciones.

[0027] El sistema cliente 103 puede comprender una pluralidad de subsistemas, *p. ej.,* una pluralidad de servidores. En el ejemplo descrito aquí, el sistema cliente 103 comprende un motor de recuperación 103a y un servidor de administración de tokens (TMS) 103b. El motor de recuperación 103a está configurado para interactuar con el dispositivo de usuario 101, y el TMS 103b está configurado para interactuar con el sistema externo 104. Alternativamente, el sistema cliente 103 comprende un único servidor para realizar estas funciones.

[0028] En los siguientes ejemplos, los datos seguros y los recursos protegidos se denominan accesibles por un usuario y los datos están asociados con el usuario. Por ejemplo, el usuario puede tener acceso a una cuenta de usuario en

línea, como una cuenta bancaria en línea, a través de una interfaz de cuenta proporcionada por el sistema externo 104. En este escenario, al usuario se le puede asignar un nombre de usuario único y un secreto compartido (*p. ej.* información de inicio de sesión), como una contraseña, que se puede utilizar para acceder a la cuenta de usuario a través de la interfaz de la cuenta. Una vez que el usuario ha accedido a la cuenta de usuario, ese usuario puede acceder a los datos a través de la cuenta de usuario. Por lo tanto, el usuario puede acceder a los datos mediante la información de inicio de sesión que es exclusiva del usuario.

[0029] Los datos seguros y los recursos protegidos que son accesibles por el primer usuario pueden ser accesibles por el propio sistema externo 104. Los datos seguros y los recursos protegidos pueden ser accesibles solo por el usuario, a menos que el usuario autorice lo contrario. En otras palabras, se evita que los datos/recursos protegidos se envíen a un dispositivo o sistema que sea remoto y distinto del sistema externo 104, como el sistema cliente 103, sin que el usuario correspondiente proporcione autorización al sistema externo 104 para los datos que se enviarán a un dispositivo o sistema remoto.

[0030] Cada uno de los sistemas externos 104, el sistema cliente 103 y el dispositivo de usuario 101 están dispuestos para comunicarse entre sí a través de una red de comunicaciones 110. La red de comunicaciones 110, en este ejemplo, es Internet 110. Sin embargo, se apreciará que podría usarse cualquier forma adecuada de red de comunicaciones 110.

[0031] Cada uno de los sistemas externos 104, el sistema cliente 103 y el dispositivo de usuario 101 están habilitados para la web y pueden comprender una pantalla, una interfaz de usuario, un procesador y una memoria. Los dispositivos y sistemas 101, 103, 104 pueden estar dispuestos para comunicar datos entre sí a través de cualquier protocolo de comunicación o conexión adecuados. Por ejemplo, los dispositivos y sistemas 101, 103, 104 pueden comunicarse entre sí a través de una conexión por cable y/o inalámbrica.

[0032] El dispositivo de usuario 101 puede ser cualquier tipo adecuado de dispositivo de computación personal, como una computadora portátil, una computadora de escritorio, un teléfono habilitado para la web, como un teléfono inteligente o una tableta. El sistema cliente 103 y el sistema externo 104 pueden ser cualquier tipo adecuado de sistema informático o colección de sistemas informáticos, como un servidor o una colección de servidores.

[0033] En referencia a las Figs. 3 y 4, hay un método implementado por computadora en donde el sistema cliente 103 obtiene acceso a un recurso protegido asociado con el usuario del dispositivo de usuario 101 desde el sistema externo 104.

[0034] En el paso 301, el dispositivo de usuario 101 transmite una solicitud de acceso al motor de recuperación 103a en el sistema cliente 103. La solicitud de acceso comprende una instrucción para que el sistema cliente 104 inicie el acceso al recurso protegido almacenado en el sistema externo 104, en otras palabras, la solicitud de acceso indica la intención del usuario de que el sistema cliente 103 acceda al recurso protegido.

[0035] En respuesta a la solicitud de acceso recibida del dispositivo de usuario 101, el sistema cliente 103 realiza los pasos 303 a 307 para obtener un token de concesión del sistema externo 104. El sistema 103 de cliente puede usar el token de concesión para identificarse al sistema externo 104 para iniciar solicitudes para el recurso protegido.

[0036] En el paso 303, el motor de recuperación 103a transmite una solicitud de token de concesión al TMS 103b.

[0037] En el paso 305, el TMS 103b reenvía la solicitud del token de concesión al sistema de autorización 105 en el sistema externo 104. El servidor de autorización 105 valida la solicitud del token de concesión. Si la solicitud del token de concesión es válida, el sistema de autorización 105 responde transmitiendo el token de concesión al TMS 103b.

[0038] En el paso 307, si se ha recibido el token de concesión, el TMS 103b reenvía el token de concesión al motor de recuperación 103a.

[0039] Una vez que el sistema cliente 103 ha recibido el token de concesión, los pasos 309 y 311 se pueden realizar para recibir un identificador de intención del sistema externo 104. El identificador de intención es una etiqueta de identificación que se puede usar para identificar una solicitud específica desde el usuario para que el sistema cliente 103 acceda a un recurso protegido asociado con el usuario desde el sistema externo 104 (es decir, la intención del usuario para que el sistema cliente 103 acceda al recurso protegido). El sistema cliente 103 puede recibir el identificador de intención, si se ha emitido previamente con un token de concesión válido.

[0040] En el paso 309, el motor de recuperación 103a transmite una solicitud de intención al sistema de recursos 107 en el sistema externo 104. La solicitud de intención se envía con el token de concesión recibido previamente, que identifica el sistema cliente 103 al sistema externo 104.

[0041] En el paso 311, en respuesta a la solicitud de intención, el sistema externo 104 valida el token de concesión. Si la solicitud de intención es válida, el sistema de recursos 107 responde transmitiendo un identificador de intención al TMS 103a.

[0042] En el paso 313, el motor de recuperación 103a reenvía el identificador de intención al dispositivo de usuario 101. Además, se envía una instrucción para redirigir al sistema de autorización 105 al dispositivo de usuario 101 junto con el identificador de intención. La instrucción de redireccionamiento puede comprender una URL correspondiente al sistema de autorización 105.

[0043] En el paso 315, el dispositivo de usuario 101 es redirigido al sistema de autorización 105 usando la URL, y el dispositivo de usuario 101 transmite el identificador de intención al sistema de autorización 105. El sistema de autorización 105 utiliza el identificador de intención para identificar la intención del usuario para que el sistema cliente 103 acceda al recurso protegido.

[0044] En el paso 317, el dispositivo de usuario 101 y el sistema de autorización 105 se comunican entre sí para que el usuario proporcione autorización para que el sistema de cliente 103 acceda al recurso protegido. Este paso puede implicar que el usuario seleccione el recurso protegido, o una parte del recurso protegido, como un subconjunto específico de datos relacionados con una cuenta de usuario específica (o grupo de perlas) almacenada en el sistema de recursos 107 a la que puede acceder el usuario.

[0045] En el paso 319, una vez que el usuario ha otorgado autorización para que el sistema cliente 104 acceda al recurso protegido, el sistema de autorización 105 transmite un código de autorización al dispositivo de usuario 101. El código de autorización comprende un indicador de que el usuario ha otorgado autorización. En este paso, el sistema de autorización 105 transmite una instrucción al dispositivo de usuario 101 para redirigir al sistema cliente 103. Esta instrucción de redireccionamiento puede comprender una URL correspondiente con el motor de recuperación en el sistema cliente 103.

[0046] En el paso 321, el dispositivo de usuario 101 se redirige al motor de recuperación 103a, y el dispositivo de usuario 101 transmite el código de autorización al motor de recuperación 103a.

[0047] En el paso 323, el motor de recuperación 103a transmite una solicitud de un token de acceso transmitiendo el código de autorización al sistema de autorización 105. El código de autorización puede transmitirse directamente desde el motor de recuperación 103a al sistema de autorización 105, o indirectamente a través del TMS 103b.

[0048] En el paso 325, el sistema de autorización 105 valida el código de autorización. Si el código de autorización es válido, el sistema de autorización 105 responde transmitiendo una ficha de acceso al motor de recuperación 103a. El token de acceso puede ser utilizado por el motor de recuperación 103a para acceder al recurso protegido almacenado en el sistema de recursos.

[0049] En el paso 327, si el token de acceso se ha recibido con éxito, el motor de recuperación 103a transmite un mensaje de éxito que indica que se ha recibido el token de acceso. Alternativamente, si el token de acceso no se ha recibido, el motor de recuperación 103a transmite un mensaje de falla que indica que el token de acceso no se ha recibido.

[0050] Con referencia a la Fig. 4, en el paso 329, el dispositivo de usuario 101 transmite una solicitud al motor de recuperación 103a para que el sistema cliente 103 recupere el recurso protegido. Si el token de acceso ha sido recibido previamente por el sistema del cliente 103, el método continúa con el paso 337. Alternativamente, si el token de acceso no se ha recibido previamente, se realizan los pasos 331 a 335 para que el sistema del cliente 103 obtenga la ficha de acceso de manera similar a la descrita anteriormente.

[0051] En el paso 331, el motor de recuperación 103a reenvía una solicitud de un token de acceso al TMS 103b. Luego, en el paso 333, el TMS 103b reenvía la solicitud de token de acceso al sistema de autorización 105 y, en respuesta, recibe el token de acceso. En el paso 335, el token de acceso se transmite desde el TMS 103b al motor de recuperación 103a.

[0052] En el paso 337, el motor de recuperación 103a transmite una solicitud para el recurso protegido transmitiendo el token de acceso al sistema de recursos 107. En el paso 339, el sistema de recursos 104 el token de acceso. Si el token de acceso es válido, el sistema de recursos responde transmitiendo el recurso protegido al motor de recuperación 103a.

[0053] En el paso 341, una vez que el sistema cliente 103 ha recibido el recurso protegido, el motor de recuperación transmite el recurso protegido al dispositivo de usuario 101. Una vez recibido, el recurso protegido se puede visualizar en el dispositivo de usuario 101 a través de una aplicación o un navegador en el dispositivo de usuario 101.

[0054] Con referencia a la Fig. 5, hay un método implementado por computadora realizado por el sistema cliente 103 que permite que el sistema cliente 103 se adapte de manera flexible a los métodos de concesión y autenticación soportados por el sistema externo 104. Este método puede usarse junto con el método descrito anteriormente con referencia a las Figs. 3 y 4.

[0055] En el paso 501, el sistema cliente 103 almacena una pluralidad de porciones de código del método de concesión. Cada una de las porciones de código del método de concesión se almacena en la memoria en el sistema cliente 103 y es ejecutable por un procesador del sistema cliente 103. La ejecución de cualquiera de las porciones de código del método de concesión hace que el sistema cliente 103 obtenga un token de acceso del sistema de autorización 105 del sistema externo 104 que utiliza un tipo específico de método de concesión. El método de concesión correspondiente a una parte de código de método de concesión particular es diferente de los métodos de concesión correspondientes a otras porciones de código del método de concesión.

[0056] Como se discutió anteriormente, el sistema de autorización 105 puede soportar uno o más de una pluralidad de diferentes tipos de método de concesión, cada uno de los cuales permite que el sistema cliente 103 acceda a un recurso protegido. En el marco de OAuth 2.0 hay varios tipos de métodos de concesión disponibles (o "tipos de concesión" como se menciona en el marco de OAuth 2.0). Los métodos de concesión pueden comprender tipos tales como los tipos de concesión "código de autorización", "implícito", "credenciales de contraseña del propietario del recurso" y "credenciales del cliente".

[0057] Una descripción general del tipo de concesión de "código de autorización" se describe anteriormente con referencia a los pasos 313 a 327 de la Fig. 3. En estos pasos, el sistema de autorización 105 proporciona un código de autorización en respuesta al usuario que autoriza el acceso al recurso protegido. El sistema cliente 103 puede entonces intercambiar el token de autorización por el token de acceso en el sistema de autorización 105.

[0058] El tipo de concesión de "credenciales de cliente" implica menos pasos que el tipo de concesión de "código de autorización". En lugar de redirigir el dispositivo de usuario 101 al sistema de autorización 105 para obtener el código de autorización, el sistema de cliente 101 transmite una solicitud para el token de acceso que comprende un identificador de cliente y un secreto de cliente, que es alguna forma de secreto compartido, como una contraseña. La solicitud del token de acceso comprende una indicación del tipo de concesión que se está utilizando, que en este caso es el tipo de concesión "credenciales del cliente". El sistema de autorización 105 valida el identificador del cliente y el secreto del cliente. Si el identificador del cliente y el secreto del cliente son válidos, el sistema de autorización 105 responde con el token de acceso.

[0059] Aunque solo se han descrito ciertos tipos de subvención en el presente documento, se podría usar cualquier otro tipo de subvención adecuado además del o los tipos de subvención descritos.

[0060] En el paso 503, el sistema cliente 103 almacena una pluralidad de porciones de código del método de autenticación. Cada una de las porciones de código del método de autenticación se almacena en la memoria en el sistema cliente 103 y es ejecutable por un procesador del sistema cliente 103. La ejecución de cualquiera de las porciones de código del método de autenticación hace que el sistema cliente 103 se autentique en el sistema externo 104 durante el proceso de obtención del token de acceso. El método de autenticación correspondiente a una porción de código de método de autenticación particular es diferente a los métodos de autenticación correspondientes a las otras porciones de código de método de autenticación.

[0061] Como se discutió anteriormente, un sistema de autorización puede soportar uno o más de una pluralidad de diferentes tipos de métodos de autenticación, cada uno de los cuales permite que el sistema cliente 103 se autentique en el sistema externo 104. En el marco de OAuth 2.0 hay una cantidad de tipos disponibles de métodos de autenticación (o "tipos de autenticación"). Los métodos de autenticación pueden comprender tipos tales como el método de autenticación "secreto del cliente" y el método de autenticación "aserción del cliente".

[0062] El método de autenticación "secreto del cliente" define la forma en que el sistema cliente 103 se autentica en el sistema de autorización 105 cuando obtiene el token de acceso. Si se utiliza el método de autenticación de "secreto de cliente", el sistema de cliente 103 transmitirá un secreto de cliente al sistema de autorización 103 cuando solicite el token de acceso. El secreto del cliente es un secreto compartido, como una contraseña, asignada al sistema del cliente 103. El sistema de autorización 105 utiliza el secreto del cliente para autenticar el sistema del cliente 103 al validar las solicitudes para el token de acceso.

[0063] El método de autenticación de "aserción de cliente" es similar al método de "secreto de cliente". Sin embargo, en el método de autenticación de "afirmación del cliente", el sistema del cliente 103 transmite una versión protegida de integridad del secreto del cliente. Por ejemplo, el secreto del cliente puede estar protegido con integridad mediante una firma digital o un Código de Autenticación de Mensaje (CAM). De esta forma, el secreto del cliente puede protegerse contra escuchas y alteraciones.

[0064] Aunque solo se han descrito ciertos tipos de autenticación en el presente documento, se podría usar cualquier otro tipo de autenticación adecuado además del tipo o tipos de autenticación descritos.

[0065] En el paso 505, el sistema cliente 103 almacena una base de datos configurable que identifica qué sistemas de autorización admiten qué tipos de métodos de concesión y autenticación. La base de datos configurable comprende una pluralidad de identificadores del sistema de autorización que son indicativos de un sistema de autorización

particular. Por lo tanto, cada identificador del sistema de autorización permite identificar un sistema de autorización específico, como el sistema de autorización 105 descrito con referencia a la Fig. 2.

[0066] Cada uno de los identificadores del sistema de autorización se almacena en asociación con uno o más de la pluralidad de tipos de métodos de concesión. En otras palabras, cada identificador del sistema de autorización está lógicamente vinculado con uno o más de los tipos de método de concesión en la base de datos. Esto permite que la base de datos indique qué tipo(s) de método de concesión admite un sistema de autorización específico.

[0067] Además, cada uno de los identificadores del sistema de autorización se almacena en asociación con uno o más de la pluralidad de tipos de métodos de autenticación. En otras palabras, cada identificador del sistema de autorización está vinculado lógicamente con uno o más de los tipos de método de autenticación en la base de datos. Esto permite que la base de datos indique qué tipo(s) de método de autenticación admite un sistema de autorización específico.

[0068] La base de datos es configurable de modo que pueda actualizarse para modificar los tipos de método de concesión y el método de autenticación que están asociados con cada identificador del sistema de autorización. Dado que el sistema cliente 103 es capaz de ejecutar una pluralidad de diferentes tipos de métodos de autenticación y concesión en virtud de las porciones de código del método de concesión y autenticación, el sistema cliente 103 puede adaptarse a los cambios en los tipos de método admitidos por un sistema externo de una manera rápida y sencilla.

[0069] Además, la base de datos configurable se puede actualizar para almacenar identificadores de sistema de autorización adicionales y tipos de métodos de concesión y autenticación asociados. Esto permite que el sistema cliente 103 se configure para comunicarse con un sistema externo con el que el sistema cliente 103 no se ha comunicado previamente.

[0070] En los pasos 505A-B, los métodos de concesión y autenticación asociados con uno o más de los sistemas de autorización pueden modificarse. Esto puede ocurrir en respuesta al sistema cliente 103 que recibe un mensaje de que los métodos de concesión y/o autenticación admitidos por un sistema de autorización han cambiado. Por ejemplo, el sistema cliente 103 puede recibir un mensaje del sistema externo 104, o de cualquier otro sistema, de que un sistema de autorización 105 ya no admite un método de concesión o autenticación particular. El sistema cliente 103 puede disociar el método de autenticación o concesión no admitida con el identificador del sistema de autorización en respuesta a este mensaje.

[0071] En otro ejemplo, el sistema cliente puede recibir un mensaje del sistema externo 104, o de cualquier otro sistema, de que ahora se admite un método de autenticación o concesión particular que no era compatible previamente con el sistema de autorización 105. El sistema cliente 103 puede asociar el método de autenticación o concesión recién admitido con el identificador del sistema de autorización en respuesta a este mensaje.

[0072] En lugar de recibir un mensaje de otro sistema con respecto a los tipos de concesión/autenticación admitidos y responder en consecuencia, un administrador en el sistema cliente 103 puede configurar la base de datos para reflejar qué métodos son compatibles con un sistema de autorización seleccionado.

[0073] El sistema cliente 103 puede realizar los pasos 505C-D para mantener una copia precisa de la base de datos configurable. Esto permite que el sistema cliente 103 se asegure de que se usan los métodos correctos de concesión/autenticación cuando se comunica con el sistema externo 104.

[0074] En el paso 505C, el sistema cliente 103 transmite una solicitud de base de datos a un sistema que aloja la base de datos que indica los sistemas de concesión/autenticación que son compatibles con una selección de sistemas de autorización. El sistema host de la base de datos responde a la solicitud de la base de datos transmitiendo al menos una parte de la base de datos al sistema cliente 103. Luego, en el paso 505D, el sistema cliente 103 actualiza la base de datos configurable usando la base de datos recibida del sistema host de la base de datos. En este paso, la base de datos configurable se configura para almacenar uno o más de los métodos de concesión/autenticación en la base de datos recibida en asociación con el identificador del sistema de autorización correspondiente.

[0075] El sistema del cliente 103 puede ejecutar el paso 505C de manera enterrada. Esto permite que el sistema cliente 103 conserve el uso del ancho de banda al reducir la cantidad de comunicación entre el sistema cliente 103 y el sistema que almacena la base de datos. El sistema del cliente 103 puede transmitir la solicitud de la base de datos de acuerdo con un horario predeterminado. Por ejemplo, la programación predeterminada puede definir un intervalo de tiempo entre solicitudes de base de datos consecutivas. En un ejemplo, el intervalo de tiempo entre cada solicitud de datos se define como 24 horas en el programa predeterminado, de modo que se envía una única solicitud de base de datos una vez al día. Esto logra un equilibrio entre el objetivo de mantener una versión precisa de la base de datos en el sistema cliente 103 y el uso del ancho de banda. El horario predeterminado puede ser configurable. Por ejemplo, el intervalo de tiempo entre solicitudes de bases de datos adyacentes puede ser configurado por un administrador del sistema cliente 103. Esto permite que el sistema cliente 103 se sintonice para que se envíe el número óptimo de solicitudes de base de datos dentro de un período de tiempo dado.

[0076] Como se discutió anteriormente, el sistema de autorización 105 puede soportar diferentes tipos de método de concesión y método de autenticación. Sin embargo, uno de estos diferentes tipos de métodos puede ser más o menos seguro que los otros tipos. Por ejemplo, el método de concesión de "código de autorización" puede ser más seguro que el método de concesión de "credenciales de cliente". En otro ejemplo, el método de autenticación "secreto del cliente" puede ser menos seguro que el método de autenticación "aserción del cliente".

[0077] En el paso 507, el sistema cliente 103 clasifica los tipos de método de concesión y método de autenticación en la base de datos configurable en función de la seguridad de cada tipo de concesión. Este paso puede implicar asociar una puntuación con cada uno de los tipos de métodos de concesión y cada uno de los tipos de métodos de autenticación, lo que indica la seguridad de cada método. Por ejemplo, el método de concesión de "código de autorización" puede asociarse con una puntuación de "10" y el método de concesión de "credenciales del cliente" puede asociarse con una puntuación de "5". De esta forma, los puntajes respectivos indican que el método de concesión del "código de autorización" es más seguro que el método de concesión de "credenciales del cliente".

[0078] En otro ejemplo, el método de autenticación "secreto del cliente" puede asociarse con una puntuación de "4" y el método de autenticación "afirmación del cliente" puede asociarse con una puntuación de "9". De esta manera, los puntajes respectivos indican que el método de autenticación de "afirmación del cliente" es más seguro que el método de autenticación "secreto del cliente".

[0079] La clasificación de los métodos de concesión y autenticación en función de su solidez de seguridad permite al sistema cliente 103 elegir el método más seguro, donde hay una opción disponible. Esto mejora la seguridad del sistema en su conjunto, ya que el uso de métodos menos seguros puede exponer el sistema a problemas como las escuchas.

[0080] En el paso 509, el sistema cliente 103 recibe una solicitud de acceso del dispositivo de usuario 101 de manera similar a la descrita en el paso 301 de la Fig. 3. La solicitud de acceso comprende una instrucción para que el sistema cliente 103 acceda a un recurso protegido. La solicitud de acceso también comprende un identificador de solicitud que indica el sistema de autorización con el que el sistema cliente 103 debe comunicarse antes de acceder al recurso protegido en el sistema de recursos correspondiente. En este ejemplo, el sistema de autorización es el sistema de autorización 105 del sistema externo 104.

[0081] En el paso 511, el sistema cliente 103 compara el sistema de autorización 105 indicado por la solicitud de acceso con los sistemas de autorización indicados por los identificadores del sistema de autorización en la base de datos configurable. Si se encuentra una coincidencia, se identifican los tipos de método de concesión y autorización asociados con el sistema de autorización coincidente.

[0082] Los tipos de métodos de autorización y concesión identificados son los métodos soportados por el sistema de autorización 105 con el que el sistema cliente 103 debe comunicarse para atender la solicitud de acceso. Puede haber una pluralidad de tipos de métodos de concesión compatibles con el sistema de autorización 105, o puede haber solo un único tipo de método de concesión compatible con el sistema de autorización 105. Puede haber una pluralidad de tipos de métodos de autenticación compatibles con el sistema de autorización 105, o puede ser solo un tipo de método de autenticación único soportado por el sistema de autorización 105.

[0083] Los pasos 511A-B se refieren al escenario en donde una pluralidad de tipos de concesión y/o autenticación son compatibles con el sistema de autorización 104. En el paso 511A, el sistema cliente 103 selecciona uno de los tipos de método de concesión y uno de los tipos de método de autenticación identificados en el paso 511. El tipo de método seleccionado puede basarse en una variedad de criterios diferentes, por ejemplo, eligiendo el método más rápido o más eficiente de cada tipo disponible.

[0084] El paso 511 B se refiere a un ejemplo específico en donde se elige el método de concesión y/o autenticación más seguro. En este paso, el sistema cliente 103 selecciona el método más seguro basado en el proceso de clasificación realizado en el paso 507. Por ejemplo, el método de concesión o el método de autenticación con la puntuación más alta se selecciona para la ejecución.

[0085] En el paso 513, se ejecuta la parte del código del método de concesión correspondiente al método de concesión seleccionado, y se ejecuta la parte del código del método de autenticación correspondiente al método de autenticación seleccionado.

[0086] En el paso 514, si el sistema cliente 103 se valida con éxito en el sistema de autorización 104 usando los métodos de concesión y autenticación seleccionados, el sistema cliente 103 recibe el token de acceso. Posteriormente, el sistema cliente 103 puede transmitir el token de acceso al sistema de recursos 107 para obtener el recurso protegido correspondiente con la solicitud de acceso en el paso 501.

[0087] Con referencia a la Fig. 6, existe un método 600 implementado por computadora que permite que el sistema cliente 103 se asegure de que tiene acceso a un token de concesión válido, que es necesario para responder con

éxito a las solicitudes del usuario para acceder a un recurso protegido. Este método se puede usar junto con el método descrito anteriormente con referencia a las Figs. 3 y 4.

[0088] Cada uno de los tokens de concesión proporcionados al sistema cliente 103 por el sistema de autorización 105 puede tener un tiempo correspondiente para expirar, que es el momento en que la identificación no se considerará válida en el sistema de autorización. Por lo tanto, un token de concesión caducado no se puede utilizar en el proceso de obtener un recurso protegido del sistema de recursos 107. Si el token de concesión almacenado en el sistema cliente 103 no es válido (es decir, el token ha caducado) en un momento en que una solicitud de acceso (tal como se recibe la solicitud descrita con referencia al paso 301 en la Fig. 3), el sistema cliente 103 puede no ser capaz de atender la solicitud de acceso con éxito, o al menos habrá un retraso en el servicio de la solicitud. Por lo tanto, el método descrito con referencia a la Fig. 6 permite que las solicitudes de acceso del usuario sean atendidas de manera confiable y rápida, asegurando que el token de concesión válido sea retenido por el sistema cliente 103.

[0089] En el paso 601, el sistema cliente 103 recibe un mensaje de intención del dispositivo de usuario 101. El mensaje de intención puede ser el mensaje de acceso descrito anteriormente. Por lo tanto, el paso 601 se puede realizar de manera similar al paso 301 descrito con referencia a la Figura 3. El mensaje de acceso puede referirse a un mensaje de intención porque este mensaje indica la intención del usuario para que el sistema cliente 103 acceda al recurso protegido.

[0090] En el paso 603, el sistema cliente 103 transmite una solicitud de un token de concesión al sistema de autorización 105. Como se explicó anteriormente con referencia a la Figura 3, el token de concesión es un token que permite que el sistema externo 104 autentique la identidad del sistema cliente 103.

[0091] En el paso 605, el sistema de autorización 105 valida la solicitud 103 del sistema cliente de un código de identificación. Si la solicitud es válida, el sistema de autorización 105 responde transmitiendo el token de concesión al sistema cliente 103. El sistema de autorización 105 puede transmitir un indicador de tiempo de vencimiento al sistema cliente 103 que indica el tiempo de vencimiento del token de concesión. Además, el sistema de autorización 105 puede transmitir un token de actualización al sistema cliente 103 que puede usarse para obtener un nuevo token de concesión (es decir, no vencido).

[0092] Los pasos 603-505 pueden realizarse de manera similar a la descrita con referencia a los pasos 303-307 en las Figuras 3 y 4. Además, los pasos 603-605 se pueden realizar antes, después o al mismo tiempo que se recibe el mensaje de intención del paso 601.

[0093] En el paso 607, se determina un intervalo de tiempo que define el tiempo entre recibir el token de concesión y solicitar un uno nuevo, y se establece un temporizador utilizando el intervalo de tiempo. El intervalo de tiempo puede ser un intervalo de tiempo predeterminado, como 1 minuto, 5 minutos o 10 minutos, etc. Este intervalo de tiempo puede basarse en el tiempo de vencimiento del token de concesión recibido. Por ejemplo, el intervalo de tiempo puede ser igual al tiempo de expiración del token de concesión, de modo que el sistema cliente 103 pueda iniciar el proceso de solicitar un nuevo token de concesión en el momento en que expire el token de concesión. En un ejemplo específico, el tiempo de expiración del token de concesión puede ser de 5 minutos y, por lo tanto, el intervalo de tiempo puede establecerse en 5 minutos. Por lo tanto, el sistema cliente 103 solicitará un nuevo token de concesión 5 minutos después de que se haya recibido el token de concesión anterior, que es el momento en que expira el token anterior.

[0094] En otro ejemplo, el intervalo de tiempo puede establecerse como una cantidad de tiempo menor que el tiempo de vencimiento del token de concesión. De esta manera, el sistema cliente 103 puede iniciar el proceso de solicitar un nuevo token de concesión antes de que expire el token de concesión. En un ejemplo específico, el tiempo de vencimiento del token de concesión puede ser de 5 minutos y el intervalo de tiempo se puede establecer en 4 minutos. Por lo tanto, el sistema de cliente 103 puede garantizar que solo haya un pequeño intervalo de tiempo entre la solicitud de un nuevo token de concesión y el vencimiento del token anterior. El intervalo de tiempo puede establecerse de modo que esta ventana no sea mayor que una longitud de ventana predefinida (p. ej., 1 minuto). Esta ventana se puede configurar configurando el intervalo de tiempo para optimizar el número de solicitudes de actualización enviadas, al tiempo que se garantiza que se mantiene un token de concesión válido en el sistema cliente 103.

[0095] En otro ejemplo, el intervalo de tiempo puede establecerse como una cantidad de tiempo mayor que el tiempo de vencimiento del token de concesión. De esta manera, el sistema cliente 103 puede garantizar que el proceso de solicitud de un nuevo token de concesión se producirá en un momento preciso después de que el token de concesión anterior haya expirado. En un ejemplo específico, el tiempo de expiración del token de concesión puede ser de 5 minutos y, por lo tanto, el intervalo de tiempo puede establecerse en 6 minutos. Por lo tanto, el sistema cliente 103 puede garantizar que solo haya un pequeño período de tiempo entre el vencimiento del token de concesión y la solicitud de uno nuevo. El intervalo de tiempo puede establecerse de modo que esta ventana no sea mayor que una longitud de ventana predefinida (p. ej., 1 minuto). Nuevamente, esta ventana se puede configurar configurando el intervalo de tiempo para optimizar el número de solicitudes de actualización enviadas, al tiempo que se garantiza que se mantiene un token de concesión válido en el sistema cliente 103.

[0096] En el paso 609, el sistema cliente 103 inicia un temporizador en respuesta a recibir el token de concesión y

usar el intervalo de tiempo establecido en el paso 607. El temporizador se usa para determinar el momento en que ha transcurrido el intervalo de tiempo.

[0097] En el paso 611, una vez transcurrido el intervalo de tiempo, el sistema cliente 103 transmite una solicitud de actualización al sistema de autorización 105. La solicitud de actualización puede comprender una instrucción para que se proporcione un nuevo token de concesión (es decir, no vencido) al sistema cliente 103 del sistema de autorización 105.

[0098] En el paso 613, el sistema cliente 103 recibe el nuevo token de concesión en respuesta a la solicitud de actualización.

[0099] En el paso 615, el cliente 103 puede transmitir el token de concesión recibido más recientemente al sistema de recursos 107 para iniciar una solicitud del recurso protegido. El paso 615 se puede realizar de una manera similar a la descrita con referencia al paso 309 de la Fig. 3.

[0100] Los pasos 601 a 615 pueden repetirse de modo que se reciban muchos tokens de concesión diferentes del sistema de autorización 107. Además, los pasos 601 a 615 pueden repetirse para otro sistema de autorización de modo que se reciban muchos tokens de concesión diferentes de una variedad de sistemas de autorizaciones. Los tokens de subvención recibidos de un sistema de autorización particular pueden tener tiempos de vencimiento similares.

[0101] En el paso 617, el intervalo de tiempo discutido en relación con los pasos 607 y 609 se calcula en base a los tiempos de vencimiento de los tokens de concesión recibidos y los sistemas de autorización específicos desde los cuales se reciben los tokens de concesión.

[0102] En un ejemplo, el sistema cliente 103 puede calcular un tiempo de vencimiento previsto de los tokens de concesión recibidos de un sistema de autorización particular. El tiempo de vencimiento previsto puede calcularse calculando un promedio de los tiempos de vencimiento del token de concesión recibido de un sistema de autorización específico, o una pluralidad de sistemas de autorización diferentes.

[0103] El tiempo de vencimiento previsto calculado en el paso 617 puede usarse para determinar el intervalo de tiempo en el paso 607. Por ejemplo, el tiempo de vencimiento previsto puede ser igual a un tiempo menor o un tiempo preestablecido mayor que el intervalo de tiempo en paso 607.

[0104] Haciendo referencia a la Fig. 7, existe un método 700 implementado por computadora que permite que el sistema cliente 103 reduzca el ancho de banda y los recursos de procesamiento utilizados al minimizar el número de solicitudes de tokens de acceso enviadas, tales como las solicitudes de fichas de acceso descritas con referencia a los pasos 323 y 325 en la Fig. 3. Por lo tanto, el método descrito con referencia a la Fig. 7 puede usarse junto con el método descrito anteriormente con referencia a las Figs. 3 y 4.

[0105] En el paso 701, el sistema cliente 103 recibe una solicitud de acceso del dispositivo de usuario 101. Este paso puede realizarse de manera similar a la descrita con referencia al paso 301 en la Fig. 3.

[0106] En el paso 703, el sistema cliente 103 transmite una solicitud de un token de acceso al servidor de autorización 105 en respuesta a la solicitud de acceso. Este paso puede realizarse de manera similar al paso 323, *p. ej.,* después de que se hayan realizado los pasos 303 a 321, como se describe con referencia a la Fig. 3.

[0107] En el paso 705, el sistema cliente 103 recibe el token de acceso del sistema de autorización 105. Este paso puede realizarse de manera similar al paso 325, como se describe con referencia a la Fig. 3. En este paso, el sistema de autorización 105 puede transmitir un indicador de tiempo de vencimiento al sistema cliente 103. El indicador de tiempo de vencimiento corresponde al token de acceso e indica el tiempo de vencimiento del token de acceso. Después del tiempo de caducidad indicado por el tiempo de caducidad, el token de acceso no puede utilizarse para acceder al recurso protegido. En otras palabras, el indicador de tiempo de caducidad es indicativo del momento en que el token de acceso correspondiente no será válido para obtener el recurso protegido del sistema de recursos 107. En el paso 505, el sistema de autorización 105 puede transmitir un token de actualización correspondiente con el token de acceso. El token de actualización puede ser utilizado por el sistema cliente 3 para obtener un token de acceso no vencido del sistema de autorización 105.

[0108] El indicador de tiempo de vencimiento puede ser indicativo de un período de tiempo durante el cual el token de acceso será válido. Por ejemplo, este período de tiempo puede expresarse como un número de segundos o minutos. Alternativamente, el tiempo de vencimiento puede indicar un punto en el tiempo en donde el token de acceso ya no será válido. Por ejemplo, la hora de vencimiento puede indicar una hora específica durante el día. El sistema de cliente 103 puede determinar el tiempo de expiración del token de acceso basándose en el período de tiempo o en los indicadores de punto en el tiempo mediante el indicador de tiempo de expiración.

[0109] En el paso 707, el sistema cliente 103 transmite el token de acceso al sistema de recursos 107 en una solicitud

para recibir el recurso protegido. Este paso puede realizarse de manera similar al paso 337 como se describe con referencia a la Fig. 4.

[0110] En el paso 711, el token de acceso recibido del sistema de autorización 107 se almacena en una unidad de almacenamiento de tokens en el sistema cliente 103. El tiempo de vencimiento indicado por el indicador de tiempo de vencimiento puede almacenarse también en la unidad de almacenamiento de tokens. El token de acceso y/o el tiempo de vencimiento indicado por el indicador de tiempo de vencimiento pueden encriptarse y almacenarse en la unidad de almacenamiento de tokens para mejorar la seguridad. En este paso, el token de acceso puede almacenarse independientemente del tiempo de vencimiento del token de acceso correspondiente. En otras palabras, el sistema cliente 103 almacena el token de acceso independientemente de si el tiempo de caducidad es corto o largo. Esto reduce el esfuerzo de procesamiento requerido para analizar el tiempo de caducidad de cada token de acceso. Alternativamente, el sistema cliente 103 puede no almacenar, o puede eliminar, el token de acceso si su tiempo de vencimiento es inferior a un umbral predeterminado. Si se almacena el token de acceso, el token de acceso puede almacenarse después de su tiempo de caducidad.

[0111] En el paso 713, el sistema cliente 103 recibe otra solicitud de acceso similar a la solicitud de acceso recibida en el paso 701.

[0112] En el paso 715, el sistema cliente 103 transmite el token de acceso almacenado al sistema de autorización 107 en otra solicitud para recibir el recurso protegido similar a la solicitud enviada en el paso 707. Por lo tanto, el sistema cliente 103 usa el token de acceso almacenado, en lugar de solicitar un nuevo token de acceso para atender la solicitud de acceso del usuario. Esto reduce el ancho de banda y los recursos de procesamiento utilizados por el sistema cliente 103.

[0113] En los pasos 719 a 727, las solicitudes de mantenimiento de almacenamiento de tokens se realizaron en el sistema cliente 103. Estos pasos ayudan a conservar los recursos de almacenamiento, mientras hacen un uso más eficiente del ancho de banda y procesamiento de recursos minimizando el número de solicitudes de nuevos tokens de acceso.

[0114] En el paso 719, el sistema cliente 103 compara el tiempo indicado por el indicador de tiempo de caducidad correspondiente a uno o más de los tokens de acceso almacenados.

[0115] En el paso 721, si el tiempo indicado por un indicador de tiempo de caducidad es posterior al tiempo actual, el método continúa con el paso 723. Alternativamente, si el tiempo indicado por el indicador de tiempo de caducidad no es posterior al actual, el método procede al paso 725.

[0116] En el paso 723, se elimina el token de acceso correspondiente al tiempo de caducidad que es posterior a la hora actual.

[0117] Los pasos 719 a 723 pueden realizarse intermitentemente. Por ejemplo, los pasos 719 pueden ejecutarse de acuerdo con un programa predeterminado. En un ejemplo, el programa predeterminado define un intervalo de tiempo entre ejecuciones adyacentes de los pasos 719 a 723. Este intervalo de tiempo puede ser configurable en el sistema cliente 103 basado en una entrada del usuario recibida de un administrador. El intervalo de tiempo puede ser configurable en el sistema cliente 103 basado en el rendimiento monitoreado del sistema cliente 103. La configuración del intervalo de tiempo puede ocurrir automáticamente.

[0118] Los pasos 725 y 727 se pueden ejecutar para realizar los pasos 719 a 723 de acuerdo con el programa predeterminado. En el paso 725, se determina el intervalo de tiempo de la programación predeterminada. Luego, en el paso 727, el método procede a repetir los pasos 719 a 723 una vez que ha transcurrido el intervalo de tiempo.

[0119] Los pasos 729 y 731 pueden realizarse en el método 700 para gestionar una situación en donde un token de acceso se ha vuelto inválido y, por lo tanto, no será utilizable para obtener el recurso protegido. Cuando un token de acceso deja de ser válido, no se debe volver a usar, ya que esto implicará que se transmitan comunicaciones innecesarias entre el sistema cliente 103 y el sistema externo 104. Sin embargo, eliminar tokens de acceso cada vez que se considere no válido implica una carga de procesamiento que sería preferible evitar. Esto es particularmente relevante cuando el sistema cliente 103 maneja una gran cantidad de token de acceso para una gran cantidad de usuarios con recursos protegidos almacenados en una variedad de sistemas externos. Los pasos 729 y 731 permiten evitar la transmisión de acceso no válida, al tiempo que evitan la carga de procesamiento que gestiona el almacenamiento de tokens de acceso de forma individual.

[0120] En el paso 729, el sistema cliente 103 recibe un mensaje de rechazo que indica que el token de acceso no es válido. Este mensaje puede recibirse desde el sistema externo 104, por ejemplo a través del sistema de autorización 105 o el sistema de recursos 107. Alternativamente, el mensaje de rechazo puede recibirse desde cualquier otro sistema, o puede recibirse a través de una entrada en el sistema cliente 103.

[0121] El mensaje de rechazo puede recibirse en respuesta al sistema externo 104 que determina que el token de

acceso ha expirado. Por ejemplo, el sistema cliente 103 puede transmitir el token de acceso almacenado al sistema de autorización 105 en un intento de acceder al recurso protegido. Sin embargo, el sistema de autorización 107 puede determinar que el token de acceso ha expirado. En respuesta a la determinación de que el token de acceso ha expirado, el sistema de autorización 107 transmite un mensaje de rechazo al sistema del cliente 103.

[0122] En otro ejemplo, el mensaje de rechazo puede recibirse en respuesta al usuario del dispositivo de usuario 101 que revoca su autorización para que el sistema cliente 103 acceda al recurso protegido. El usuario puede informar al sistema de autorización 107 que su autorización ha sido revocada. Esto invalidará el token de acceso correspondiente y su token de actualización correspondiente. Sin embargo, en este escenario, el sistema cliente 103 ignorará que el token de acceso y el token de actualización han sido invalidados. Por lo tanto, el sistema cliente 103 puede continuar transmitiendo solicitudes de acceso al recurso protegido utilizando el token de acceso no válido. El sistema cliente 103 recibirá un mensaje de rechazo del sistema externo 104 en respuesta a cada una de estas solicitudes porque el token de acceso no es válido. Sin embargo, el sistema cliente 103 aún podría transmitir solicitudes de actualización utilizando el token de actualización no válido, bajo el supuesto de que el token de acceso ha expirado en lugar de que se haya revocado la autorización del usuario. Todos estos procesos representan una carga innecesaria en los recursos de procesamiento y el ancho de banda del sistema cliente 103. Si el token de acceso tiene un token de actualización correspondiente, el mensaje de rechazo comprende una indicación de que el token de actualización no es válido.

[0123] En el paso 731, en lugar de eliminar el token de acceso y el token de actualización directamente en respuesta al mensaje de rechazo, el sistema cliente 103 establece un indicador de invalidación en asociación con el token de acceso correspondiente y el token de actualización. Establecer el indicador de invalidación implica una sobrecarga de procesamiento menor que eliminar los tokens. Por lo tanto, cuando el sistema cliente 103 está administrando muchos tokens, esto equivaldrá a una mejora significativa en la eficiencia.

[0124] El indicador de invalidación puede ser un campo de bits de adición almacenado en asociación con el token de acceso y el token de actualización. Por ejemplo, si el campo de bits se establece en "1", esto puede indicar que el token correspondiente no es válido y, si el campo de bits se establece en "0", esto puede indicar que el token correspondiente no es válido (o viceversa).

[0125] En otro ejemplo, el indicador de invalidación puede establecerse modificando el indicador de tiempo de caducidad asociado con el token de acceso y/o el token de actualización. En este ejemplo, el indicador de tiempo de vencimiento se estableció en el pasado para indicar que los tokens ya no son válidos. Por lo tanto, cuando los pasos 719 a 727 se realizan posteriormente, los tokens se eliminarán como parte de los pasos de mantenimiento del almacenamiento de tokens.

[0126] Con referencia a la Fig. 8, el sistema cliente 103 comprende una interfaz de comunicación 801 que comprende un receptor 803 y un transmisor 805. El sistema cliente 103 comprende un procesador 807, un módulo de identificación 813, un módulo de clasificación 815, un módulo temporizador 817, un módulo de cálculo de intervalo de tiempo 819, un módulo de mantenimiento de almacenamiento de tokens y un módulo de configuración de bandera 823. El sistema cliente 103 también comprende el motor de recuperación 103a y el servidor de gestión de tokens 103b descritos anteriormente.

[0127] Hay un recurso de almacenamiento 825 en el sistema cliente 103 que comprende un recurso de almacenamiento de porción de código de método de concesión 827, un recurso de almacenamiento de código de método de autenticación 829, un recurso de almacenamiento de base de datos configurable 831 y una unidad de almacenamiento de token 833.

[0128] El receptor 803 y el transmisor 805 están configurados para recibir y transmitir mensajes, instrucciones y tokens hacia y desde el sistema cliente 103 como se explicó anteriormente.

[0129] El recurso de almacenamiento 825 está configurado para almacenar porciones de código del método de concesión, como se describió anteriormente con referencia al paso 501, en el recurso de almacenamiento de porciones de código del método de concesión 827. El recurso de almacenamiento 825 está configurado para almacenar porciones de código del método de autenticación, como se describe anteriormente con referencia al paso 503, en el recurso de almacenamiento de porción de código del método de autenticación 829. El recurso de almacenamiento 825 está configurado para almacenar la base de datos configurable, como se describió anteriormente con referencia al paso 505, en el recurso de almacenamiento de base de datos configurable 831. La unidad de almacenamiento de tokens 833 está dispuesta para almacenar tokens, como los tokens de acceso, los tokens de concesión y los tokens de actualización descritos anteriormente.

[0130] El módulo de clasificación 817 está configurado para realizar los procesos de clasificación descritos anteriormente, tales como los descritos anteriormente con referencia al paso 507. El módulo de identificación 813 está configurado para identificar el método de autenticación y los métodos de concesión soportados por un servidor de autorización, como se describe anteriormente con referencia al paso 511. El procesador 807 está configurado para ejecutar instrucciones, tales como la instrucción de las porciones de código de método de autenticación y concesión seleccionadas, como se describe con referencia al paso 513. El módulo temporizador 817 está configurado para activar

un temporizador para un período de tiempo, por ejemplo como se describió anteriormente con referencia a los pasos 607, 609. Además, el módulo temporizador 817 se puede usar para monitorear un tiempo actual para compararlo con el tiempo de vencimiento de un token, como se describió anteriormente con referencia al paso 719. El módulo de cálculo de intervalo de tiempo 819 está configurado para calcular un intervalo de tiempo para configurar el temporizador, como se describió anteriormente con referencia al paso 725. El módulo de gestión de almacenamiento de tokens 821 está configurado para comparar el tiempo actual indicado por el temporizador con el tiempo de caducidad de un token, y para eliminar un token en respuesta, como se describió anteriormente con referencia a los pasos 721 y 723 anteriores. El módulo de configuración de bandera 823 está configurado para establecer una bandera de invalidación en asociación con una ficha, como se describe anteriormente con referencia al paso 731.

[0131] La Fig. 9 muestra un dispositivo electrónico ejemplar 901 de acuerdo con cualquiera de los dispositivos o sistemas electrónicos de esta divulgación (tal como el dispositivo de usuario 101, el sistema cliente 103, el sistema externo 104, el sistema de autorización 105, el sistema de recursos 107, el motor de recuperación 103a o el TMS 103b). El dispositivo electrónico 901 comprende circuitos de procesamiento 910 (tales como un microprocesador) y una memoria 912. El dispositivo electrónico 901 también puede comprender uno o más de los siguientes subsistemas: una fuente de alimentación 914, una pantalla 916, un transceptor 920 y una entrada 926.

[0132] La circuitería de procesamiento 910 puede controlar el funcionamiento del dispositivo electrónico 901 y los subsistemas conectados a los que está acoplada en comunicación la circuitería de procesamiento. La memoria 912 puede comprender una o más de memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de acceso aleatorio no volátil (NVRAM), memoria flash, otra memoria volátil y otra memoria no volátil.

[0133] La pantalla 916 puede estar acoplada comunicativamente con la circuitería de procesamiento 910, que puede configurarse para hacer que la pantalla 916 muestre imágenes representativas de los datos seguros, o recursos protegidos, compartidos entre las entidades en el sistema 100.

[0134] La pantalla 916 puede comprender una interfaz sensible al tacto, tal como una pantalla táctil. La pantalla 916 se puede usar para interactuar con el software que se ejecuta en el procesador 910 del dispositivo electrónico 901. La interfaz sensible al tacto permite al usuario proporcionar información a la circuitería de procesamiento 910 a través de un toque discreto, toques o uno o más gestos para controlar el funcionamiento de los circuitos de procesamiento y las funciones descritas en este documento. Se apreciará que otras formas de interfaz de entrada pueden emplearse adicional o alternativamente para el mismo propósito, tal como la entrada 926 que puede comprender un teclado o un ratón en el dispositivo de entrada.

[0135] El transceptor 920 puede ser uno o más transceptores de RF de largo alcance que están configurados para operar de acuerdo con estándares de comunicación tales como LTE, UMTS, 3G, EDGE, GPRS, GSM y Wi-Fi. Por ejemplo, el dispositivo electrónico 901 puede comprender un primer transceptor inalámbrico 921, como un transceptor celular, que está configurado para comunicarse con una torre celular 903 a través de un protocolo de datos celulares como LTE, UMTS, 3G, EDGE, GPRS o GSM y un segundo transceptor 928, como un transceptor Wi-Fi, que está configurado para comunicarse con un punto de acceso inalámbrico 904 a través de un estándar Wi-Fi como 802,11 ac/n/g/b/a. A este respecto y para los fines de todas las realizaciones de este documento con respecto a un protocolo inalámbrico de largo alcance, un protocolo inalámbrico de largo alcance puede ser un protocolo que sea capaz y esté diseñado para la comunicación a través de 5, 10, 20, 30, 40, 50 o 100m. Esto contrasta con el protocolo inalámbrico de corto alcance mencionado anteriormente. El protocolo inalámbrico de largo alcance puede comunicarse utilizando una mayor potencia que el protocolo inalámbrico de corto alcance. El alcance (p. ej., la distancia de la línea de visión) entre los nodos finales de largo alcance (dispositivo electrónico y enrutador o estación base) para el protocolo inalámbrico de largo alcance puede ser mayor que el alcance (p. ej., la distancia de la línea de visión) entre nodos finales de corto alcance (p. ej., dispositivo electrónico y baliza inalámbrica).

[0136] El dispositivo electrónico 901 puede configurarse para comunicarse a través del transceptor 920 con una red 940. La red 940 puede ser una red de área amplia, como Internet, o una red de área local. El dispositivo electrónico 901 puede configurarse además para comunicarse a través del transceptor 920 y la red 940 con uno o más sistemas o dispositivos de usuario. Estos servidores o dispositivos de usuario pueden ser cualquiera de los descritos aquí.

[0137] El término "que comprende" abarca "que incluye" así como "que consiste", *p. ej.,* una composición "que comprende" X puede consistir exclusivamente en X o puede incluir algo adicional, *p. ej.,* X + Y.

[0138] La palabra "sustancialmente" no excluye "completamente", *p. ej.,* una composición que está "sustancialmente libre" de Y puede estar completamente libre de Y. Cuando sea necesario, la palabra "sustancialmente" puede omitirse de la definición de la invención.

[0139] A menos que se indique lo contrario, cada realización como se describe en el presente documento puede combinarse con otra realización como se describe en el presente documento.

[0140] Los métodos descritos en este documento pueden realizarse mediante software en forma legible por máquina en un medio de almacenamiento tangible, *p. ej.,* en forma de un programa de computadora que comprende medios

de código de programa de computadora adaptados para realizar todos los pasos de cualquiera de los métodos descritos aquí cuando el programa se ejecuta en una computadora y donde el programa de computadora se puede incorporar en un medio legible por computadora. Los ejemplos de medios de almacenamiento tangibles (o no transitorios) incluyen discos, memorias USB, tarjetas de memoria, etc. y no incluyen señales propagadas. El software puede ser adecuado para su ejecución en un procesador paralelo o en un procesador en serie, de modo que los pasos del método se puedan llevar a cabo en cualquier orden adecuado o simultáneamente. Esto reconoce que el firmware y el software pueden ser productos valiosos y comercializables por separado. Su objetivo es abarcar el software, que se ejecuta o controla hardware "tonto" o estándar, para llevar a cabo las funciones deseadas. También está destinado a abarcar el software que "describe" o define la configuración del hardware, como el software HDL (lenguaje de descripción de hardware), que se utiliza para diseñar chips de silicio, o para configurar chips programables universales, para llevar a cabo las funciones deseadas.

[0141] Se apreciará que los módulos descritos en el presente documento pueden implementarse en hardware o en software. Además, los módulos pueden implementarse en varias ubicaciones en todo el sistema.

[0142] Los expertos en la materia se darán cuenta de que los dispositivos de almacenamiento utilizados para almacenar las instrucciones del programa se pueden distribuir a través de una red. Por ejemplo, una computadora remota puede almacenar un ejemplo del proceso descrito como software. Una computadora local o terminal puede acceder a la computadora remota y descargar una parte o la totalidad del software para ejecutar el programa. Alternativamente, la computadora local puede descargar partes del software según sea necesario, o ejecutar algunas instrucciones de software en la terminal local y algunas en la computadora remota (o red de computadoras). Los expertos en la materia también se darán cuenta de que al utilizar técnicas convencionales conocidas por los expertos en la materia, todas o una parte de las instrucciones del software pueden llevarse a cabo mediante un circuito dedicado, como un DSP, una matriz lógica programable o similar.

[0143] Cualquier valor de rango o de dispositivo dado aquí puede ampliarse o alterarse sin perder el efecto buscado, como será evidente para el experto en la materia.

[0144] Se entenderá que los beneficios y ventajas descritas anteriormente pueden referirse a una realización o pueden referirse a varias realizaciones. Las realizaciones no se limitan a las que resuelven alguno o todos los problemas establecidos o las que tienen alguno o todos los beneficios y ventajas indicados.

[0145] Cualquier referencia a “un” elemento se refiere a uno o más de esos elementos. El término "que comprende" se usa en el presente documento para significar que incluye los bloques o elementos del método identificados, pero que dichos bloques o elementos no comprenden una lista exclusiva y que un método o aparato puede contener bloques o elementos adicionales.

[0146] Los pasos de los métodos descritos en este documento pueden llevarse a cabo en cualquier orden adecuado, o simultáneamente cuando sea apropiado.

[0147] Los aspectos de cualquiera de los ejemplos descritos anteriormente pueden combinarse con los aspectos de cualquiera de los otros ejemplos descritos para formar ejemplos adicionales sin perder el efecto buscado. Cualquiera de los módulos descritos anteriormente puede implementarse en hardware o software.

[0148] Se entenderá que la descripción anterior de una realización preferida se proporciona únicamente a modo de ejemplo y que los expertos en la técnica pueden realizar diversas modificaciones. Aunque se han descrito varias realizaciones anteriormente con un cierto grado de particularidad, o con referencia a una o más realizaciones individuales, los expertos en la materia podrían realizar numerosas modificaciones a las realizaciones descritas sin apartarse del alcance de esta invención.

REIVINDICACIONES

1. Un método implementado por computadora para obtener un token de acceso para proporcionar acceso a un recurso protegido almacenado en un sistema de recursos, comprendiendo el método:

el almacenamiento (501; 503), en un sistema cliente:

una pluralidad de porciones de código del método de concesión, cada una ejecutable para obtener acceso al token de acceso usando uno de una pluralidad de tipos de método de concesión, en donde cada tipo respectivo de método de concesión es diferente a los otros tipos de método de concesión; y
una pluralidad de porciones de código del método de autenticación cada una ejecutable para autenticar el sistema cliente usando un método de autenticación diferente, en donde cada tipo respectivo de método de autenticación es diferente a los otros tipos de método de autenticación;

almacenar (505), en el sistema cliente, una base de datos configurable que comprende una pluralidad de identificadores del sistema de autorización, cada uno indicativo de un sistema de autorización respectivo, en donde cada uno de la pluralidad de identificadores del sistema de autorización está asociado con uno o más de la pluralidad de tipos de método de concesión que es compatible con el sistema de autorización respectivo, y cada uno de la pluralidad de identificadores del sistema de autorización está asociado con uno o más de la pluralidad de tipos de métodos de autenticación que son compatibles con el sistema de autorización respectivo;
recibir (509), en el sistema cliente, desde un dispositivo de usuario una solicitud de acceso que comprende una instrucción para que el sistema cliente acceda a un recurso protegido, la instrucción que comprende un identificador de solicitudes indicativo de un sistema de autorización para autorizar el acceso al recurso protegido;
identificar (511), en la base de datos configurable, un tipo de método de concesión seleccionado de uno o más de los tipos de métodos de concesión asociados con un identificador del sistema de autorización correspondiente al identificador de solicitud;
identificar (511), en la base de datos configurable, un tipo de método de autenticación seleccionado, de uno o más de los tipos de métodos de autenticación asociados con el identificador del sistema de autorización correspondiente al identificador de solicitud;
ejecutar (513), en el sistema del cliente, la parte del código del método de concesión correspondiente al tipo de método de concesión seleccionado para solicitar el token de acceso para acceder al recurso protegido;
ejecutar (513), en el sistema cliente, la porción de código del método de autenticación correspondiente al tipo de método de autenticación seleccionado para autenticar el sistema del cliente en el sistema de autorización; y
recibir (514) el token de acceso en el sistema cliente desde el sistema de autorización, en respuesta a la ejecución de la parte del código del método de concesión y la parte del código del método de autenticación.

2. El método implementado por computadora de la reivindicación 1 que comprende además:

modificar (505A), en el sistema del cliente, uno o más de la pluralidad de tipos de método de concesión en la base de datos configurable asociada con al menos uno de la pluralidad de identificadores del sistema de autorización almacenados en la base de datos configurable, formando así una base de datos configurable modificada;
identificar (511), en el sistema cliente, un tipo de método de concesión seleccionado, en la base de datos configurable modificada, de uno o más de los tipos de métodos de concesión asociados con un identificador del sistema de autorización correspondiente al identificador de solicitud; y
ejecutar (513), en el sistema cliente, la porción del código del método de concesión correspondiente al tipo de método de concesión seleccionado para solicitar el token de acceso para acceder al recurso protegido.

3. El método implementado por computadora de la reivindicación 1 o la reivindicación 2, que comprende además:

modificar (505B), en el sistema cliente, el uno o más de la pluralidad de tipos de método de autenticación en la base de datos configurable asociada con al menos uno de la pluralidad de identificadores del sistema de autorización almacenados en la base de datos configurable, formando así una base de datos configurable modificada en el sistema cliente;
identificar (511), en el sistema del cliente, un tipo de método de autenticación seleccionado, en la base de datos configurable modificada, de uno o más de los tipos de métodos de autenticación asociados con un identificador del sistema de autorización correspondiente al identificador de solicitud; y
ejecutar (513), en el sistema cliente, la parte del código del método de autenticación correspondiente al tipo de método de autenticación seleccionado para autenticar el sistema cliente en el sistema de autorización.

4. El método implementado por computadora de cualquiera de las reivindicaciones anteriores que comprende además:

transmitir (505C) una solicitud de base de datos a un sistema host de bases de datos desde el sistema cliente y, en respuesta, recibir (505D) en el sistema del cliente al menos una parte de una base de datos; y
actualizar (505D), uno o más de la pluralidad de tipos de método de concesión y/o uno o más de la pluralidad de tipos de método de autenticación asociados con al menos uno de la pluralidad de identificadores del sistema de autorización almacenados en la base de datos configurable utilizando la base de datos recibida.

5. El método implementado por computadora de la reivindicación 4, en donde la solicitud de la base de datos se transmite de forma intermitente de acuerdo con un programa predeterminado y, opcionalmente, en donde el programa predeterminado define un intervalo de tiempo entre solicitudes de bases de datos consecutivas.

6. El método implementado por computadora de cualquiera de las reivindicaciones anteriores en donde al menos uno de los identificadores del sistema de autorización está asociado con una pluralidad de uno o más tipos de método de concesión que son compatibles con el sistema de autorización respectivo, y el método comprende además:

identificar (511) en la base de datos configurable, en el sistema del cliente, los tipos de métodos de concesión asociados con el identificador del sistema de autorización correspondiente al primer identificador;
seleccionar (511A), en el sistema del cliente, un tipo de método de concesión de los tipos de método de concesión identificados; y
ejecutar (513), en el sistema del cliente, la parte del código del método de concesión correspondiente al tipo de método de concesión seleccionado.

7. El método implementado por computadora de la reivindicación 6 que comprende además:

clasificar, en el sistema del cliente, la pluralidad de tipos de métodos de concesión almacenados en el base de datos configurable basada en la fortaleza de seguridad de cada tipo de método de concesión; en donde el paso de selección (511A) comprende seleccionar (511B) de los tipos de método de concesión identificados, el tipo de método de concesión que se clasifica con la mayor seguridad en relación con los otros tipos de métodos de concesión identificados.

8. El método implementado por computadora de cualquiera de las reivindicaciones anteriores, en donde al menos uno de la pluralidad de identificadores del sistema de autorización está asociado con una pluralidad de uno o más tipos de método de autenticación que son compatibles con el sistema de autorización respectivo, y el método comprende además:

identificar (511) en la base de datos configurable, en el sistema del cliente, los tipos de métodos de autenticación
asociados con el identificador del sistema de autorización correspondiente al primer identificador;
seleccionar (511A), en el sistema del cliente, un tipo de método de autorización de la pluralidad de tipos de métodos de autorización identificados; y
ejecutar (513), en el sistema cliente, la porción de código del método de autenticación correspondiente al tipo de método de autenticación seleccionado.

9. El método implementado por computadora de la reivindicación 8 que comprende además:

clasificar, en el sistema del cliente, la pluralidad de tipos de métodos de autenticación almacenados en la base de datos configurable en función de la seguridad de cada tipo de método de autenticación respectivo;
en donde el paso de seleccionar (511A) comprende seleccionar (511B), de los tipos de métodos de autenticación identificados, el tipo de método de autenticación clasificado con la mayor seguridad en relación con los otros tipos de métodos de autenticación identificados.

10. El método implementado por computadora de cualquiera de las reivindicaciones anteriores, en donde la pluralidad de porciones de código del método de concesión comprende una porción de código del método de concesión de código de autorización que cuando se ejecuta hace que el sistema cliente:

transmita (313) una instrucción al dispositivo del usuario para redirigir el dispositivo del usuario al sistema de autorización;
reciba (321) un código de autorización del dispositivo del usuario; y
transmita (323) el código de autorización al sistema de autorización y, en respuesta, reciba (325) el token de acceso.

11. El método implementado por computadora de cualquiera de las reivindicaciones anteriores, en donde la pluralidad de porciones de código del método de concesión comprende una porción de código del método de concesión de credenciales del cliente que cuando se ejecuta hace que el sistema del cliente:

transmita un secreto compartido al sistema de autorización y, en respuesta, reciba el token de acceso, sin solicitar un código de autorización.

12. El método implementado por computadora de cualquiera de las reivindicaciones anteriores, en donde la pluralidad de porciones de código del método de autenticación comprende una porción de código del método secreto del cliente que cuando se ejecuta hace que el sistema del cliente:

transmita un secreto compartido al sistema de autorización para autenticar el sistema cliente en el sistema de autorización.

13. El método implementado por computadora de cualquiera de las reivindicaciones anteriores, en donde la pluralidad de porciones de código del método de autenticación comprende una porción de código del método de afirmación del cliente que cuando se ejecuta hace que el sistema cliente:

transmita un identificador de integridad protegido del sistema del cliente al sistema de autorización para autenticar el sistema del cliente en el sistema de autorización.

14. El método implementado por computadora de cualquiera de las reivindicaciones anteriores que comprende además:

transmitir el token de acceso del sistema cliente al sistema de recursos y, en respuesta, recibir el recurso protegido.

15. Un sistema cliente (103) para obtener un token de acceso para acceder a un recurso protegido almacenado en un sistema de recursos (107), comprendiendo el sistema cliente (103):

un recurso de almacenamiento (825) configurado para almacenar:

una pluralidad de porciones de código del método de concesión, cada una ejecutable para obtener acceso al token de acceso utilizando uno de una pluralidad de tipos de método de concesión, en donde cada tipo respectivo de método de concesión es diferente a los otros tipos de método de concesión;

una pluralidad de porciones de código del método de concesión, cada una ejecutable para autenticar el sistema cliente utilizando un método de autenticación diferente, en donde cada tipo respectivo de método de autenticación es diferente a los otros tipos de método de autenticación;

una base de datos configurable (831) que comprende una pluralidad de identificadores de sistema de autenticación, cada uno identificativo de un sistema de autorización respectivo (105), en donde cada uno de la pluralidad de identificadores de sistema de autenticación está asociado con uno o más de la pluralidad de tipos de método de concesión que son apoyados por el sistema de autorización respectivo (105), y cada uno de la pluralidad de identificadores de sistema de autorización está asociado con uno o más de la pluralidad de tipos de método de autenticación que son apoyados por el sistema de autorización respectivo (105);

el sistema cliente (103) comprende además la circuitería de procesamiento configurada para:

recibir, desde un dispositivo de usuario (101), una solicitud de acceso que comprende una instrucción para que el sistema cliente (103) acceda a un recurso protegido, comprendiendo la instrucción un identificador de solicitud indicativo de un sistema de autorización (105) para autorizar el acceso al recurso protegido;

identificar un tipo de método de concesión seleccionado, en la base de datos configurable (831), de uno o más de los tipos de método de concesión asociados con un identificador del sistema de autorización correspondiente al identificador de solicitud;

identificar un tipo de método de autenticación seleccionado, en la base de datos configurable (831), de uno o más de los tipos de métodos de autenticación asociados con el identificador del sistema de autorización correspondiente al identificador de solicitud;

ejecutar la parte del código del método de concesión correspondiente al tipo de método de concesión seleccionado para solicitar el token de acceso para acceder al recurso protegido;

ejecutar la parte del código del método de autenticación correspondiente al tipo de método de autenticación seleccionado para autenticar el sistema cliente (103) en el sistema de autorización (105); y

recibir el token de acceso del sistema de autorización (105), en respuesta a la ejecución de la parte del código del método de concesión y la parte del código del método de autenticación.

FIG. 1

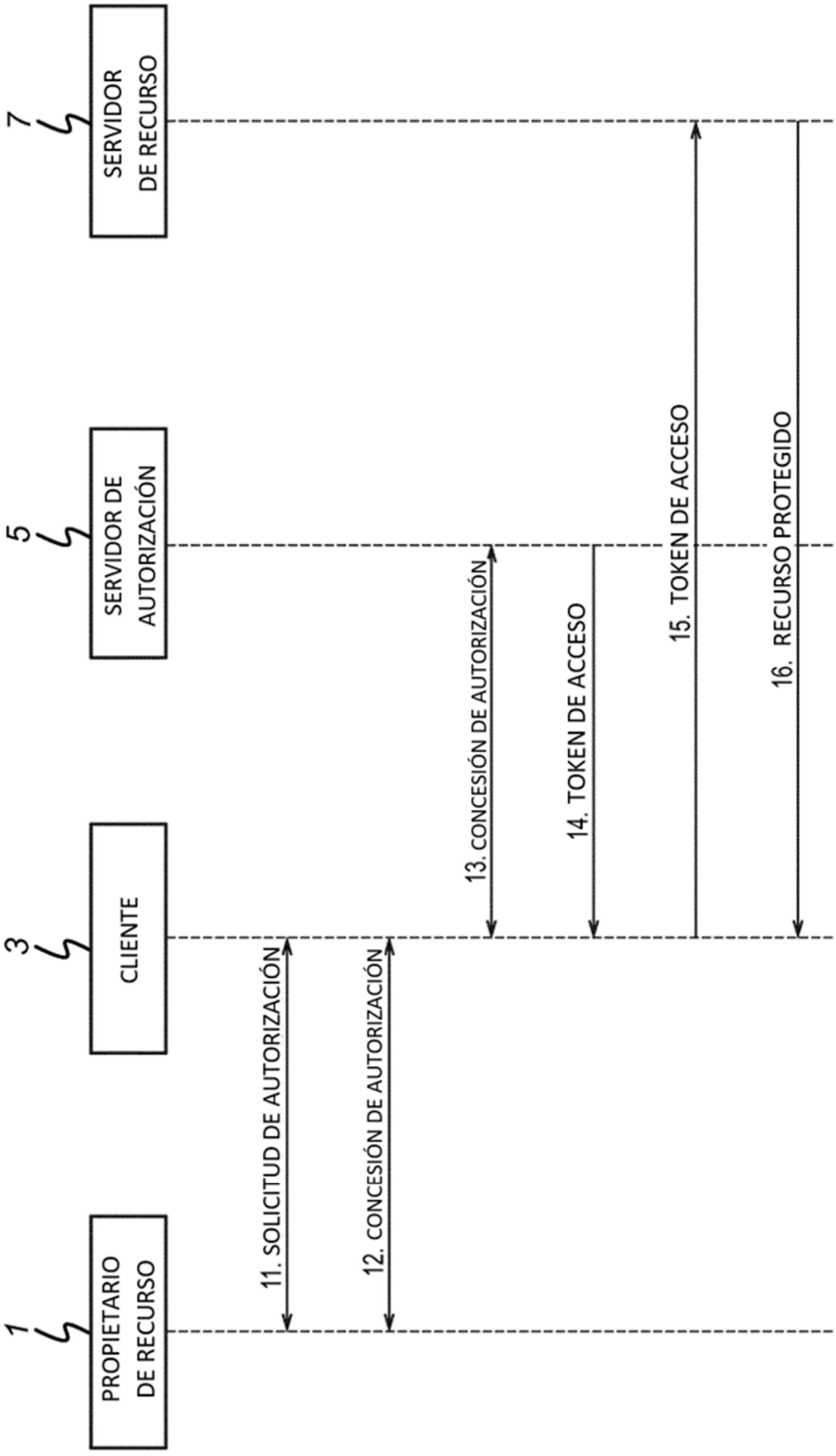
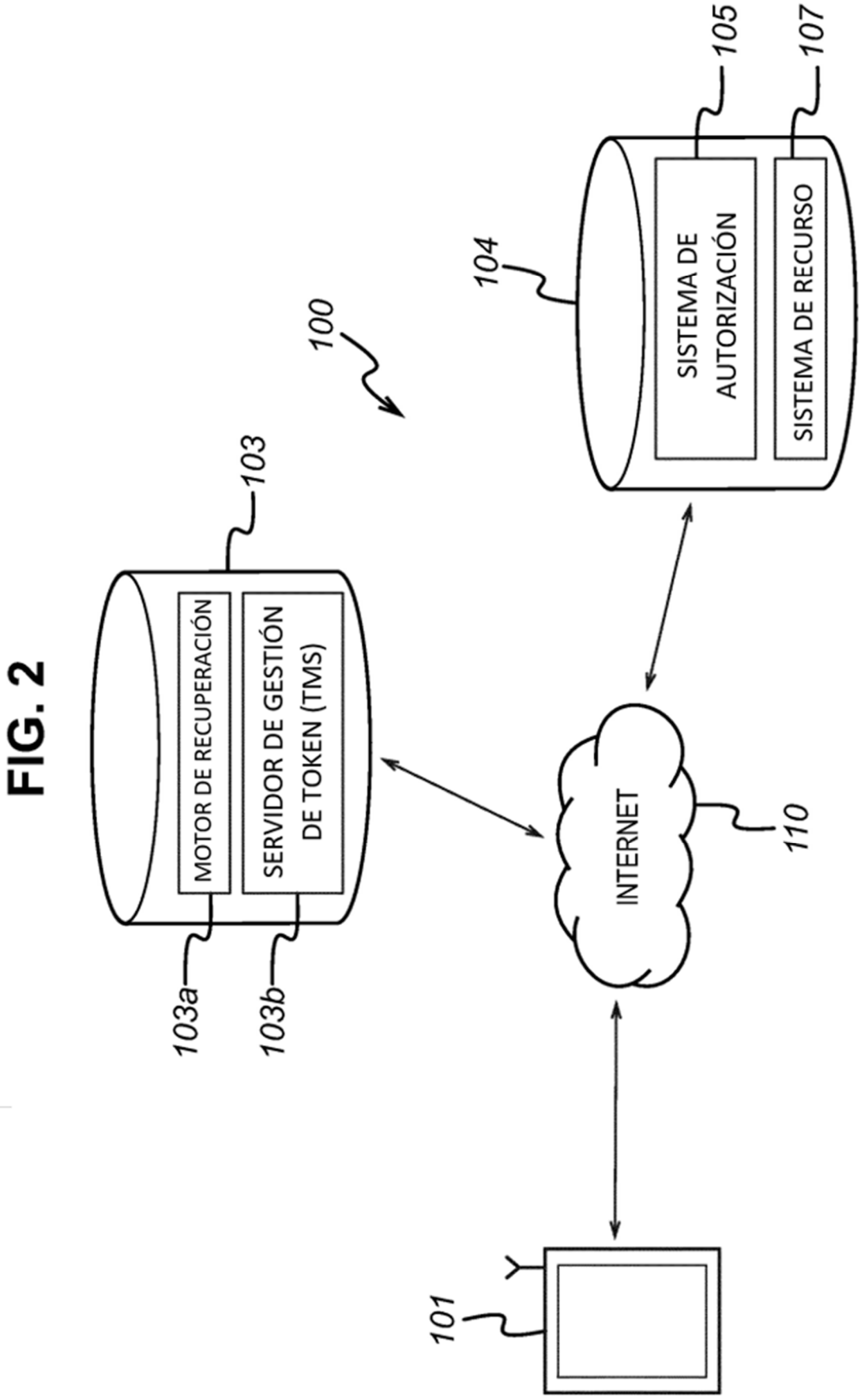

1
PROPIETARIO DE RECURSO
3
CLIENTE
5
SERVIDOR DE AUTORIZACIÓN
7
SERVIDOR DE RECURSO
11. SOLICITUD DE AUTORIZACIÓN
12. CONCESIÓN DE AUTORIZACIÓN
13. CONCESIÓN DE AUTORIZACIÓN
14. TOKEN DE ACCESO
15. TOKEN DE ACCESO
16. RECURSO PROTEGIDO

FIG. 2


100
101
103
103a
103b
104
105
107
110
MOTOR DE RECUPERACIÓN
SERVIDOR DE GESTIÓN DE TOKEN (TMS)
SISTEMA DE AUTORIZACIÓN
SISTEMA DE RECURSO
INTERNET

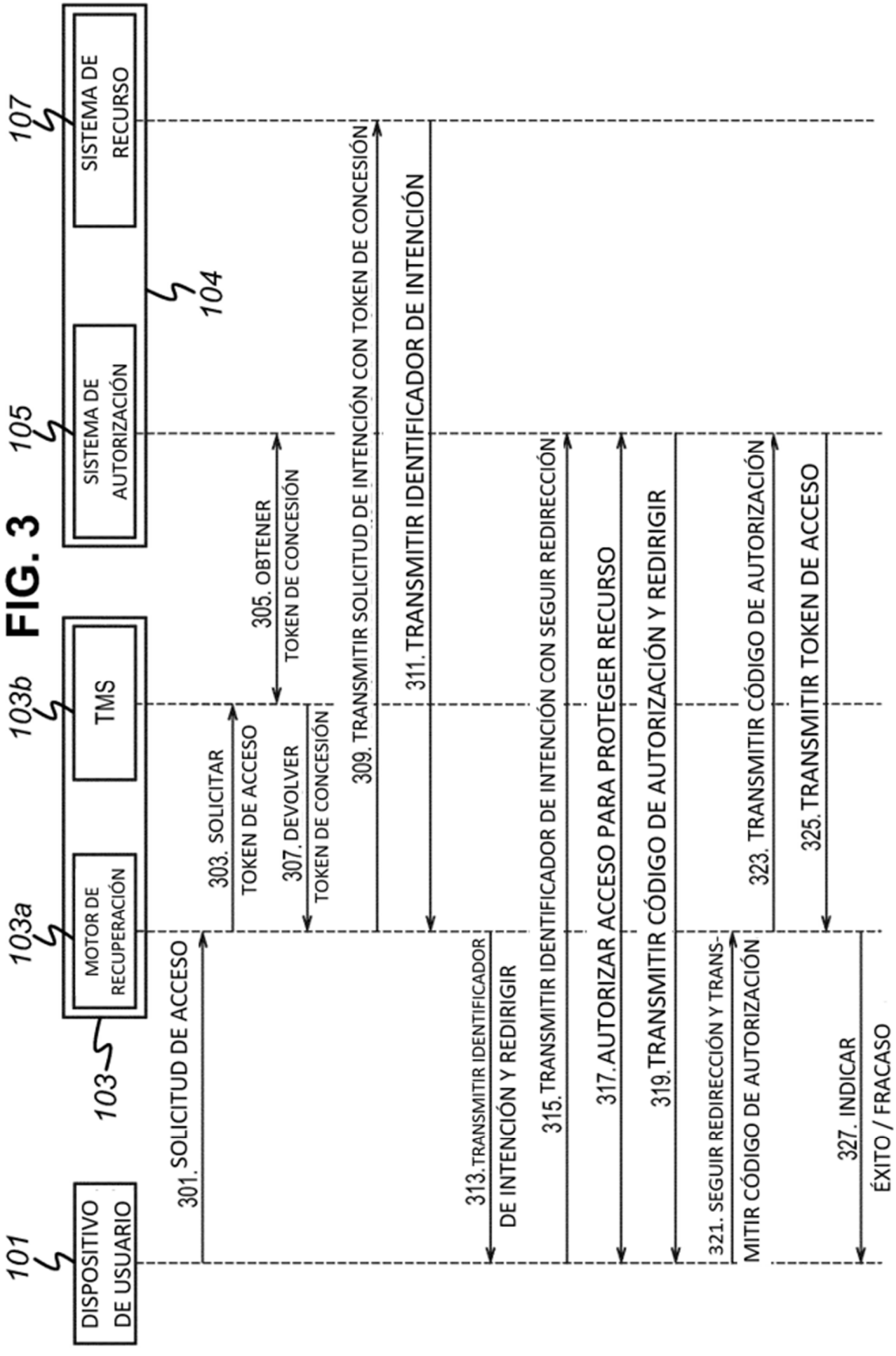

101
DISPOSITIVO DE USUARIO
103
103a
MOTOR DE RECUPERACIÓN
103b
TMS
105
SISTEMA DE AUTORIZACIÓN
104
107
SISTEMA DE RECURSO
301. SOLICITUD DE ACCESO
303. SOLICITAR TOKEN DE ACCESO
305. OBTENER TOKEN DE CONCESIÓN
307. DEVOLVER TOKEN DE CONCESIÓN
309. TRANSMITIR SOLICITUD DE INTENCIÓN CON TOKEN DE CONCESIÓN
311. TRANSMITIR IDENTIFICADOR DE INTENCIÓN
313. TRANSMITIR IDENTIFICADOR DE INTENCIÓN Y REDIRIGIR
315. TRANSMITIR IDENTIFICADOR DE INTENCIÓN CON SEGUIR REDIRECCIÓN
317. AUTORIZAR ACCESO PARA PROTEGER RECURSO
319. TRANSMITIR CÓDIGO DE AUTORIZACIÓN Y REDIRIGIR
321. SEGUIR REDIRECCIÓN Y TRANSMITIR CÓDIGO DE AUTORIZACIÓN
323. TRANSMITIR CÓDIGO DE AUTORIZACIÓN
325. TRANSMITIR TOKEN DE ACCESO
327. INDICAR ÉXITO / FRACASO

FIG. 3

FIG. 4

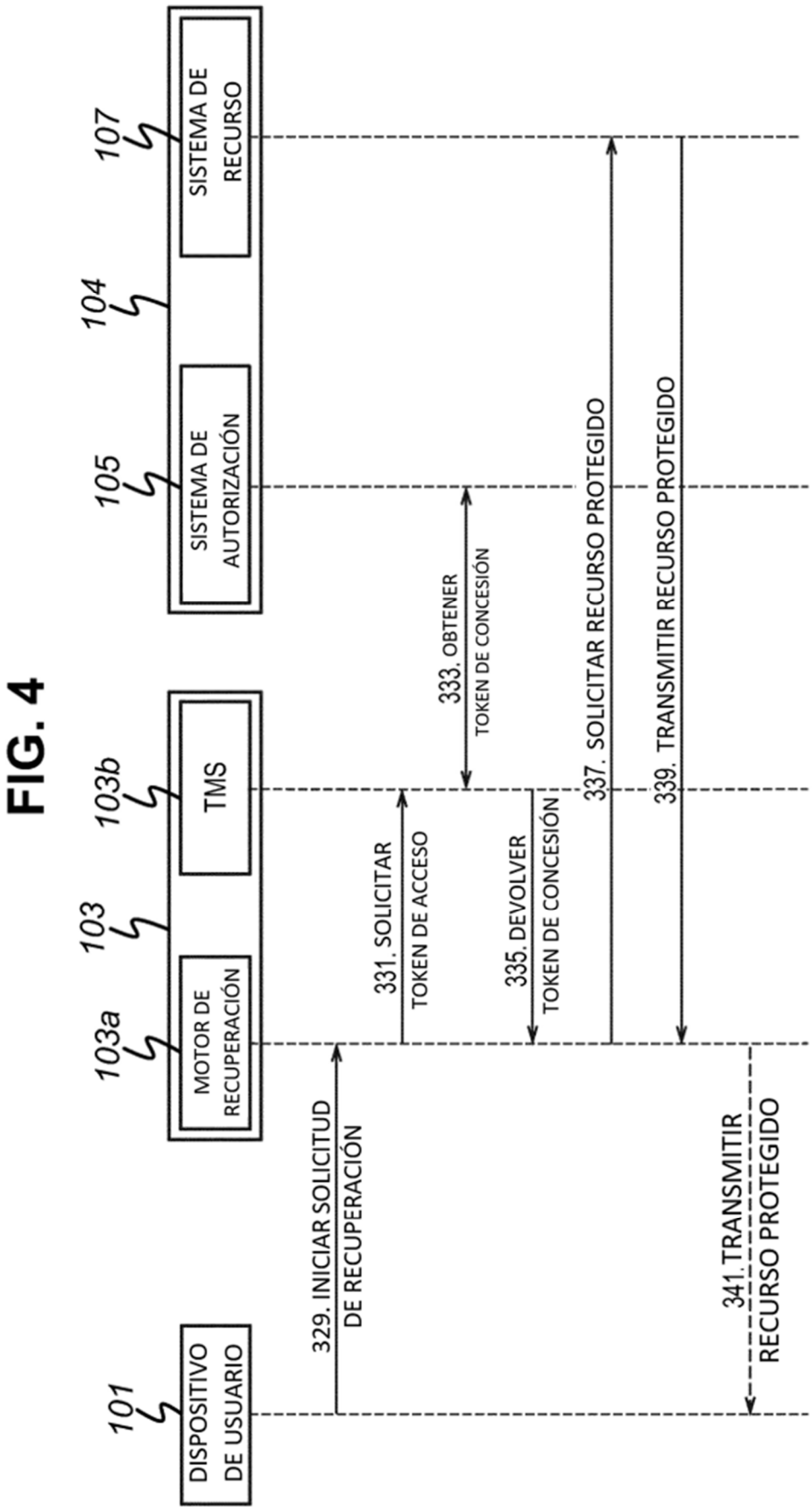

101
DISPOSITIVO DE USUARIO
103
103a
MOTOR DE RECUPERACIÓN
103b
TMS
104
105
SISTEMA DE AUTORIZACIÓN
107
SISTEMA DE RECURSO
329. INICIAR SOLICITUD DE RECUPERACIÓN
331. SOLICITAR TOKEN DE ACCESO
333. OBTENER TOKEN DE CONCESIÓN
335. DEVOLVER TOKEN DE CONCESIÓN
337. SOLICITAR RECURSO PROTEGIDO
339. TRANSMITIR RECURSO PROTEGIDO
341. TRANSMITIR RECURSO PROTEGIDO

FIG. 5

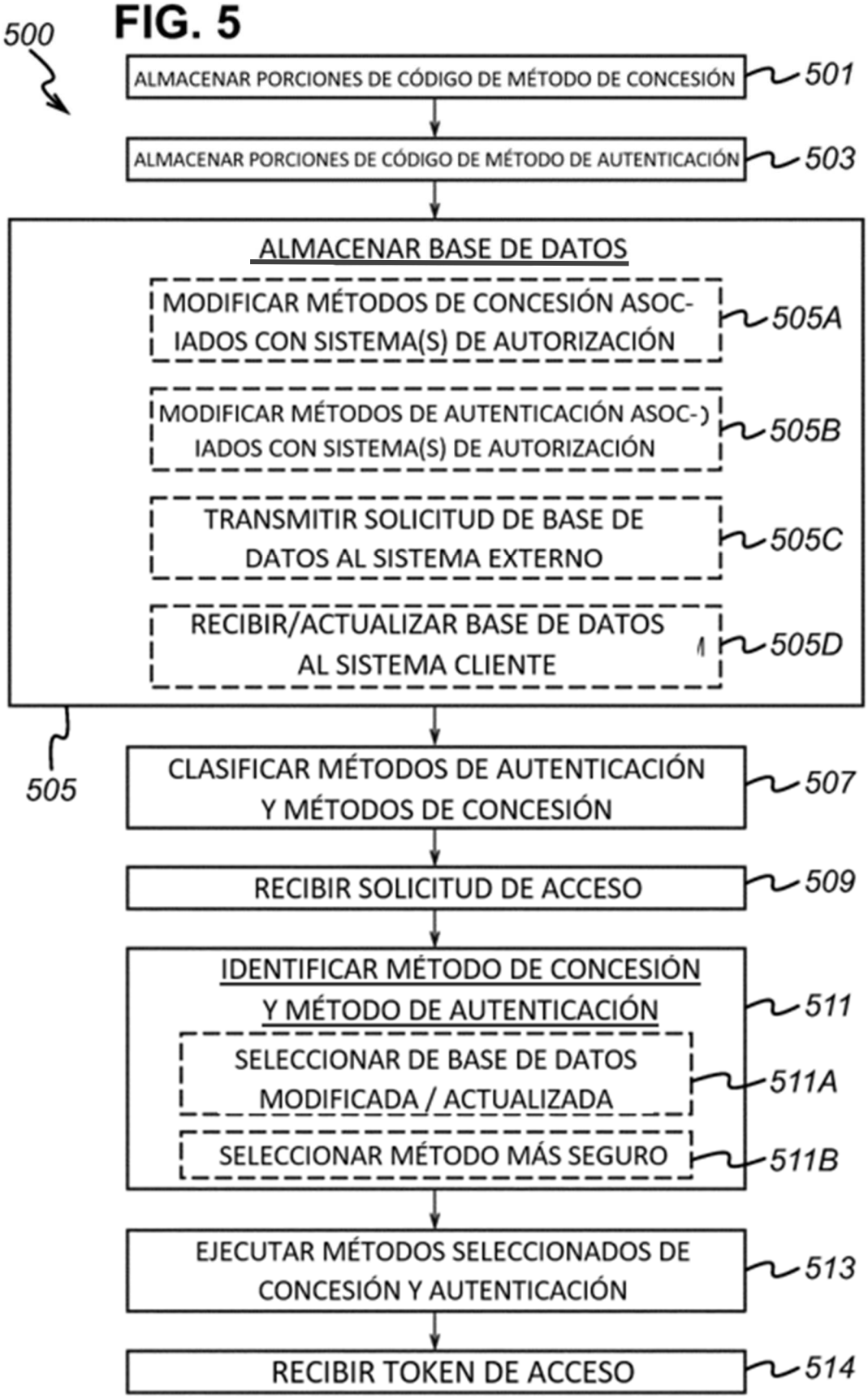

500
ALMACENAR PORCIONES DE CÓDIGO DE MÉTODO DE CONCESIÓN
501
ALMACENAR PORCIONES DE CÓDIGO DE MÉTODO DE AUTENTICACIÓN
503
ALMACENAR BASE DE DATOS
MODIFICAR MÉTODOS DE CONCESIÓN ASOC-IADOS CON SISTEMA(S) DE AUTORIZACIÓN
505A
MODIFICAR MÉTODOS DE AUTENTICACIÓN ASOC-) IADOS CON SISTEMA(S) DE AUTORIZACIÓN
505B
TRANSMITIR SOLICITUD DE BASE DE DATOS AL SISTEMA EXTERNO
505C
RECIBIR/ACTUALIZAR BASE DE DATOS AL SISTEMA CLIENTE
505D
505
CLASIFICAR MÉTODOS DE AUTENTICACIÓN Y MÉTODOS DE CONCESIÓN
507
RECIBIR SOLICITUD DE ACCESO
509
IDENTIFICAR MÉTODO DE CONCESIÓN Y MÉTODO DE AUTENTICACIÓN
511
SELECCIONAR DE BASE DE DATOS MODIFICADA / ACTUALIZADA
511A
SELECCIONAR MÉTODO MÁS SEGURO
511B
EJECUTAR MÉTODOS SELECCIONADOS DE CONCESIÓN Y AUTENTICACIÓN
513
RECIBIR TOKEN DE ACCESO
514

FIG. 6

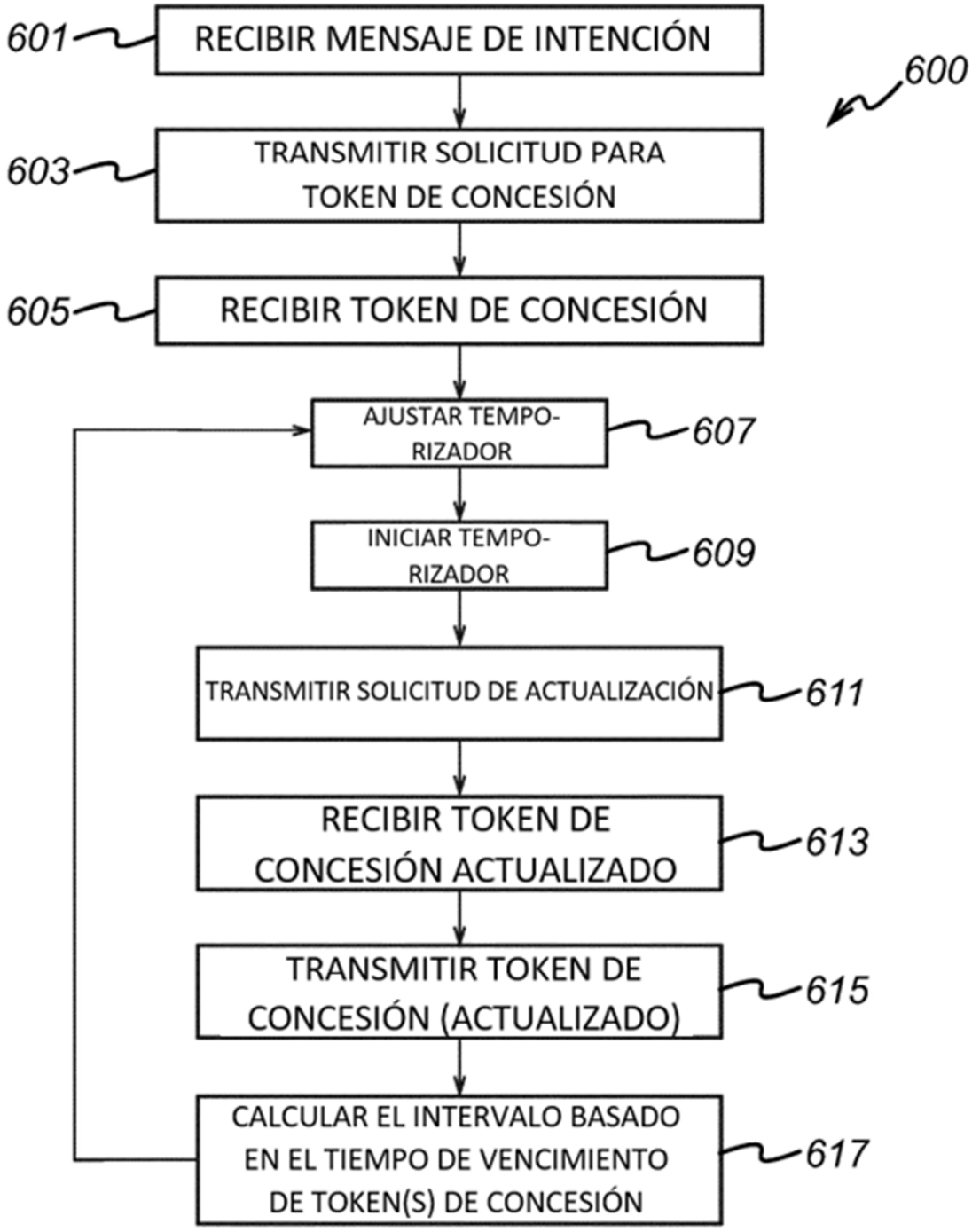

601
RECIBIR MENSAJE DE INTENCIÓN
600
603
TRANSMITIR SOLICITUD PARA TOKEN DE CONCESIÓN
605
RECIBIR TOKEN DE CONCESIÓN
AJUSTAR TEMPO-RIZADOR
607
INICIAR TEMPO-RIZADOR
609
TRANSMITIR SOLICITUD DE ACTUALIZACIÓN
611
RECIBIR TOKEN DE CONCESIÓN ACTUALIZADO
613
TRANSMITIR TOKEN DE CONCESIÓN (ACTUALIZADO)
615
CALCULAR EL INTERVALO BASADO EN EL TIEMPO DE VENCIMIENTO DE TOKEN(S) DE CONCESIÓN
617

FIG. 7

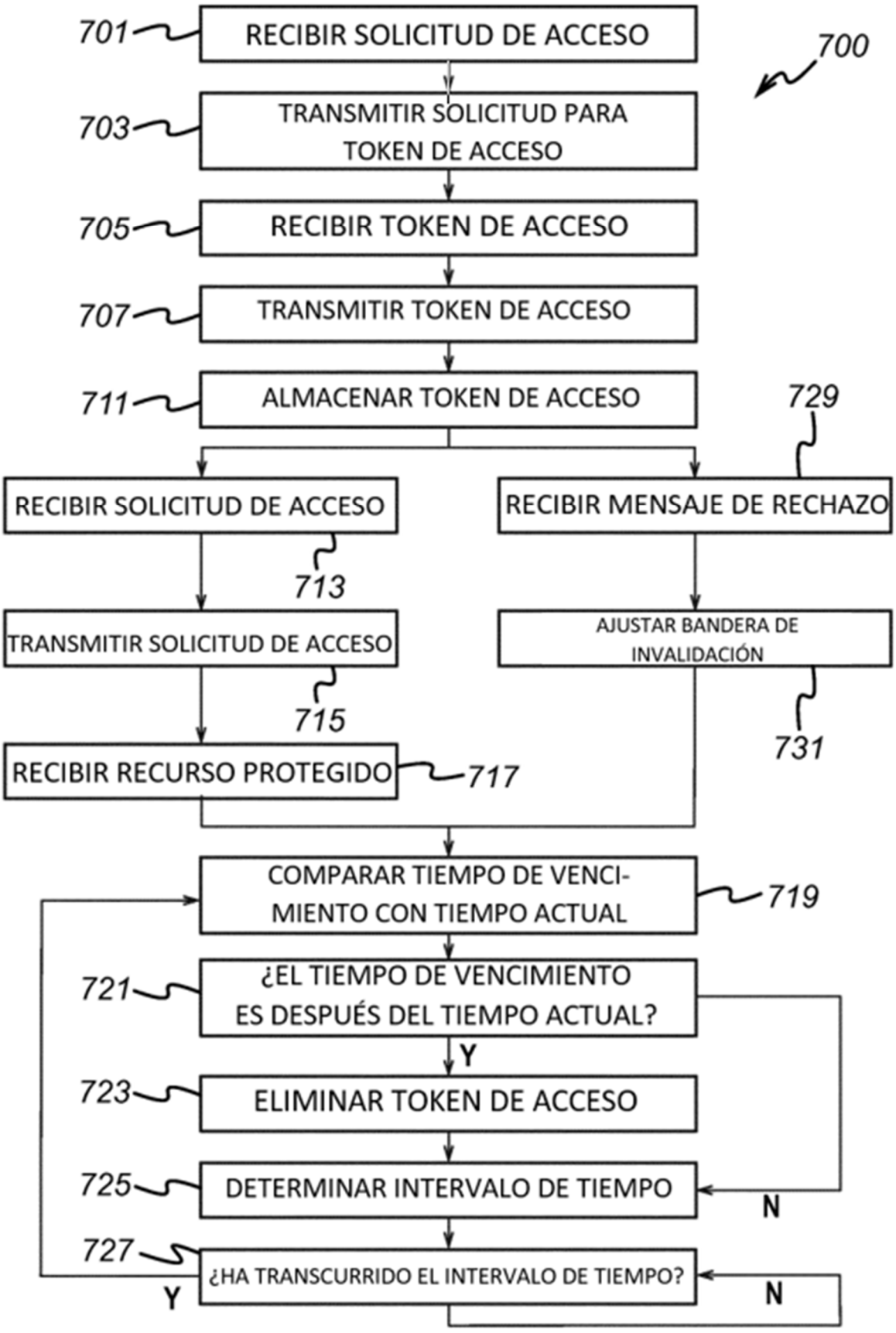

701
RECIBIR SOLICITUD DE ACCESO
700
703
TRANSMITIR SOLICITUD PARA TOKEN DE ACCESO
705
RECIBIR TOKEN DE ACCESO
707
TRANSMITIR TOKEN DE ACCESO
711
ALMACENAR TOKEN DE ACCESO
729
RECIBIR SOLICITUD DE ACCESO
RECIBIR MENSAJE DE RECHAZO
713
TRANSMITIR SOLICITUD DE ACCESO
AJUSTAR BANDERA DE INVALIDACIÓN
715
731
RECIBIR RECURSO PROTEGIDO
717
COMPARAR TIEMPO DE VENCIMIENTO CON TIEMPO ACTUAL
719
721
¿EL TIEMPO DE VENCIMIENTO ES DESPUÉS DEL TIEMPO ACTUAL?
Y
723
ELIMINAR TOKEN DE ACCESO
725
DETERMINAR INTERVALO DE TIEMPO
N
727
¿HA TRANSCURRIDO EL INTERVALO DE TIEMPO?
Y
N

FIG. 8

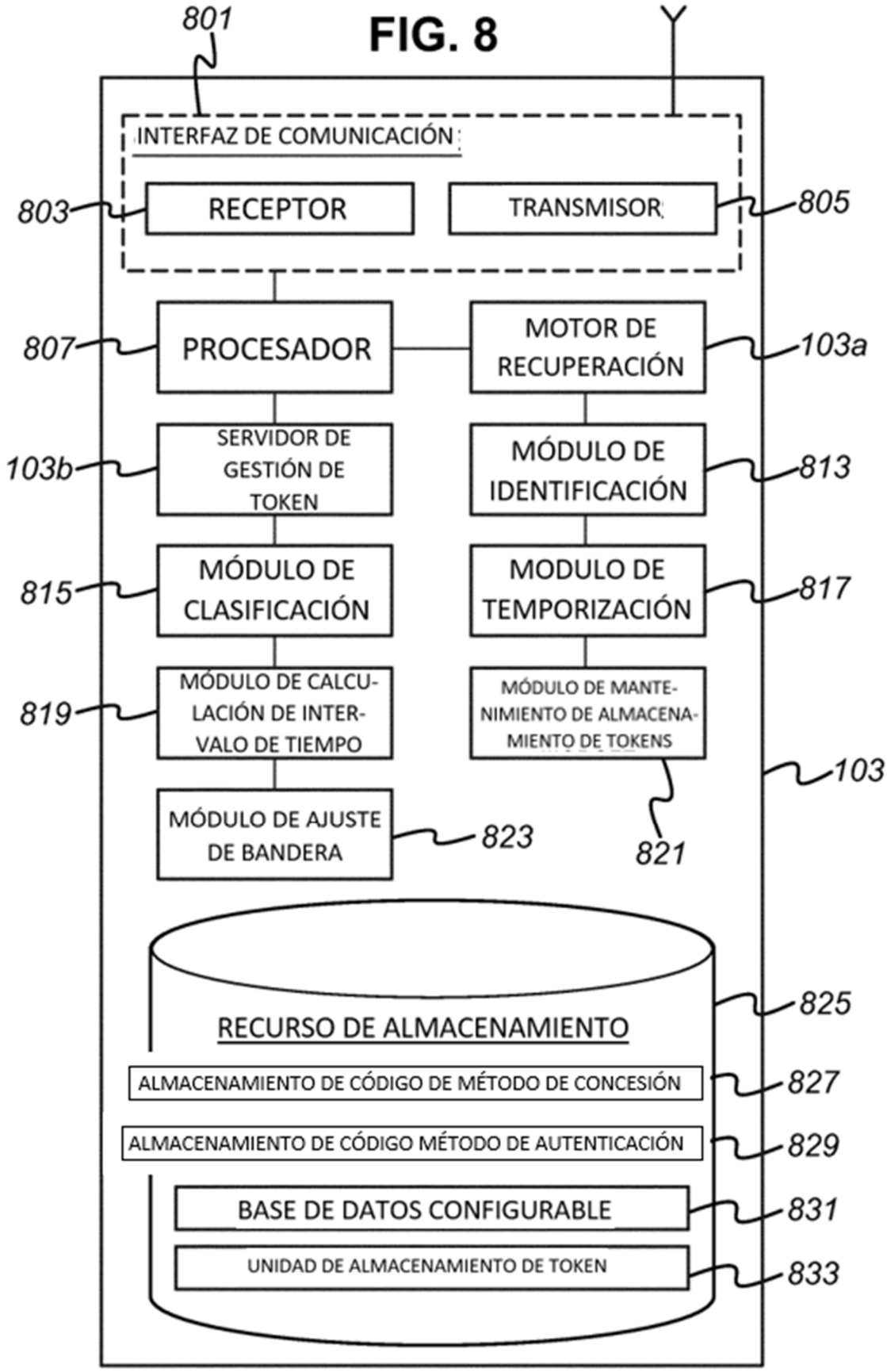
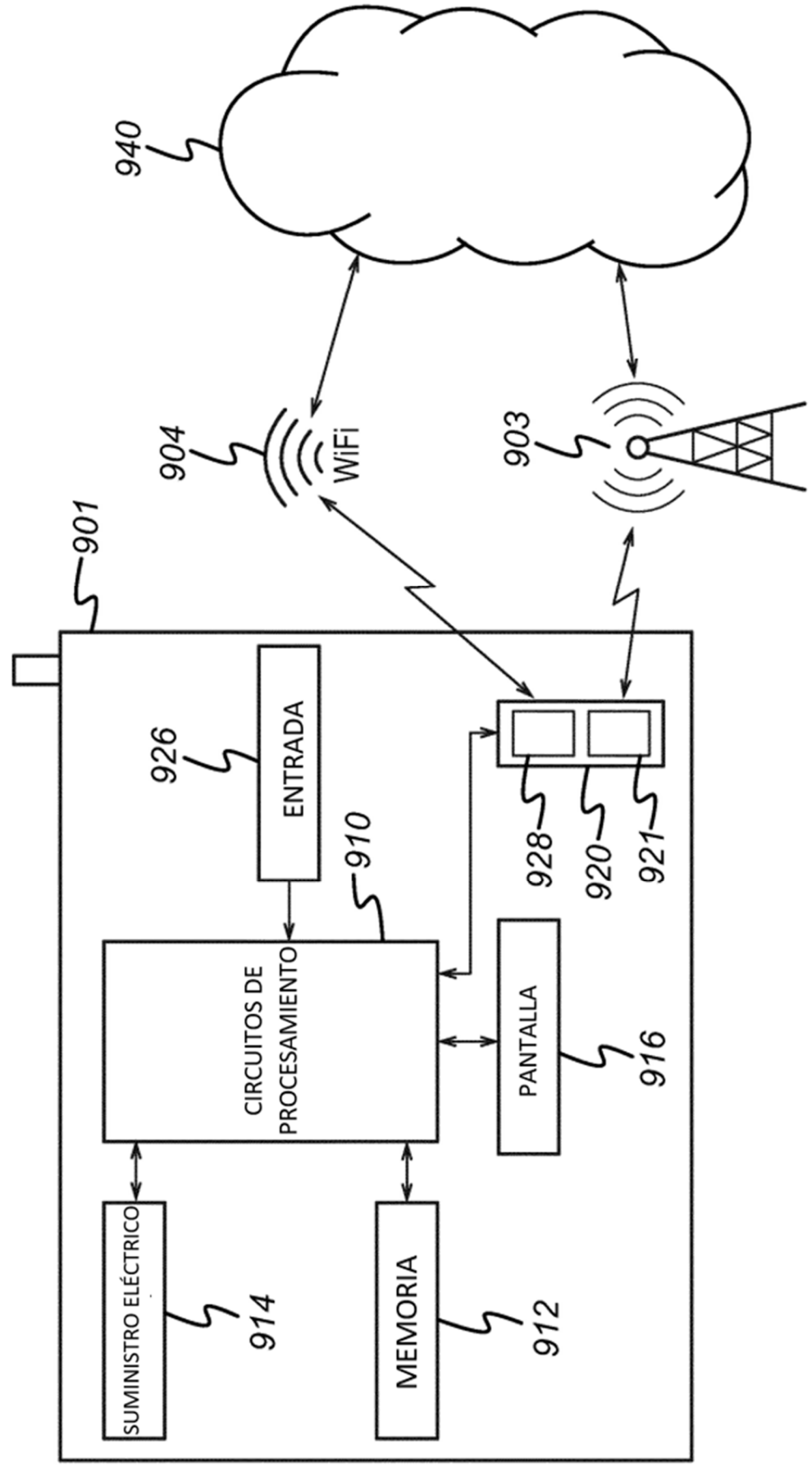

801
INTERFAZ DE COMUNICACIÓN
803
RECEPTOR
TRANSMISOR
805
807
PROCESADOR
MOTOR DE RECUPERACIÓN
103a
103b
SERVIDOR DE GESTIÓN DE TOKEN
MÓDULO DE IDENTIFICACIÓN
813
815
MÓDULO DE CLASIFICACIÓN
MODULO DE TEMPORIZACIÓN
817
819
MÓDULO DE CALCULACIÓN DE INTERVALO DE TIEMPO
MÓDULO DE MANTENIMIENTO DE ALMACENAMIENTO DE TOKENS
103
MÓDULO DE AJUSTE DE BANDERA
823
821
825
RECURSO DE ALMACENAMIENTO
ALMACENAMIENTO DE CÓDIGO DE MÉTODO DE CONCESIÓN
827
ALMACENAMIENTO DE CÓDIGO MÉTODO DE AUTENTICACIÓN
829
BASE DE DATOS CONFIGURABLE
831
UNIDAD DE ALMACENAMIENTO DE TOKEN
833

FIG. 9


940
904
WiFi
903
901
926
ENTRADA
910
928
920
921
CIRCUITOS DE PROCESAMIENTO
PANTALLA
916
SUMINISTRO ELÉCTRICO
914
MEMORIA
912