(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 875 366**

(51) Int. CI.:

G06F 21/62 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.02.2018 E 18155399 (1)**

(97) Fecha y número de publicación de la concesión europea: **31.03.2021 EP 3522062**

(54) Título: **Sistema para autorizar acceso de datos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.11.2021

(73) Titular/es:

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

(72) Inventor/es:

FORREST, MICHAEL

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Sistema para autorizar acceso de datos

Campo técnico

Esta divulgación se refiere a un sistema, un método y un programa informático para autorizar el acceso a datos de usuario seguros.

Antecedentes

En los sistemas de comunicaciones digitales, los datos pueden transferirse entre dispositivos a altas velocidades y en grandes volúmenes. Esto es ventajoso para distribuir información ampliamente, pero tiene el inconveniente de la posibilidad de que datos confidenciales se distribuyan a entidades maliciosas o fraudulentas que pueden comprometer la seguridad de un usuario. Por lo tanto, es de suma importancia que los sistemas de comunicaciones digitales estén diseñados para permitir que los datos sensibles se compartan de una manera estrictamente controlada para evitar que dichas entidades maliciosas o fraudulentas accedan a los datos privados de un usuario. La US 9,641,517 describe un sistema y método para proporcionar características de seguridad para comunicaciones entre ordenadores. Después de que un usuario ha probado una asociación con una de varias formas, se recibe un identificador de usuario del usuario que no puede usarse para registrar al usuario en un sistema de consolidación de datos por un sistema de coincidencia del sistema de consolidación de datos. La validez del usuario y la forma se verifican en el sistema de coincidencia y, en respuesta a la verificación, el identificador de usuario se convierte en un identificador de usuario diferente y el identificador de usuario diferente se proporciona a un sistema de provisión de datos por el sistema de coincidencia. El sistema de provisión de datos proporciona los datos al usuario en respuesta, y el sistema de coincidencia envía los datos al sistema de consolidación de datos.

Sumario

La invención se expone en las reivindicaciones adjuntas. En un aspecto de la invención, hay un método implementado por ordenador para compartir datos asociados con un primer usuario, el método comprendiendo: almacenar, en un primer sistema, datos de usuario asociados con el primer usuario; almacenar, en el primer sistema, una base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; almacenar, en el primer sistema, una base de datos de entidades no autorizadas que comprende una pluralidad de etiquetas de entidades no autorizadas, cada una indicativa de un identificador de una entidad no autorizada; recibir un primer mensaje de acceso, desde un segundo sistema, asociado con una solicitud de acceso a los datos de usuario almacenados en el primer sistema, el primer mensaje de acceso comprendiendo una segunda etiqueta del sistema indicativa de un identificador del segundo sistema; en respuesta a recibir el primer mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades autorizadas y la pluralidad de etiquetas de entidades no autorizadas almacenadas en el primer sistema; en respuesta a la identificación de que la segunda etiqueta del sistema coincide con una etiqueta de entidad autorizada y que la segunda etiqueta del sistema no coincide con una etiqueta de entidad no autorizada, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso; e impedir la transmisión del mensaje de concesión, si la segunda etiqueta del sistema en el primer mensaje de acceso coincide con una etiqueta de entidad no autorizada y/o no coincide con una etiqueta de entidad autorizada.

De esta manera, el método permite verificar la identidad del segundo sistema tanto con la base de datos de entidades autorizadas como con la base de datos de entidades no autorizadas, de tal manera que el primer sistema puede determinar si el segundo sistema es una entidad autorizada. La base de datos de entidades no autorizadas puede usarse para anular cualquier decisión tomada en base a la base de datos de entidades autorizadas. Esto permite que la base de datos de entidades no autorizadas corrija cualquier error que pueda estar presente en la base de datos de entidades autorizadas. Por ejemplo, la base de datos de entidades autorizadas puede estar desactualizada y puede indicar incorrectamente que una entidad en particular está autorizada. En esta situación, se puede hacer referencia a la base de datos de entidades no autorizadas para asegurarse que los datos seguros del usuario no se envíen a la entidad que de hecho no es una entidad autorizada.

En otro aspecto de la invención, hay un método implementado por ordenador para compartir datos asociados con un primer usuario, el método comprendiendo: almacenar, en un primer sistema, datos de usuario asociados con el primer usuario; transmitir, desde el primer sistema a un sistema de autorización, una solicitud para acceder a una base de datos de entidades autorizadas almacenada en el sistema de autorización, en donde la base de datos de entidades autorizadas comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; recibir y almacenar, en el primer sistema, por lo menos una parte de la base de datos de entidades autorizadas; recibir un mensaje de acceso, desde un segundo sistema, asociado con una solicitud de acceso a los datos almacenados en el primer sistema, el mensaje de acceso comprendiendo una segunda etiqueta del sistema indicativa de un identificador del segundo sistema; en respuesta a recibir el mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades

autorizadas almacenadas en el primer sistema; identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema y, en respuesta, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso.

De esta manera, el primer sistema puede verificar una copia local de la base de datos de entidades autorizadas en lugar de consultar el sistema de autorización. La verificación del sistema de autorización en cada caso en el que se requiere puede imponer una carga a los recursos de procesamiento. Por tanto, almacenar una copia local de la base de datos ayuda a aliviar esta carga. El sistema de autorización puede dar servicio a otros sistemas similares que requieren acceso a la base de datos de entidades autorizadas y, en esta situación, el sistema de autorización puede crear un denominado "cuello de botella" o un punto único de fallo para el sistema. El primer sistema puede detectar entidades autorizadas de manera más fiable y rápida almacenando una copia de la base de datos en el propio primer sistema. Esto mejorará la capacidad del primer sistema para garantizar la seguridad de los datos del usuario.

En otro aspecto de la invención, se proporciona un método implementado por ordenador para compartir datos asociados con un primer usuario, el método comprendiendo: almacenar, en un primer sistema, datos de usuario asociados con el primer usuario; almacenar, en el primer sistema, una base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; recibir un primer mensaje de acceso, desde un segundo sistema, asociado con una solicitud de acceso a los datos de usuario almacenados en el primer sistema, el primer mensaje de acceso comprendiendo una segunda etiqueta del sistema indicativa de un identificador del segundo sistema; en respuesta a recibir el primer mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema e identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema y, en respuesta, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso; recibir un segundo mensaje de acceso, desde el segundo sistema, asociado con la solicitud de acceso a los datos de usuario almacenados en el primer sistema, el segundo mensaje de acceso comprendiendo la segunda etiqueta del sistema; en respuesta a recibir el segundo mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema e identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema y, en respuesta, trasmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso.

De esta manera, es posible que el primer sistema determine si el segundo sistema está autorizado para recibir datos de usuario seguros en por lo menos dos casos antes de que se transmitan los datos. Puede haber un desfase entre la primera solicitud del segundo sistema para acceder a los datos y la segunda solicitud. En este momento, es posible que el segundo sistema pase de estar autorizado para recibir datos de usuario a no estar autorizado. Por ejemplo, el segundo sistema puede estar sujeto a una brecha de seguridad en este momento. Como el estado del segundo sistema se verifica inicialmente y una segunda vez antes de que se transfieran los datos, es posible evitar transmitir los datos a una entidad no autorizada.

En otro aspecto de la invención, hay un sistema de gestión de datos para compartir datos asociados con un primer usuario, el sistema de gestión de datos comprendiendo: un recurso de almacenamiento de datos configurado para: almacenar datos de usuario asociados con el primer usuario; almacenar una base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; y almacenar una base de datos de entidades no autorizadas que comprende una pluralidad de etiquetas de entidades no autorizadas, cada una indicativa de un identificador de una entidad no autorizada; y en donde el sistema de gestión de datos comprende además circuitos de procesamiento configurados para: recibir un primer mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso a los datos de usuario almacenados en el primer sistema, el primer mensaje de acceso comprendiendo una etiqueta de sistema remoto indicativa de un identificador del sistema remoto; comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas y la pluralidad de etiquetas de entidades no autorizadas almacenadas en el primer sistema, en respuesta a recibir el primer mensaje de acceso; transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso, en respuesta a identificar que la etiqueta del sistema remoto coincide con una etiqueta de entidad autorizada y que la etiqueta del sistema remoto no coincide con una etiqueta de entidad no autorizada; y evitar la transmisión del mensaje de concesión, si la etiqueta del sistema remoto en el primer mensaje de acceso coincide con una etiqueta de entidad no autorizada y/o no coincide con una etiqueta de entidad autorizada.

En otro aspecto de la invención, hay un sistema de gestión de datos para compartir datos asociados con un primer usuario, el sistema de gestión de datos comprendiendo: un recurso de almacenamiento de datos configurado para: almacenar datos de usuario asociados con el primer usuario; almacenar una base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; y almacenar una base de datos de entidades no autorizadas que comprende una pluralidad de etiquetas de entidades no autorizadas, cada una indicativa de un identificador de una entidad no

autorizada; un receptor dispuesto para recibir un primer mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso a los datos de usuario almacenados en el primer sistema, el primer mensaje de acceso comprendiendo una etiqueta de sistema remoto indicativa de un identificador del sistema remoto; un módulo de comparación dispuesto para comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas y la pluralidad de etiquetas de entidades no autorizadas almacenadas en el recurso de almacenamiento de datos en respuesta a la recepción del primer mensaje de acceso; y un transmisor dispuesto para transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso en respuesta a la identificación de que la etiqueta del sistema remoto coincide con una etiqueta de entidad autorizada y que la etiqueta del sistema remoto no coincide con una etiqueta de entidad no autorizada; y en donde el transmisor está dispuesto para evitar la transmisión del mensaje de concesión, si la etiqueta del sistema remoto en el primer mensaje de acceso coincide con una etiqueta de entidad no autorizada y/o no coincide con una etiqueta de entidad autorizada.

En otro aspecto de la invención, hay un sistema de gestión de datos para compartir datos asociados con un primer usuario, el sistema de gestión de datos comprendiendo: un recurso de almacenamiento de datos configurado para: almacenar datos de usuario asociados con el primer usuario; en donde el sistema de gestión de datos comprende además circuitos de procesamiento configurados para: transmitir, desde el sistema de gestión de datos a un sistema de autorización, una solicitud para acceder a una base de datos de entidades autorizadas almacenada en el sistema de autorización, en donde la base de datos de entidades autorizadas comprende una pluralidad de etiquetas de entidades autorizadas cada una indicativa de un identificador de una entidad autorizada; recibir y almacenar, en el sistema de gestión de datos, por lo menos una parte de la base de datos de entidades autorizadas; recibir un mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso para los datos almacenados en el sistema de gestión de datos, el mensaje de acceso comprendiendo una etiqueta del sistema remoto indicativa de un identificador del sistema remoto; en respuesta a recibir el mensaje de acceso, comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas almacenadas en el sistema de gestión de datos; identificar una coincidencia entre la etiqueta del sistema remoto y por lo menos una de la pluralidad de etiquetas de entidades autorizadas almacenadas en el sistema de gestión de datos y, en respuesta, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso.

En otro aspecto de la invención, hay un sistema de gestión de datos para compartir datos asociados con un primer usuario, el sistema de gestión de datos comprendiendo: un recurso de almacenamiento de datos configurado para almacenar datos de usuario asociados con el primer usuario; un transmisor dispuesto para transmitir, desde el sistema de gestión de datos a un sistema de autorización, una solicitud para acceder a una base de datos de entidades autorizadas almacenada en el sistema de autorización, en donde la base de datos de entidades autorizadas comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; un receptor dispuesto para recibir por lo menos una parte de la base de datos de entidades autorizadas, en donde el recurso de almacenamiento de datos está dispuesto para almacenar una parte de la base de datos de entidades autorizadas; en donde el receptor está dispuesto para recibir un mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso a los datos almacenados en el sistema de gestión de datos, el mensaje de acceso comprendiendo una etiqueta del sistema remoto indicativa de un identificador del sistema remoto; un módulo de comparación dispuesto para comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas almacenadas en el sistema de gestión de datos, en respuesta a la recepción del mensaje de acceso; y un módulo de identificación dispuesto para identificar una coincidencia entre la etiqueta del sistema remoto y por lo menos una de la pluralidad de etiquetas de entidades autorizadas almacenadas en el sistema de gestión de datos y, en respuesta, hacer que el transmisor transmita un mensaje de concesión indicativo de que se concede la solicitud de acceso.

En otro aspecto de la invención, hay un sistema de gestión de datos para compartir datos asociados con un primer usuario, el sistema de gestión de datos comprendiendo: un recurso de almacenamiento de datos configurado para: almacenar datos de usuario asociados con el primer usuario; almacenar una base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; en donde el sistema de gestión de datos comprende además circuitos de procesamiento configurados para: recibir un primer mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso para los datos del usuario, el primer mensaje de acceso comprendiendo una etiqueta del sistema remoto indicativa de un identificador del sistema; comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas, en respuesta a la recepción del primer mensaje de acceso, e identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades autorizadas y, en respuesta, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso; recibir un segundo mensaje de acceso, desde el sistema remoto, asociado con la solicitud de acceso a los datos del usuario, el segundo mensaje de acceso comprendiendo la etiqueta del sistema remoto; comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas, en respuesta a la recepción del segundo mensaje de acceso; e identificar una coincidencia entre la etiqueta del sistema remoto y por lo menos una de la pluralidad de etiquetas de entidades autorizadas y, en respuesta, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso.

En otro aspecto de la invención, hay un sistema de gestión de datos para compartir datos asociados con un

primer usuario, el sistema de gestión de datos comprendiendo: un recurso de almacenamiento de datos configurado para almacenar datos de usuario asociados con el primer usuario; y almacenar una base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada; y un receptor dispuesto para recibir un primer mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso a los datos del usuario, el primer mensaje de acceso comprendiendo una etiqueta del sistema remoto indicativa de un identificador del sistema remoto; un módulo de comparación dispuesto para comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas, en respuesta a la recepción del primer mensaje de acceso, y hacer que un módulo de identificación identifique una coincidencia entre la etiqueta del sistema remoto y por lo menos una de la pluralidad de etiquetas de entidades autorizadas y, en respuesta, hacer que un transmisor transmita un mensaje de concesión indicativo de que se concede la solicitud de acceso; en donde el receptor está dispuesto para recibir un segundo mensaje de acceso, desde el sistema remoto, asociado con la solicitud de acceso a los datos del usuario, el segundo mensaje de acceso comprendiendo la etiqueta del sistema remoto; en donde el módulo de comparación está dispuesto para comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas, en respuesta a la recepción del segundo mensaje de acceso; y hacer que el módulo de identificación identifique una coincidencia entre la etiqueta del sistema remoto y por lo menos una de la pluralidad de etiquetas de entidades autorizadas y, en respuesta, hacer que el transmisor transmita un mensaje de concesión indicativo de que se concede la solicitud de acceso.

En otro aspecto de la invención, hay un programa informático que comprende instrucciones que, cuando el programa es ejecutado por un ordenador, hacen que el ordenador lleve a cabo el método descrito en la presente.

En otro aspecto de la invención, hay una señal portadora de datos que lleva el programa informático descrito en la presente.

En otro aspecto de la invención, hay un medio legible por ordenador que, cuando el programa es ejecutado por un ordenador, hace que el ordenador lleve a cabo el método descrito en la presente.

Breve descripción de los dibujos

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

La Fig. 1 ilustra la arquitectura general de un sistema para autorizar el acceso a datos de usuario seguros;

La Fig. 2 ilustra un diagrama de secuencia de protocolo de un método implementado por ordenador para autorizar el acceso a datos de usuario seguros;

La Fig. 3 ilustra un diagrama de flujo de un método implementado por ordenador realizado por el sistema para autorizar el acceso a datos de usuario seguros;

La Fig. 4 ilustra un diagrama de secuencia de protocolo del método implementado por ordenador para autorizar el acceso a datos de usuario seguros;

La Fig. 5 ilustra un diagrama esquemático de un sistema de gestión de datos; y

La Fig. 6 ilustra un diagrama esquemático de un dispositivo de ejemplo en el sistema.

Descripción detallada

En referencia a la Fig. 1, hay un sistema 100 para gestionar el acceso a los datos asociados con un primer usuario. El sistema comprende un sistema de gestión de datos (DMS) 102, un primer dispositivo de usuario 104, un sistema de autorización 105 y un sistema remoto 108.

El DMS 102 está dispuesto para almacenar datos relacionados con los usuarios del sistema 100. Específicamente, el DMS 102 almacena datos que están asociados con el primer usuario, y los datos pueden comprender uno o más elementos de datos seguros. Cada uno de estos elementos de datos es indicativo de información privada relacionada con un usuario del DMS 102 (por ejemplo, el primer usuario). En un ejemplo, cada elemento de datos comprende datos financieros relacionados con el primer usuario, como detalles que permiten al primer usuario realizar pagos o los detalles de transacciones financieras anteriores realizadas por el primer usuario.

Los siguientes sistemas y métodos se describen en el contexto de la gestión del acceso a datos financieros y pagos. Sin embargo, estos sistemas y métodos podrían usarse para gestionar el acceso a cualquier tipo de datos seguros para los que se restringirá el acceso de terceros no autorizados.

En los siguientes ejemplos, se hace referencia a los datos como accesibles por el primer usuario y a que los datos están asociados con el primer usuario. Por ejemplo, el primer usuario puede tener acceso a una cuenta de usuario en línea, como una cuenta bancaria en línea, a través de una interfaz de cuenta. En este escenario, al primer usuario se le puede asignar un nombre de usuario único y un secreto compartido (por ejemplo, información de inicio de sesión), como una contraseña, que puede usarse para acceder a la cuenta de usuario a través de la interfaz de la cuenta. Una vez que el primer 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 primer usuario puede acceder a los datos a través de la información de inicio de sesión que es exclusiva del primer usuario.

Los datos seguros a los que puede acceder el primer usuario pueden ser accesibles por el propio DMS 102. Solo el primer usuario puede acceder a los datos seguros, a menos que el primer usuario autorice lo contrario. En otras palabras, se evita que los datos seguros se envíen a un dispositivo o sistema que es remoto y distinto del DMS 102, como el sistema remoto 108, sin que el primer usuario proporcione autorización al DMS 102 para que los datos sean enviado a un dispositivo o sistema remoto.

El sistema 100 comprende un primer dispositivo de usuario 104 que es operado por el primer usuario. El sistema 100 también comprende un sistema remoto 108 al que pueden enviarse los datos accesibles conjuntamente.

Cada uno del DMS 102, el sistema remoto 108, el sistema de autorización 105 y el primer dispositivo de usuario 104 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 de red de comunicaciones 110 adecuada.

Cada uno del DMS 102, el sistema remoto 108, el primer dispositivo de usuario 104 y el sistema de autorización 105 están habilitados para web y pueden comprender una pantalla, una interfaz de usuario, un procesador y una memoria. Los dispositivos y sistemas 102, 104, 105, 108 pueden disponerse para comunicar datos entre sí a través de cualquier protocolo o conexión de comunicaciones adecuados. Por ejemplo, los dispositivos y sistemas 102, 104, 105, 108 pueden comunicarse entre sí a través de una conexión por cable y/o inalámbrica.

El primer dispositivo de usuario 104 puede ser cualquier tipo adecuado de dispositivo informático personal, como un ordenador portátil, un ordenador de escritorio, un teléfono habilitado para la web, como un teléfono inteligente o una tableta. El DMS 102, el sistema de autorización 105 y el sistema remoto 108 pueden ser cualquier tipo adecuado de sistema informático o grupo de sistemas informáticos, como un servidor o un grupo de servidores.

En referencia a la Fig. 2, es un método para que el primer usuario permita que el sistema remoto 108 acceda a los datos seguros almacenados en el DMS 102 usando el primer dispositivo de usuario 104.

En el paso 1, el DMS 102 transmite una solicitud al sistema de autorización 105 para acceder a una base de datos de entidades autorizadas. La base de datos de entidades autorizadas está almacenada en el sistema de autorización 105 y comprende una lista de entidades que se consideran autorizadas para acceder a los datos del usuario. Se considera que las entidades autorizadas no son entidades fraudulentas, inescrupulosas o maliciosas. En otras palabras, las entidades en la lista de entidades autorizadas se consideran "seguras" en el sentido de que se ha considerado que estas entidades no imponen un riesgo para la seguridad de un usuario, o por lo menos se ha considerado que imponen un riesgo bajo para la seguridad de un usuario. Por ejemplo, cada entidad puede estar asociada con una puntuación de seguridad y si la puntuación de seguridad para una entidad particular cumple con un umbral seguro predeterminado, los detalles de identificación para esa entidad se almacenarán en la lista de entidades autorizadas. Sin embargo, si la puntuación de seguridad para una entidad no alcanza el umbral de seguridad predeterminado, los detalles de identificación de esa entidad no se almacenarán en la lista de entidades autorizadas.

La base de datos de entidades autorizadas comprende una pluralidad de etiquetas, cada una de las cuales es indicativa de un identificador para una entidad autorizada. Por lo tanto, es posible determinar si una entidad está autorizada comparando su identificador con los identificadores de las entidades autorizadas en la base de datos de entidades autorizadas.

En el paso 2, el sistema de autorización 105 transmite por lo menos una parte de la base de datos de entidades autorizadas al DMS 102. El sistema de autorización 105 puede transmitir la totalidad de la base de datos de la entidad autorizada al DMS 102, de tal manera que el DMS 102 pueda acceder a una copia completa de la base de datos de entidades autorizadas. Sin embargo, una parte de la base de datos de entidades autorizadas puede transmitirse al DMS 102 para conservar el uso del ancho de banda y los recursos de almacenamiento en el DMS 102. Por ejemplo, el DMS 102 puede requerir solo una parte de la base de datos de entidades autorizadas. En este ejemplo, el DMS 102 solicita una parte de la base de datos y el sistema de autorización 105 responde con la parte de la base de datos que se solicitó. Una vez que se ha recibido la base de datos de entidades autorizadas (o una parte de la misma), el DMS 102 almacena la base de datos localmente en un recurso de almacenamiento de datos en el DMS 102.

De esta manera, el DMS 102 es capaz de verificar una copia local de la base de datos de entidades autorizadas en lugar de consultar el sistema de autorización 105. El sistema de autorización 105 es remoto y distinto del DMS 102. Por tanto, verificar el sistema de autorización 105 en cada caso donde se requiera impondría una carga sobre los recursos de procesamiento del DMS 102. Además, el sistema de autorización 105 puede dar servicio a otros sistemas similares que requieren acceso a la base de datos de entidades autorizadas, y en esta situación el sistema de autorización 105 puede crear el denominado "cuello de botella" o punto único de fallo para el sistema. Como el DMS 102 obtiene una copia local de la base de datos de entidades autorizadas, el DMS 102 puede detectar entidades autorizadas de forma más fiable y rápida. Esto mejorará la capacidad del DMS 102 para asegurar la seguridad de los datos del usuario.

Los pasos 1 y 2 pueden repetirse, de tal manera que la copia local de la base de datos de entidades autorizadas se mantenga actualizada en el DMS 102. Esto es ventajoso para que el DMS 102 sea capaz de determinar qué entidades están autorizadas y cuáles no. Por ejemplo, en un momento dado, una entidad en particular puede considerarse autorizada (o ser "segura"). Sin embargo, esta entidad puede estar sujeta a una violación de seguridad, y la base de datos de entidades autorizadas puede actualizarse en el sistema de autorización 105 para eliminar esa entidad de la base de datos. Si la copia local del DMS 102 no está actualizada y la entidad que ya no está autorizada intenta acceder a los datos del usuario desde el DMS 102, entonces el DMS 102 podría transmitir los datos a la entidad, lo que pondría en riesgo la seguridad de la información de los usuarios. Para ayudar a aliviar este problema, el DMS 102 puede transmitir una pluralidad de solicitudes para la base de datos de entidades autorizadas en base a un patrón o secuencia de tiempo predeterminados. Por ejemplo, el DMS 102 puede almacenar un intervalo de tiempo predefinido que determina el intervalo de tiempo entre transmisiones posteriores de la solicitud. Este intervalo de tiempo puede ser configurable, de tal manera que un operador del DMS 102 pueda establecer la secuencia o patrón de tiempo. Por ejemplo, el operador puede aumentar o disminuir el intervalo de tiempo en base a las condiciones del sistema, o el DMS 102 puede actualizar el intervalo de tiempo automáticamente.

El DMS 102 puede usarse para detectar y contar incidentes de fraude. El intervalo de tiempo puede aumentarse o disminuirse en base a una serie de incidentes de fraude detectados. El intervalo de tiempo puede aumentar si aumenta el número de incidentes de fraude detectados. El intervalo de tiempo puede disminuir si disminuye el número de incidentes de fraude detectados.

Si el sistema de autorización 105 no proporciona una respuesta al mensaje enviado en el paso 1, o si el sistema de autorización 105 no proporciona por lo menos una parte de la base de datos de entidades autorizadas en respuesta al mensaje enviado en el paso 1, el DMS 102 no ejecuta los pasos para permitir que se envíen datos de usuario al sistema remoto 108. Por ejemplo, en este escenario, el DMS 102 puede evitar que se ejecuten uno o más de los pasos 6, 6a, 8, 9 11a y 12.

Además de almacenar la base de datos de entidades autorizadas, el DMS 102 puede almacenar una base de datos de entidades no autorizadas. La base de datos de entidades no autorizadas comprende una lista de entidades que se consideran no autorizadas para acceder a los datos del usuario. Las entidades no autorizadas se consideran entidades fraudulentas, inescrupulosas o maliciosas. En otras palabras, las entidades de la lista de entidades no autorizadas se consideran "inseguras" en el sentido de que se ha considerado que estas entidades imponen un riesgo a la seguridad de un usuario o que imponen un alto riesgo a la seguridad de un usuario. Por ejemplo, cada entidad puede estar asociada con una puntuación de seguridad y si la puntuación de seguridad para una entidad particular alcanza un umbral no seguro predeterminado, esa entidad se almacenará en la lista de entidades no autorizadas. Sin embargo, si la puntuación de seguridad para una entidad no cumple el umbral no seguro predeterminado, la entidad no se almacenará en la lista de entidades no autorizadas.

La base de datos de entidades no autorizadas comprende una pluralidad de etiquetas, cada una de las cuales es indicativa de un identificador de una entidad no autorizada. Por lo tanto, es posible determinar si una entidad no está autorizada comparando el identificador de la entidad con los identificadores de las entidades no autorizadas en la base de datos de entidades no autorizadas.

En el paso 3, el DMS 102 recibe un mensaje de detección de entidad no autorizada. Este mensaje puede recibirse desde el sistema de autorización 108, como se muestra en la Fig. 2. Sin embargo, el mensaje puede ser recibido por un sistema diferente que sea distinto y remoto del DMS 102, o el mensaje puede ser generado por el DMS 102.

El mensaje de detección de entidad no autorizada comprende una etiqueta que indica un identificador de una entidad que no está autorizada para recibir datos de usuario. La etiqueta puede indicar la identidad de una entidad que se sospecha que es fraudulenta, inescrupulosa o maliciosa. En otras palabras, la entidad identificada en el mensaje de detección de entidad no autorizada se ha considerado "insegura" en el sentido de que se ha considerado que la entidad impone un riesgo a la seguridad de un usuario, o se ha considerado que impone un alto riesgo a la seguridad de un usuario. Por ejemplo, la entidad identificada en el mensaje de detección de entidad no

autorizada puede estar asociada con una puntuación de seguridad que cumple con el umbral no seguro predeterminado. Esta determinación puede realizarse en el DMS 102 o en un sistema remoto, como el sistema de autorización 105. Esta determinación puede realizarse automáticamente en base a los datos de seguridad asociados con la entidad indicada en el mensaje. La determinación puede realizarse manualmente en base a entradas del usuario.

En el paso 4, una vez que se ha recibido el mensaje de detección de entidad no autorizada, el DMS 102 actualiza la base de datos de entidades no autorizadas para incluir la etiqueta del mensaje de detección de entidad no autorizada. De esta manera, es posible que el DMS 102 actualice la base de datos de entidades no autorizadas de forma ad-hoc para entidades específicas. Por lo tanto, la base de datos de entidades no autorizadas puede mantenerse de una manera más eficiente y fiable.

En el paso 5, el primer usuario envía un mensaje a través del primer dispositivo de usuario 104 que es indicativo de que el primer usuario proporciona su consentimiento para que el sistema remoto 108 acceda a los datos seguros accesibles por el primer usuario que están almacenados en el DMS 102. El mensaje que proporciona el consentimiento del primer usuario para acceder a los datos seguros se envía desde el primer dispositivo de usuario 104 al sistema remoto 108. El mensaje en el paso 5 puede ser indicativo de que el primer usuario da su consentimiento para que se realice un pago desde una cuenta bancaria a la que tiene acceso el primer usuario.

En el paso 6, el sistema remoto 108 se conecta al DMS 102. En este paso, el sistema remoto 108 crea un recurso de solicitud de cuenta. Esto informa al DMS 102 que uno de sus usuarios está otorgando al sistema remoto 108 acceso a los datos asociados con la cuenta en línea de ese usuario. En este paso, el DMS 102 responde con un identificador para el recurso. Este paso lo lleva a cabo el sistema remoto 108 que realiza una solicitud POST, que está respaldada por el Protocolo de transferencia de hipertexto, a un punto final en el DMS 102. Si el mensaje en el paso 5 es indicativo de que el primer usuario está dando su consentimiento para un pago, en el paso 5 se crea un recurso de pago con un identificador correspondiente para el recurso de pago.

En el paso 6, se envía una carga útil de configuración de solicitud de cuenta desde el sistema remoto 108 al DMS 102, que comprende campos que describen los datos a los que el primer usuario ha dado su consentimiento para que acceda el sistema remoto 108. Los campos de la carga útil de configuración pueden comprender un campo de permisos, un campo de fecha de vencimiento y un campo de período. El campo de permisos comprende un identificador para un grupo de datos o una lista de identificadores para grupos de datos a los que el primer usuario ha dado su consentimiento para que acceda el sistema remoto 108. El campo de fecha de vencimiento comprende un tiempo de vencimiento opcional en cuyo punto se impedirá que el sistema remoto 108 acceda a los datos del primer usuario almacenados en el DMS 102. El campo de período comprende un intervalo de fecha/hora que puede usarse para proporcionar acceso únicamente a elementos de datos almacenados en el DMS 102 que están asociados con fechas/horas que están dentro del intervalo de fecha/hora. Por ejemplo, el campo de período puede especificar un período de historial de transacciones. El DMS 102 usa el período del historial de transacciones para determinar que el sistema remoto 108 solo debe tener acceso a las transacciones que se realizaron dentro del período del historial de transacciones. El sistema remoto 108 puede enviar múltiples solicitudes de cuenta para el mismo usuario, con diferentes cargas útiles de configuración en cada solicitud.

En el paso 6, el sistema remoto 108 transmite una etiqueta/identificador que indica la identidad del sistema remoto 108. Luego, en el paso 6a el DMS 102 compara la identidad del sistema remoto 108 con las identidades de las entidades almacenadas en la base de datos de entidades autorizadas. Si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 indica que se concede la solicitud de configuración de cuenta. Por ejemplo, si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 transmite el identificador del recurso al sistema remoto 108.

Alternativamente, si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 evita que se conceda la solicitud de configuración de cuenta. Por ejemplo, si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 no transmite el identificador del recurso al sistema remoto 108. El DMS 102 puede transmitir un fallo o solicitar un mensaje de rechazo al sistema remoto 108, si el sistema remoto no está en la base de datos de entidades autorizadas.

En el paso 6a, el DMS 102 también puede comparar la identidad del sistema remoto 108 con las identidades de las entidades almacenadas en la base de datos de entidades no autorizadas. Esto puede producirse localmente en el DMS 102 usando la copia local de la base de datos autorizada, o el DMS 102 puede interactuar con el sistema de autorización 105 para la comparación. El DMS 102 puede ejecutar la comparación en base a tanto la base de datos de entidades autorizadas local como la base de datos de entidades autorizadas almacenada en el sistema de autorización. Si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base de datos de entidades no autorizadas, el DMS 102 indica que se concede la solicitud de configuración de cuenta. Por ejemplo, si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base

de datos de entidades no autorizadas, el DMS 102 transmite el identificador para el recurso al sistema remoto 108.

Alternativamente, si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades no autorizadas, el DMS 102 evita que se conceda la solicitud de configuración de cuenta. Por ejemplo, si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades no autorizadas, el DMS 102 no transmite el identificador para el recurso al sistema remoto 108. El DMS 102 puede transmitir un mensaje de fallo o de rechazo de solicitud al sistema remoto 108, si el sistema remoto está listado en la base de datos de entidades no autorizadas.

En el paso 7, si se ha completado la solicitud de cuenta, el sistema remoto transmite un mensaje de redireccionamiento al primer dispositivo de usuario 104 que indica al dispositivo 104 que sea redirigido al DMS 102. El mensaje de redireccionamiento incluye un identificador de solicitud de cuenta asociado con la solicitud de cuenta establecida en el paso 6. El identificador de solicitud de cuenta permite al DMS 102 correlacionar los mensajes transmitidos desde el primer dispositivo de usuario 104 con la solicitud de cuenta que se configuró en el paso 6.

En el paso 7, el primer dispositivo de usuario 104 se redirige al DMS 102. Por ejemplo, el primer usuario es redirigido a una página web o una aplicación a través de la cual el primer usuario puede acceder a su cuenta en línea. Cuando el primer dispositivo de usuario 104 se redirige al DMS 102, el primer dispositivo de usuario 104 proporciona el identificador de solicitud de cuenta al DMS 102. Esto permite que el DMS 102 correlacione los mensajes del primer dispositivo de usuario 104 con la solicitud de cuenta del paso 6.

En el paso 8, el DMS 102 autentica al primer usuario a través del primer dispositivo de usuario 104. Esto puede producirse cuando el primer usuario introduce su información de inicio de sesión en la página web o la aplicación usando el primer dispositivo de usuario 104. Una vez que el usuario ha sido autenticado el usuario puede dar su consentimiento para que el sistema remoto 108 acceda a sus datos o autorice la solicitud de pago. Luego, el DMS 102 actualiza el estado del recurso de solicitud de cuenta para indicar que la solicitud de cuenta ha sido autorizada por el primer usuario. Esto puede implicar establecer una bandera asociada con el primer usuario para indicar que los datos están autorizados para ser compartidos con el sistema remoto 108, donde previamente se estableció la bandera para indicar que los datos no están autorizados para ser compartidos con el sistema remoto 108.

La cuenta de usuario en línea puede comprender una pluralidad de subcuentas. Por ejemplo, la cuenta bancaria en línea del usuario puede comprender diferentes subcuentas, como una cuenta corriente y una cuenta de ahorro. Durante la autorización, el primer usuario selecciona las cuentas a las que se ha autorizado que acceda el sistema remoto 108. Esta selección puede ser ejecutada por el primer usuario a través de una interfaz de usuario en el primer dispositivo 104 de usuario.

En el método, el consentimiento para que los datos se compartan se gestiona en el paso 5 entre el primer usuario y el sistema remoto 108. Por tanto, el primer usuario no puede cambiar los detalles de la solicitud de cuenta interactuando con el DMS 102 en el paso 8. El primer usuario solo podrá autorizar o rechazar los detalles de la solicitud de cuenta en su totalidad en el paso 8. Para que el primer usuario cambie los detalles de la solicitud de cuenta, es necesario que el paso 5 se repita con diferentes parámetros de consentimiento proporcionados por el primer usuario.

En los pasos 9 y 10, el primer dispositivo 104 de usuario se redirige de nuevo al sistema remoto 108.

En el paso 11, el sistema remoto 108 transmite una solicitud de acceso al elemento de datos seguro. Esto se lleva a cabo realizando una solicitud GET, que está respaldada por el Protocolo de transferencia de hipertexto, al recurso relevante en el DMS 102. Si se proporcionó el consentimiento de pago en el paso 5, el sistema remoto transmite una solicitud para que se realice el pago. Esto se lleva a cabo realizando una solicitud POST, que está respaldada por el Protocolo de transferencia de hipertexto, al recurso relevante en el DMS 102. La solicitud en el paso 11 comprende un identificador para el sistema remoto 108 que el DMS 102 puede usar para comparar con la base de datos de entidades autorizadas y la base de datos de entidades no autorizadas para determinar si el sistema remoto 108 está autorizado para acceder a los datos seguros.

En el paso 11a, el DMS 102 compara la identidad del sistema remoto 108 con las identidades de las entidades almacenadas en la base de datos de entidades autorizadas. Esto puede producirse localmente en el DMS 102 usando la copia local de la base de datos autorizada, o el DMS 102 puede interactuar con el sistema de autorización 105 para la comparación. El DMS 102 puede ejecutar la comparación en base a tanto la base de datos de entidades autorizadas local como la base de datos de entidades autorizadas almacenada en el sistema de autorización. Si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 indica que se concede la solicitud del paso 11. Por ejemplo, si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 pasa al paso 12.

Alternativamente, si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base de datos de entidades autorizadas, el DMS 102 evita que se conceda la solicitud del paso 11. El DMS 102 puede transmitir un mensaje de fallo o solicitud de rechazo al sistema remoto 108, si el sistema remoto no está listado en la base de datos de entidades autorizadas.

En el paso 11a, el DMS 102 también puede comparar la identidad del sistema remoto 108 con las identidades de las entidades almacenadas en la base de datos de entidades no autorizadas. Si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base de datos de entidades no autorizadas, el DMS 102 indica que se concede la solicitud del paso 11. Por ejemplo, si la identidad del sistema remoto 108 no coincide con la identidad de una entidad en la base de datos de entidades no autorizadas, el DMS 102 procede al paso 12.

Alternativamente, si la identidad del sistema remoto 108 coincide con la identidad de una entidad en la base de datos de entidades no autorizadas, el DMS 102 evita que se conceda la solicitud del paso 11. El DMS 102 puede transmitir un mensaje de fallo o solicitud de rechazo al sistema remoto 108, si el sistema remoto está listado en la base de datos de entidades no autorizadas.

En el paso 12, si el primer usuario ha dado su consentimiento y el sistema remoto 108 está listado en la base de datos de entidades autorizadas pero no en la base de datos de entidades no autorizadas, el elemento de datos seguro al que puede acceder el primer usuario se transmite desde el DMS 102 al sistema remoto 108, o si se solicitó un pago, se realiza el pago.

El ejemplo anterior se ha descrito en el contexto de proporcionar y otorgar consentimiento para que se transfieran los datos del primer usuario. Sin embargo, el método anterior podría implementarse como un mecanismo para proporcionar y otorgar consentimiento para que el primer usuario realice un pago a través del sistema remoto 108 desde la cuenta bancaria del primer usuario.

La Fig. 3 muestra un diagrama de flujo que ilustra, a nivel general, un método para compartir el elemento de datos seguro accesible por el primer usuario con el sistema remoto 108.

En el paso 20, los datos seguros que están asociados con el primer usuario se almacenan en un recurso de almacenamiento de datos en el DMS 102. El primer usuario puede tener acceso a los datos seguros a través de una cuenta de usuario en línea, como una cuenta bancaria en línea, a través de un interfaz de cuenta como se ha analizado anteriormente. Los datos seguros pueden comprender datos financieros indicativos de transacciones ejecutadas previamente vinculadas con una cuenta perteneciente al primer usuario, o datos de pago que permiten iniciar un pago desde una cuenta perteneciente al primer usuario.

En el paso 21, se almacena una base de datos de entidades autorizadas en el recurso de almacenamiento de datos en el DMS 102. La base de datos de entidades autorizadas comprende una pluralidad de etiquetas de entidades autorizadas, cada una indicativa de un identificador de una entidad autorizada.

Opcionalmente, en los pasos 21a y 21b, el DMS 102 solicita y almacena una copia local de la base de datos de entidades autorizadas. En el paso 21a, el DMS 102 transmite una solicitud al sistema de autorización 108 para acceder a la base de datos de entidades autorizadas almacenada en el sistema de autorización 108.

El DMS 102 puede transmitir una pluralidad de solicitudes del paso 21a en una secuencia predefinida. La secuencia temporal predefinida puede configurarse en el DMS 102. Por ejemplo, cada una de las solicitudes puede transmitirse secuencialmente con un intervalo temporal predeterminado entre cada solicitud sucesiva.

En el paso 21b, en respuesta a cada solicitud transmitida en el paso 21a, el DMS 102 recibe y almacena por lo menos una parte de la base de datos de entidades autorizadas.

En el paso 22, se almacena una base de datos de entidades no autorizadas en el DMS 102. La base de datos de entidades no autorizadas comprende una pluralidad de etiquetas de entidades no autorizadas, cada una indicativa de un identificador de una entidad no autorizada;

Opcionalmente, en el paso 22a, el DMS 102 recibe un mensaje de detección de entidad no autorizada. El mensaje puede recibirse mediante una entrada en el DMS 102. El mensaje de detección no autorizado comprende una etiqueta indicativa de un identificador de una entidad sospechosa de actividad fraudulenta y/o sospechosa de haber sido sometida a una violación de seguridad. En el paso 22b, los datos de la entidad no autorizada se actualizan almacenando la etiqueta del mensaje de detección de entidad no autorizada como una etiqueta de entidad no autorizada indicativa de un identificador de una entidad no autorizada. Esta etiqueta se almacena en la base de datos de entidades no autorizadas.

En el paso 23, el DMS 102 recibe un primer mensaje de acceso, desde el sistema remoto 108, asociado

con una solicitud de acceso a los datos de usuario almacenados en el primer sistema. El primer mensaje de acceso comprende una etiqueta indicativa de un identificador del sistema remoto 108.

En el paso 24, en respuesta a la recepción del primer mensaje de acceso, el DMS 102 compara la etiqueta del sistema remoto 108 con la pluralidad de etiquetas de entidades autorizadas en la base de datos de entidades autorizadas.

En el paso 25, si la etiqueta para el sistema remoto 108 no está almacenada en la base de datos de entidades autorizadas, el método pasa al paso 29 en el que el DMS 102 no realiza la acción solicitada en el paso 23. Por otro lado, si la etiqueta para el sistema remoto 108 está almacenada en la base de datos de entidades autorizadas, el método pasa al paso 30 en el que el DMS 102 realiza la acción solicitada en el paso 23.

Opcionalmente, el DMS 102 puede requerir que la etiqueta del sistema remoto 108 se compare con la base de datos de entidades no autorizadas. En este caso, el método pasa al paso 26.

En el paso 26, el DMS 102 compara la etiqueta del sistema remoto 108 con la pluralidad de etiquetas de entidades no autorizadas en la base de datos de entidades no autorizadas.

En el paso 27, si la etiqueta para el sistema remoto está almacenada en una base de datos de entidades no autorizadas, el método pasa al paso 29 en el que el DMS 102 no realiza la acción solicitada en el paso 23. Por otro lado, si la etiqueta para el sistema remoto 108 no está almacenada en la base de datos de entidades no autorizadas, el método pasa al paso 30 en el que el DMS 102 realiza la acción solicitada en el paso 23.

Opcionalmente, el DMS 102 puede recibir un segundo mensaje de acceso antes de conceder la acción como en el paso 30. En el caso, se repiten los pasos 24, 25, 26, 27, 29 y 30. Sin embargo, la etiqueta recibida en la segunda solicitud se usa para la comparación con las bases de datos de entidades autorizadas y no autorizadas en este caso.

La Fig. 4 muestra un diagrama de secuencia de protocolo que ilustra el método descrito con referencia a la Fig. 2 con mayor detalle. En referencia a la Fig. 4, el DMS 102 descrito anteriormente comprende además una identidad de confianza y una autoridad de atributos 102a (TIAA) y un proveedor de identidad 102b (IDP).

En los pasos 40, 40a y 41, el sistema remoto 108 y el DMS 102 interactúan para que se transmita un token de intención al sistema remoto 108. Específicamente, en el paso 40 el sistema remoto 108 transmite una solicitud de un token de acceso al TIAA 102a en el DMS 102. El token de acceso que se solicita es un token web que está configurado para permitir que el sistema remoto 108 envíe una interfaz de programación de aplicaciones (API) de intención al DMS 102.

El token de acceso solicitado por el sistema remoto 108 será válido durante un período de tiempo predeterminado. Por tanto, el token de acceso puede ser usado más de una vez por el sistema remoto 108. En este ejemplo, el token web es un token web de notación de objetos JavaScript (JSON).

En el paso 40, la solicitud del token de acceso se transmite directamente al TIAA 102a, y la solicitud comprende un identificador de cliente y un secreto de cliente. El identificador de cliente y el secreto de cliente se asignan con anterioridad al sistema remoto 108, cuando el sistema remoto 108 se registra con el DMS 102. El TIAA 102a valida el identificador de cliente y el secreto de cliente para autenticar el sistema remoto 108.

En el paso 40a, el DMS 102 compara la identidad del sistema remoto 108 con las identidades almacenadas en la base de datos de entidades autorizadas y/o las identidades almacenadas en la base de datos de entidades no autorizadas. El DMS 102 puede ejecutar esta comparación interactuando con el sistema de autorización o haciendo referencia a las copias locales de la base de datos de entidades autorizadas y/o la base de datos de entidades no autorizadas. El paso 40a puede producirse de una manera similar a la descrita con referencia al paso 6a anterior y/o de una manera similar a la descrita con referencia a los pasos 24, 25, 26, 27, 29 y 30 anteriores. En el paso 40a, si se determina que el sistema remoto 108 es una entidad autorizada y/o no es una entidad no autorizada, el método pasa al paso 41.

En el paso 41, el TIAA 102a genera un token de acceso de intención y transmite el token de acceso de intención al sistema remoto 108.

En el paso 42, el primer usuario transmite un mensaje al sistema remoto 108 que indica que el primer usuario ha solicitado que el DMS 102 transmita un elemento de datos seguro al sistema remoto 108. En este ejemplo, los datos seguros son un elemento de datos al que puede acceder el primer usuario a través de una interfaz de cuenta de una cuenta de almacenamiento de datos en línea compartida. El mensaje puede indicar una instrucción para que se realice un pago usando una cuenta bancaria accesible por el primer usuario en el DMS 102.

En el paso 43, el sistema remoto 108 transmite una API de intento de consentimiento externo, y el sistema remoto 108 transmite el token de acceso de intento proporcionado previamente en respuesta a la solicitud del primer usuario en el paso 42. El sistema remoto 108 también envía los detalles del solicitud de consentimiento del usuario, como el tipo de cuenta, período de tiempo, permisos, como se describe con referencia a la carga útil de configuración de solicitud de cuenta en el paso 2 de la Fig. 2. Si el mensaje del paso 42 indica una instrucción de pago, el sistema remoto 108 transmite un identificador de transacción al DMS 102. En el paso 43, el TIAA 102a recibe la API de intención de consentimiento externo y valida el token de acceso de intención correspondiente.

En el paso 43a, se autentica la identidad del sistema remoto 108 para determinar si el sistema remoto 108 es una entidad autorizada y/o una entidad no autorizada. Si el sistema remoto no es una entidad autorizada o el token de acceso de intención no es válido, se rechazará la API de intención de consentimiento externo y se devolverá un código de error al sistema remoto 108. Si el sistema remoto es una entidad no autorizada o el token de acceso de intención no es válido, la API de intención de consentimiento externo será rechazada y se devuelve un código de error al sistema remoto 108. El paso 43a se produce de manera similar al paso 40a.

Además, en el paso 43, el DMS 102 usa una API de intención de consentimiento interno, que genera un identificador de consentimiento único que se corresponde con la solicitud recibida del sistema remoto 108 y sigue siendo válida durante todo el ciclo de vida de la solicitud. La API de consentimiento interno almacena los detalles de la intención en una base de datos de consentimiento junto con el identificador de consentimiento. Luego, en el paso 44, el DMS 102 devuelve el identificador de consentimiento al sistema remoto 108.

En el paso 45, una vez que el sistema remoto 108 ha recibido el identificador de consentimiento de la API de intención de consentimiento, el sistema remoto 108 recupera una URL de redireccionamiento de un registro que apunta al TIAA 102a. En este paso, el sistema remoto 108 redirige el primer dispositivo de usuario 104 al TIAA 102a con el identificador de cliente, el identificador de consentimiento y los detalles de la solicitud de consentimiento del usuario. Esta información se envía mediante OAuth 2.0.

En el paso 46, el primer dispositivo de usuario 104 se redirige al TIAA 102a, que valida el identificador del cliente y los detalles de la solicitud de consentimiento del usuario. En el paso 46a, la identidad del sistema remoto 108 se autentica de nuevo como en los pasos 40a y 43a.

En el paso 47, el TIAA 102a transmite un identificador uniforme de recursos (URI) de redireccionamiento al primer dispositivo de usuario 104 y un primer código de referencia. Esto redirige el primer dispositivo de usuario 104 al IDP 102b junto con el primer código de referencia. A su vez, el IDP 102b transmite una solicitud al TIAA102a para el identificador de consentimiento y los detalles de la solicitud de consentimiento del usuario. Entonces, es necesario que el IDP 102b obtenga un identificador de enlace. El IDP 102b llamará entonces a una API para obtener el identificador de enlace. Además, se requiere una llamada al TIAA 102b para traducir el identificador de cliente y el identificador del sistema remoto 108 en nombres textuales.

En el paso 48, se solicita al primer usuario que autentique su identidad. Por ejemplo, se pide al primer usuario que introduzca su información de inicio de sesión única a través de una interfaz de usuario. Luego, el primer usuario maneja la interfaz de usuario de la cuenta en línea para navegar a una página o área de consentimiento. En ese momento, se configura una API de autorización interna para obtener el consentimiento del primer usuario para que la solicitud coincida con los datos recibidos previamente a través de la API de intención de consentimiento para obtener el consentimiento total que se le pide al cliente que autorice. Esto se logra a través del identificador de enlace o mediante un enfoque de enlace profundo directo (solo para dispositivos móviles) usando el identificador de consentimiento directamente.

En el paso 48, el IDP 102b construye una lista de cuentas que puede seleccionar el primer usuario. Esto se construirá generando una lista de todas las cuentas a las que el primer usuario tiene acceso a los datos, o las cuentas desde las que el usuario puede realizar un pago, o las cuentas que están habilitadas para compartir datos. Por ejemplo, ciertos tipos de cuentas pueden habilitarse o deshabilitarse para compartir datos. Los tipos de cuenta habilitados aparecerán en la lista, mientras que los tipos de cuenta deshabilitados no aparecerán en la lista. En este paso, al primer usuario se le presenta el consentimiento que han solicitado y la lista de cuentas para que elija el primer usuario. Luego, el cliente autoriza el consentimiento, y como el usuario ha sido autenticado, se conocerá un identificador del primer usuario. La autorización recibida del usuario se firmará digitalmente dentro de la IDP 102b y se almacenará en asociación con el consentimiento autorizado.

En el paso 50, el primer dispositivo de usuario se redirige de nuevo al TIAA 102a.

En el paso 51, el TIAA 102a envía un código de autorización y un URI al primer dispositivo de usuario. El URI se asigna al sistema remoto 108 cuando el sistema remoto 108 se registra con el DMS 102 inicialmente y se usa para redirigir el primer dispositivo de usuario al sistema remoto 108.

En el paso 52, el primer dispositivo de usuario 10 se redirige al sistema remoto 108.

En el paso 53, el sistema remoto 108 envía el código de autorización al TIAA 102a que valida el código de autorización y la identidad del sistema remoto 108. En el paso 53a, se autentica de nuevo la identidad del sistema remoto 108 como en los pasos 40a, 43a y 46a.

En el paso 54, el TIAA 102a transmite un token de acceso y un token de actualización al sistema remoto 108. En solicitudes posteriores, el sistema remoto 108 transmitirá el token de actualización en lugar del código de autorización. Después de la validación, el TIAA 102a emitirá un nuevo token de acceso y un nuevo token de actualización.

En el paso 55, el sistema remoto 108 transmite una API de ejecución externa al DMS 102, que coincide con los detalles contenidos en el consentimiento autorizado. En este paso, el elemento de datos seguro que es accesible conjuntamente por el primer usuario y el segundo usuario se transmite al sistema remoto 108. En el paso 55a, la identidad del sistema remoto 108 se autentica de nuevo de una manera similar a la descrita anteriormente.

El identificador de consentimiento se pasa a una API de ejecución interna en el DMS 102, que llamará a una API de consentimiento autorizado de validación interna usando el identificador de consentimiento junto con cualquier dato adicional requerido de la API de ejecución para que coincida con el consentimiento autorizado (como el número de cuenta y detalles de pago).

La API de consentimiento autorizado de validación verificará que el identificador de consentimiento exista y no haya caducado. La API de consentimiento autorizado de validación también verificará que los detalles pasados coincidan con el consentimiento autorizado. Esto puede incluir verificar que la API que se está ejecutando dentro del alcance de la autorización del usuario que ha sido autorizada, que la cuenta que se solicita dentro de las cuentas ha sido autorizada.

La API de validación de consentimiento autorizado devolverá un mensaje de éxito o error a la API de ejecución de llamada. Para un mensaje de éxito, la API también devolverá la traducción del identificador de consentimiento del cliente al identificador de cliente real como se usa por el IDP 102b, el identificador de la cuenta de consentimiento al identificador de cuenta real y cualquier otro dato que se haya guardado en el momento de la autorización (por ejemplo, una puntuación biométrica para detectar fraude).

En referencia a la Fig. 5, el DMS 102 comprende una interfaz de comunicación 501 que comprende un receptor 502 y un transmisor 503. El DMS 102 también comprende un módulo de identificación 504, un módulo de comparación 505 y un recurso de almacenamiento de datos 506.

El receptor 502 y el transmisor 503 están configurados para recibir y transmitir los mensajes hacia y desde el DMS 102 como se ha explicado anteriormente. El módulo de comparación 507 está dispuesto para comparar una etiqueta con las etiquetas almacenadas en la base de datos de entidades autorizadas o la base de datos de entidades no autorizadas, como se ha explicado anteriormente. El módulo de identificación 504 está dispuesto para identificar si una etiqueta está almacenada en la base de datos de entidades autorizadas o en la base de datos de entidades no autorizadas, como se ha explicado anteriormente. El recurso de almacenamiento de datos 506 está dispuesto para almacenar los elementos de datos seguros en el DMS 102.

La Fig. 6 muestra un dispositivo electrónico 401 ejemplar de acuerdo con cualquiera de los dispositivos o sistemas electrónicos de esta divulgación (como el primer dispositivo de usuario 102, el sistema de autorización 105, el sistema remoto 108, el DMS 102, el TIAA 102a o el IDP 102b). El dispositivo electrónico 401 comprende circuitería de procesamiento 410 (como un microprocesador) y una memoria 412. El dispositivo electrónico 401 también puede comprender uno o más de los siguientes subsistemas: una fuente de alimentación 414, una pantalla 416, un transceptor 420 y una entrada 426.

La circuitería de procesamiento 410 puede controlar el funcionamiento del dispositivo electrónico 401 y los subsistemas conectados a los que la circuitería de procesamiento está acoplada comunicativamente. La memoria 412 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.

La pantalla 416 puede acoplarse comunicativamente con la circuitería de procesamiento 410, que puede configurarse para hacer que la pantalla 416 emita imágenes representativas de los datos seguros compartidos entre las entidades en el sistema 100.

La pantalla 416 puede comprender una interfaz sensible al tacto, como una pantalla táctil. La pantalla 416 puede usarse para interactuar con el software que se ejecuta en el procesador 410 del dispositivo electrónico 401. La interfaz sensible al tacto permite al usuario proporcionar entrada a la circuitería de procesamiento 410 mediante un toque, toques o uno o más gestos discretos para controlar el funcionamiento de la circuiterías de procesamiento y las funciones descritas en la presente. Se apreciará que pueden emplearse adicional o alternativamente otras

formas de interfaz de entrada para el mismo propósito, como la entrada 426 que puede comprender un teclado o un ratón en el dispositivo de entrada.

El transceptor 420 puede ser uno o más transceptores de RF de largo alcance que están configurados para operar de acuerdo con estándares de comunicación como LTE, UMTS, 3G, EDGE, GPRS, GSM y Wi-Fi. Por ejemplo, el dispositivo electrónico 401 puede comprender un primer transceptor inalámbrico 421, como un transceptor celular, que está configurado para comunicarse con una torre celular 403 a través de un protocolo de datos celulares como LTE, UMTS, 3G, EDGE, GPRS o GSM. y un segundo transceptor 428, como un transceptor Wi-Fi, que está configurado para comunicarse con un punto de acceso inalámbrico 404 a través de un estándar Wi-Fi como 802.11 ac/n/g/b/a. A este respecto y para los propósitos de todas las realizaciones de la presente relacionadas con un protocolo inalámbrico de largo alcance, un protocolo inalámbrico de largo alcance puede ser un protocolo que es capaz y está diseñado para comunicaciones sobre 5, 10, 20, 30, 40, 50 o 100 m. Esto contrasta con el protocolo inalámbrico de corto alcance mencionado anteriormente. El protocolo inalámbrico de largo alcance puede comunicarse utilizando mayor potencia que el protocolo inalámbrico de corto alcance. El intervalo (por ejemplo, distancia de 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 intervalo (por ejemplo, distancia de línea de visión) entre los nodos finales de corto alcance (por ejemplo, dispositivo electrónico y baliza inalámbrica).

El dispositivo electrónico 401 puede configurarse para comunicarse a través del transceptor 420 con una red 440. La red 440 puede ser una red de área amplia, como Internet, o una red de área local. El dispositivo electrónico 401 puede configurarse además para comunicarse a través del transceptor 420 y la red 440 con uno o más sistemas 14 o dispositivos de usuario 11, 12, 13. Estos servidores o dispositivos de usuario pueden ser cualquiera de los descritos en la presente.

El término "que comprende" abarca "que incluye" así como "que consiste", por ejemplo, una composición "que comprende" X puede consistir exclusivamente en X o puede incluir algo adicional, por ejemplo, X + Y.

A menos que se indique lo contrario, cada realización como se describe en la presente puede combinarse con otra realización como se describe en la presente.

Los métodos descritos en la presente pueden realizarse mediante software en forma legible por máquina en un medio de almacenamiento tangible, por ejemplo, en forma de un programa informático que comprende medios de código de programa de ordenador adaptados para realizar todos los pasos de cualquiera de los métodos descritos en la presente cuando el programa se ejecuta en un ordenador y donde el programa informático puede estar incorporado en un medio legible por ordenador. 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 en paralelo o en un procesador en serie, de tal manera que los pasos del método pueden llevarse a cabo en cualquier orden adecuado, o simultáneamente. Esto reconoce que el firmware y el software pueden ser productos valiosos negociables por separado. Se pretende que abarque software, que se ejecuta o controla en hardware "tonto" o estándar, para llevar a cabo las funciones deseadas. También se pretende que abarque software que "describe" o define la configuración de hardware, como software HDL (lenguaje de descripción de hardware) , como se usa para diseñar chips de silicio, o para configurar chips programables universales, para llevar a cabo las funciones deseadas.

Se apreciará que los módulos descritos en la presente pueden implementarse en hardware o en software. Además, los módulos pueden implementarse en varias localizaciones del sistema.

Los expertos en la técnica se darán cuenta de que los dispositivos de almacenamiento utilizados para almacenar instrucciones de programas pueden distribuirse a través de una red. Por ejemplo, un ordenador remoto puede almacenar un ejemplo del proceso descrito como software. Un ordenador local o terminal puede acceder al ordenador remoto y descargar una parte o todo el software para ejecutar el programa. Alternativamente, el ordenador local puede descargar partes del software según sea necesario, o ejecutar algunas instrucciones de software en el terminal local y algunas en el ordenador remoto (o red de ordenadores). Los expertos en la técnica también se darán cuenta de que mediante la utilización de técnicas convencionales conocidas por los expertos en la técnica, 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 similares.

Cualquier intervalo o valor de dispositivo dado en la presente puede ampliarse o alterarse sin perder el efecto buscado, como será evidente para el experto en la técnica.

Se entenderá que los beneficios y ventajas descritos anteriormente pueden estar relacionados con una realización o pueden estar relacionados con varias realizaciones. Las realizaciones no se limitan a aquellas que resuelven alguno o todos los problemas indicados o aquellas que tienen alguno o todos los beneficios y ventajas expuestos.

Cualquier referencia a "un" elemento se refiere a uno o más de esos elementos. El término "que comprende" se usa en la presente para que signifique que incluye los bloques o elementos del método identificados, pero que tales bloques o elementos no comprenden una lista exclusiva y que un método o aparato puede contener bloques o elementos adicionales.

Los pasos de los métodos descritos en la presente pueden llevarse a cabo en cualquier orden adecuado, o simultáneamente cuando sea apropiado. Además, los bloques individuales pueden eliminarse de cualquiera de los métodos sin apartarse del alcance de la materia descrita en la presente. Los aspectos de cualquiera de los ejemplos descritos anteriormente pueden combinarse con 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.

Se entenderá que la descripción anterior de una realización preferida se da a modo de ejemplo solamente y que los expertos en la técnica pueden realizar varias modificaciones. Aunque se han descrito anteriormente varias realizaciones con cierto grado de particularidad, o con referencia a una o más realizaciones individuales, los expertos en la técnica podrían realizar numerosas alteraciones a las realizaciones divulgadas sin apartarse del alcance de esta invención.

REIVINDICACIONES

1. Un método implementado por ordenador para compartir datos asociados con un primer usuario, el método comprendiendo:

almacenar, en un primer sistema, datos de usuario asociados con el primer usuario;
almacenar, en el primer sistema, una primera base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas cada una indicativa de un identificador de una entidad autorizada, en donde almacenar la primera base de datos de entidades autorizadas comprende:

transmitir, desde el primer sistema a un sistema de autorización, una pluralidad de solicitudes para acceder a una segunda base de datos de entidades autorizadas almacenada en el sistema de autorización; y
recibir y almacenar, en el primer sistema, por lo menos una parte de la segunda base de datos de entidades autorizadas en respuesta a cada una de la pluralidad de solicitudes de acceso a la base de datos de entidades autorizadas;
en donde la pluralidad de solicitudes para acceder a la segunda base de datos de entidades autorizadas se transmite en una secuencia temporal predefinida, en donde la secuencia temporal predefinida comprende un intervalo de tiempo predefinido entre cada solicitud adyacente de las solicitudes para acceder a la segunda base de datos de entidades autorizadas, y en donde la secuencia temporal predefinida es configurada por el primer sistema, en base a las condiciones del sistema

almacenar, en el primer sistema, una base de datos de entidades no autorizadas que comprende una pluralidad de etiquetas de entidades no autorizadas cada una indicativa de un identificador de una entidad no autorizada;
recibir un primer mensaje de acceso, desde un segundo sistema, asociado con una solicitud de acceso a los datos de usuario almacenados en el primer sistema, el primer mensaje de acceso comprendiendo una segunda etiqueta del sistema indicativa de un identificador del segundo sistema;
en respuesta a recibir el primer mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades autorizadas y la pluralidad de etiquetas de entidades no autorizadas almacenadas en el primer sistema;
en respuesta a identificar que la segunda etiqueta del sistema coincide con una etiqueta de entidad autorizada y que la segunda etiqueta del sistema no coincide con una etiqueta de entidad no autorizada, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso; y
evitar la transmisión del mensaje de concesión, si la segunda etiqueta del sistema en el primer mensaje de acceso coincide con una etiqueta de entidad no autorizada y/o no coincide con una etiqueta de entidad autorizada.

2. El método implementado por ordenador de la reivindicación 1, en el que almacenar la base de datos de entidades autorizadas en el primer sistema comprende:

transmitir, desde el primer sistema a un sistema de autorización, una solicitud para acceder a una base de datos de entidades autorizadas almacenada en el sistema de autorización;
recibir y almacenar, en el primer sistema, por lo menos una parte de la base de datos de entidades autorizadas en respuesta a la solicitud para acceder a la base de datos de entidades autorizadas.

3. El método implementado por ordenador de cualquiera de las reivindicaciones anteriores, en el que el primer mensaje de acceso comprende una solicitud de un token web de intención que valida una solicitud de acceso a los datos de usuario almacenados en el primer sistema.

4. El método implementado por ordenador de la reivindicación 1 o 2, en el que el primer mensaje de acceso comprende una solicitud de acceso a los datos de usuario almacenados en el primer sistema.

5. El método implementado por ordenador de la reivindicación 1 o 2, en el que el primer mensaje de acceso comprende una solicitud para redirigir un primer dispositivo de usuario al primer sistema para que el primer usuario proporcione autorización para que el segundo sistema acceda a los datos del usuario.

6. El método implementado por ordenador de cualquiera de las reivindicaciones anteriores que comprende además:

recibir un segundo mensaje de acceso, desde el segundo sistema, asociado con la solicitud de acceso a los datos de usuario almacenados en el primer sistema, el segundo mensaje de acceso comprendiendo la segunda etiqueta del sistema;
en respuesta a recibir el segundo mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema e identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades autorizadas

almacenadas en la primera sistema y, en respuesta, transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso.

7. El método implementado por ordenador de la reivindicación 6, en el que el segundo mensaje de acceso comprende una solicitud de un token web de ejecución que valida una solicitud para que el primer sistema transmita los datos de usuario al segundo sistema.

8. El método implementado por ordenador de la reivindicación 6, en el que el segundo mensaje de acceso comprende una solicitud para que el primer sistema transmita los datos del usuario al segundo sistema.

9. El método implementado por ordenador de cualquiera de las reivindicaciones 6 a 8, que comprende además:
en respuesta a recibir el segundo mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades no autorizadas almacenadas en el primer sistema y no identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades no autorizadas almacenadas en el primer sistema y, en respuesta, transmitiendo un mensaje de concesión indicativo de que se ha concedido la solicitud de acceso.

10. El método implementado por ordenador de la reivindicación 9, que comprende además:
en respuesta a recibir el segundo mensaje de acceso, comparar la segunda etiqueta del sistema con la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema y no identificar una coincidencia entre la segunda etiqueta del sistema y por lo menos una de la pluralidad de etiquetas de entidades autorizadas almacenadas en el primer sistema y, en respuesta, evitar la transmisión del mensaje de concesión.

11. El método implementado por ordenador de cualquiera de las reivindicaciones precedentes que comprende además:

recibir o introducir, en el primer sistema, un mensaje de detección de entidades no autorizadas que comprende una etiqueta indicativa de un identificador de una entidad sospechosa de actividad fraudulenta y/o sospechosa de haber sido sometida a una violación de seguridad;
almacenar, en la base de datos de entidades no autorizadas del primer sistema, la etiqueta del mensaje de detección de entidades no autorizadas como una etiqueta de entidad no autorizada indicativa de un identificador de una entidad no autorizada.

12. Un sistema de gestión de datos para compartir datos asociados con un primer usuario, el sistema de gestión de datos comprendiendo:

un recurso de almacenamiento de datos configurado para:

almacenar datos de usuario asociados con el primer usuario;
almacenar una primera base de datos de entidades autorizadas que comprende una pluralidad de etiquetas de entidades autorizadas cada una indicativa de un identificador de una entidad autorizada, en donde almacenar la primera base de datos de entidades autorizadas comprende:

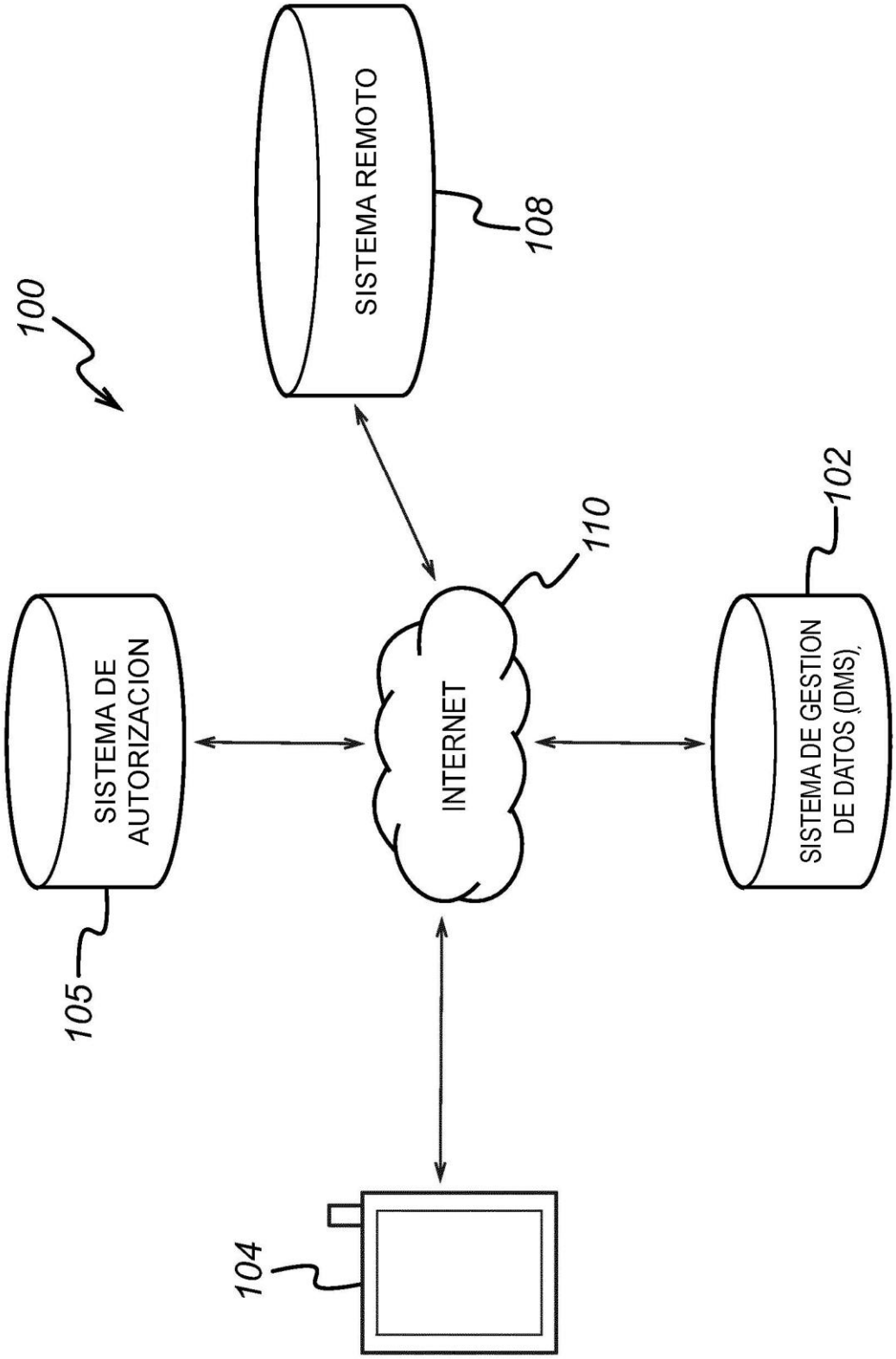
transmitir, desde el primer sistema a un sistema de autorización, una pluralidad de solicitudes para acceder a una segunda base de datos de entidades autorizadas almacenada en el sistema de autorización; y
recibir y almacenar, en el primer sistema, por lo menos una parte de la segunda base de datos de entidades autorizadas en respuesta a cada una de la pluralidad de solicitudes de acceso a la base de datos de entidades autorizadas;
en donde la pluralidad de solicitudes para acceder a la segunda base de datos de entidades autorizadas se transmite en una secuencia temporal predefinida, en donde la secuencia temporal predefinida comprende un intervalo de tiempo predefinido entre cada solicitud adyacente de las solicitudes para acceder a la segunda base de datos de entidades autorizadas, y en donde la secuencia temporal predefinida es configurada por el primer sistema, en base a las condiciones del sistema; y
almacenar una base de datos de entidades no autorizadas que comprende una pluralidad de etiquetas de entidades no autorizadas cada una indicativa de un identificador de una entidad no autorizada; y

en donde el que el sistema de gestión de datos comprende además circuitería de procesamiento configurada para:

recibir un primer mensaje de acceso, desde un sistema remoto, asociado con una solicitud de acceso a los datos de usuario almacenados en el primer sistema, el primer mensaje de acceso comprendiendo una etiqueta del sistema remoto indicativa de un identificador del sistema remoto;
comparar la etiqueta del sistema remoto con la pluralidad de etiquetas de entidades autorizadas y la pluralidad de etiquetas de entidades no autorizadas almacenadas en el primer sistema, en respuesta a la

recepción del primer mensaje de acceso;
transmitir un mensaje de concesión indicativo de que se concede la solicitud de acceso, en respuesta a la identificación de que la etiqueta del sistema remoto coincide con una etiqueta de entidad autorizada y que la etiqueta del sistema remoto no coincide con una etiqueta de entidad no autorizada; y
evitar la transmisión del mensaje de concesión, si la etiqueta del sistema remoto en el primer mensaje de acceso coincide con una etiqueta de entidad no autorizada y/o no coincide con una etiqueta de entidad autorizada.

FIG. 1


100
SISTEMA REMOTO
108
SISTEMA DE AUTORIZACION
105
INTERNET
110
SISTEMA DE GESTION DE DATOS (DMS),
102
104

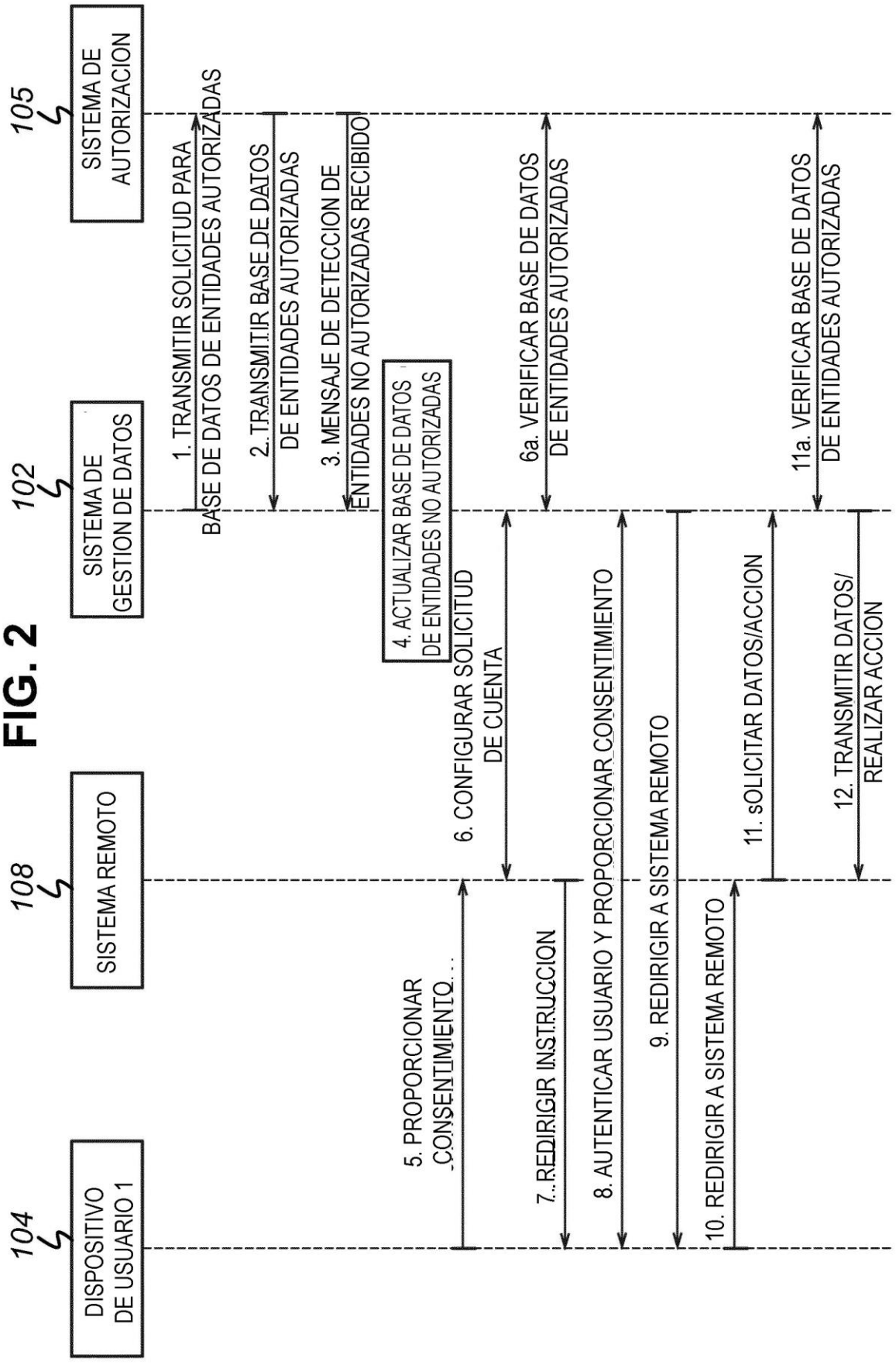

104
DISPOSITIVO DE USUARIO 1
108
SISTEMA REMOTO
102
SISTEMA DE GESTION DE DATOS
105
SISTEMA DE AUTORIZACION
1. TRANSMITIR SOLICITUD PARA BASE DE DATOS DE ENTIDADES AUTORIZADAS
2. TRANSMITIR BASE DE DATOS DE ENTIDADES AUTORIZADAS
3. MENSAJE DE DETECCION DE ENTIDADES NO AUTORIZADAS RECIBIDO
4. ACTUALIZAR BASE DE DATOS DE ENTIDADES NO AUTORIZADAS
5. PROPORCIONAR CONSENTIMIENTO
6. CONFIGURAR SOLICITUD DE CUENTA
6a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
7. REDIRIGIR INSTRUCCION
8. AUTENTICAR USUARIO Y PROPORCIONAR CONSENTIMIENTO
9. REDIRIGIR A SISTEMA REMOTO
10. REDIRIGIR A SISTEMA REMOTO
11. sOLICITAR DATOS/ACCION
11a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
12. TRANSMITIR DATOS/ REALIZAR ACCION

FIG. 2

FIG. 3

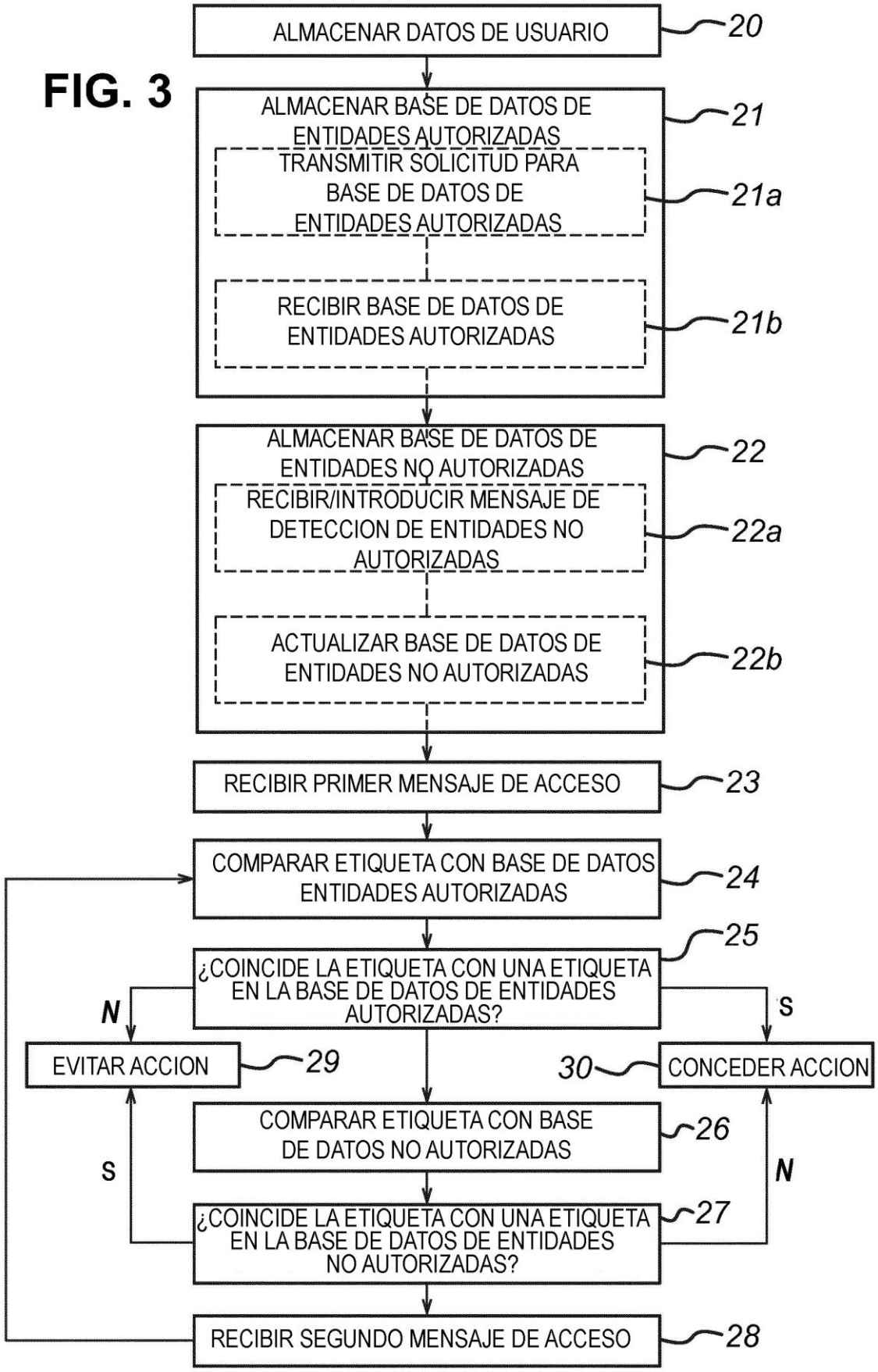

ALMACENAR DATOS DE USUARIO
20
ALMACENAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
21
TRANSMITIR SOLICITUD PARA BASE DE DATOS DE ENTIDADES AUTORIZADAS
21a
RECIBIR BASE DE DATOS DE ENTIDADES AUTORIZADAS
21b
ALMACENAR BASE DE DATOS DE ENTIDADES NO AUTORIZADAS
22
RECIBIR/INTRODUCIR MENSAJE DE DETECCION DE ENTIDADES NO AUTORIZADAS
22a
ACTUALIZAR BASE DE DATOS DE ENTIDADES NO AUTORIZADAS
22b
RECIBIR PRIMER MENSAJE DE ACCESO
23
COMPARAR ETIQUETA CON BASE DE DATOS ENTIDADES AUTORIZADAS
24
¿COINCIDE LA ETIQUETA CON UNA ETIQUETA EN LA BASE DE DATOS DE ENTIDADES AUTORIZADAS?
25
N
S
EVITAR ACCION
29
30
CONCEDER ACCION
COMPARAR ETIQUETA CON BASE DE DATOS NO AUTORIZADAS
26
S
N
¿COINCIDE LA ETIQUETA CON UNA ETIQUETA EN LA BASE DE DATOS DE ENTIDADES NO AUTORIZADAS?
27
RECIBIR SEGUNDO MENSAJE DE ACCESO
28

FIG. 4

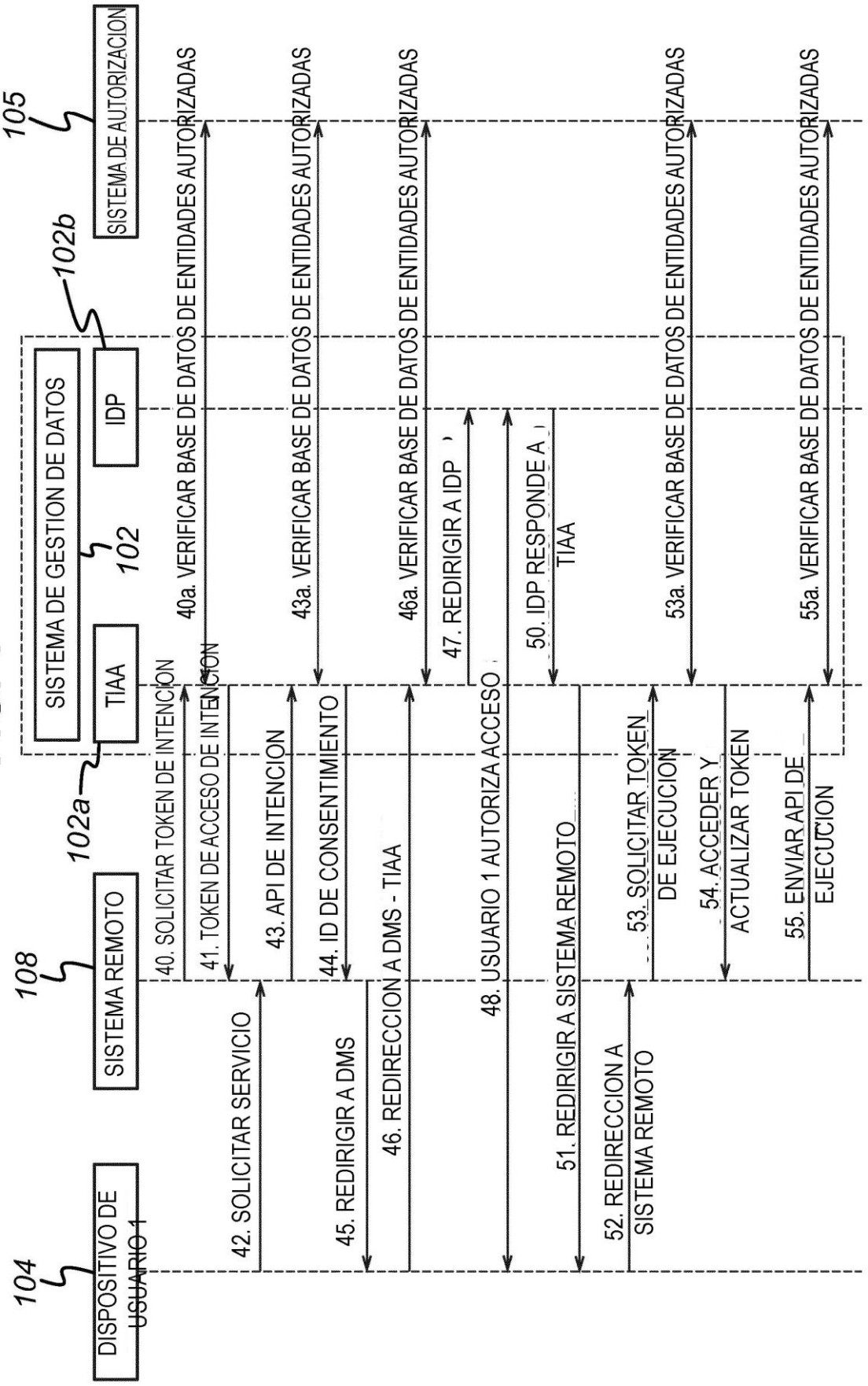

104
DISPOSITIVO DE USUARIO 1
108
SISTEMA REMOTO
102a
TIAA
SISTEMA DE GESTION DE DATOS
102
IDP
102b
105
SISTEMA DE AUTORIZACION
40. SOLICITAR TOKEN DE INTENCION
40a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
41. TOKEN DE ACCESO DE INTENCION
42. SOLICITAR SERVICIO
43. API DE INTENCION
43a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
44. ID DE CONSENTIMIENTO
45. REDIRIGIR A DMS
46. REDIRECCION A DMS - TIAA
46a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
47. REDIRIGIR A IDP
48. USUARIO 1 AUTORIZA ACCESO
50. IDP RESPONDE A TIAA
51. REDIRIGIR A SISTEMA REMOTO
52. REDIRECCION A SISTEMA REMOTO
53. SOLICITAR TOKEN DE EJECUCION
53a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS
54. ACCEDER Y ACTUALIZAR TOKEN
55. ENVIAR API DE EJECUCION
55a. VERIFICAR BASE DE DATOS DE ENTIDADES AUTORIZADAS

FIG. 5

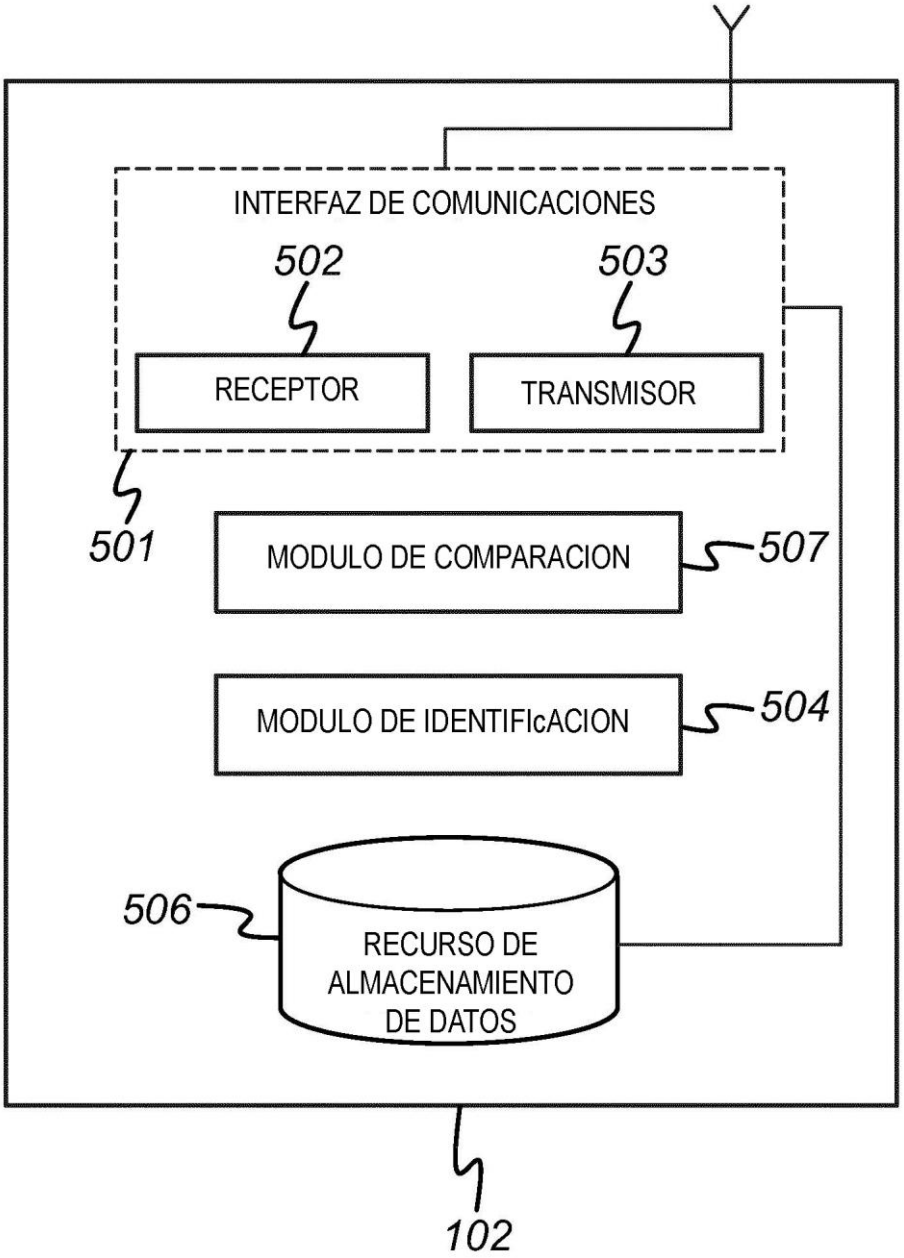
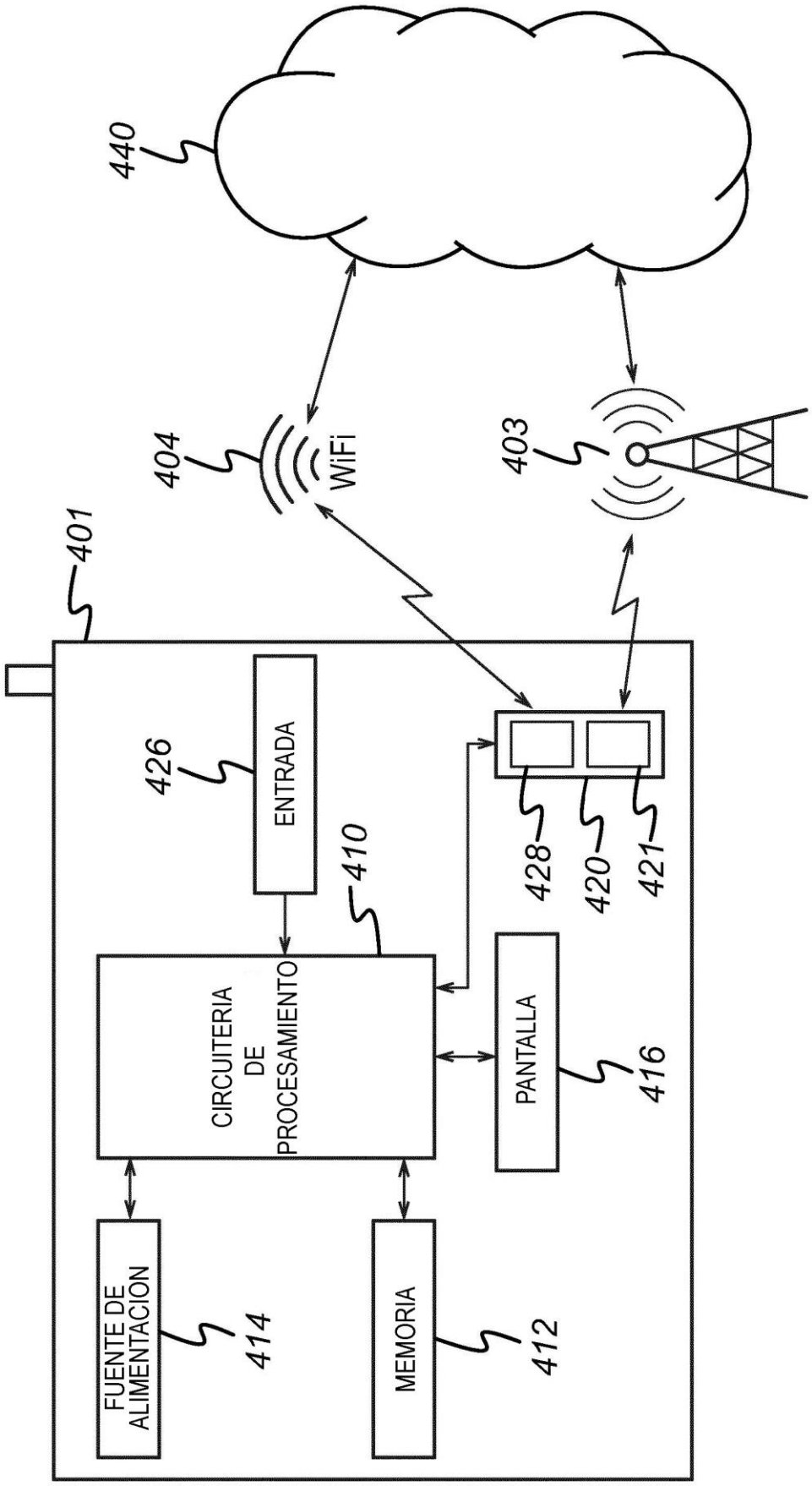

INTERFAZ DE COMUNICACIONES
502
503
RECEPTOR
TRANSMISOR
501
MODULO DE COMPARACION
507
MODULO DE IDENTIFIcACION
504
506
RECURSO DE ALMACENAMIENTO DE DATOS
102

FIG. 6


440
404
WiFi
403
401
426
ENTRADA
410
428
420
421
CIRCUITERIA DE PROCESAMIENTO
PANTALLA
416
FUENTE DE ALIMENTACION
414
MEMORIA
412