(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 023 749**

(51) Int. CI.:

***H04L 9/40*** (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.07.2017 PCT/GB2017/052027**

(87) Fecha y número de publicación internacional: **18.01.2018 WO18011559**

(96) Fecha de presentación y número de la solicitud europea: **11.07.2017 E 17742835 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2025 EP 3482550**

(54) Título: **Proporcionar acceso a datos almacenados estructurados**

(30) Prioridad:

**11.07.2016 GB 201612038**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**03.06.2025**

(73) Titular/es:

**LOOKIIMEDIA (UK) LIMITED (100.00%)**
**27 John's Mews**
**London WC1N 2NS, GB**

(72) Inventor/es:

**O'TOOLE, JULIA**

(74) Agente/Representante:

**CARVAJAL Y URQUIJO, Isabel**

## DESCRIPCIÓN

Proporcionar acceso a datos almacenados estructurados

Campo de la invención

La presente invención se encuentra en el campo del acceso a datos. Más particularmente, pero no exclusivamente, la presente invención se refiere a la autenticación del acceso a los datos.

Antecedentes de la invención

Asegurar el acceso a datos confidenciales es un desafío, ya que los delitos cibernéticos, incluidos el pirateo de cuentas, el fraude, los delitos financieros y el espionaje industrial, están aumentando cada vez más. Los ladrones y piratas informáticos emplean varios métodos para adivinar nombres de usuario y contraseñas, obteniendo acceso a sistemas y datos seguros.

Algunos proveedores en línea han abordado los problemas de seguridad al exigir que los usuarios se autentiquen utilizando contraseñas cada vez más complicadas. Sin embargo, las contraseñas complicadas son difíciles de recordar para los usuarios, porque los usuarios deben recordar un número cada vez mayor de contraseñas para funcionar en la era del comercio electrónico.

Otra solución que los proveedores en línea han aplicado es la autenticación de dos o múltiples factores, que a menudo requiere que el usuario ingrese una contraseña y un código único enviado al usuario por SMS o correo electrónico. La autenticación multifactor es más segura que una simple contraseña, pero aún es posible que los piratas informáticos intercepten mensajes SMS y correos electrónicos para recibir el código.

Además, cuando un usuario olvida una contraseña, el proceso de restablecimiento de contraseña suele ser un proceso de varios pasos que resulta frustrante para los usuarios. Para restablecer una contraseña, el usuario a veces debe responder a preguntas de restablecimiento de contraseña, responder a preguntas sobre números de cuenta u otra información personal, llamar a un representante de servicio al cliente y/o recibir y seguir un enlace de restablecimiento recibido por correo electrónico.

Una solución para administrar y recordar contraseñas que proporcionan acceso a información segura es un administrador de contraseñas. La información dentro de un administrador de contraseñas, que a menudo incluye nombres de usuario y contraseñas, se mantiene en un único almacén de datos al que se puede acceder al autenticarse con una contraseña maestra. Si bien mantener la información en un solo almacén de datos puede no presentar un problema cuando la información que se está protegiendo no es confidencial, es posible que algunos usuarios no deseen acceder a su información más confidencial cada vez que accedan a información que no es confidencial. Por ejemplo, es posible que un usuario que desee acceder a la información relacionada con un sitio web promocional no desee acceder a la información relacionada con sus cuentas bancarias y de inversión al mismo tiempo.

Otro problema con los administradores de contraseñas es que algunas cuentan con contraseñas maestras que no son recuperables. Un usuario que olvida una contraseña maestra irrecuperable puede perder el acceso a la información guardada para siempre.

Las publicaciones de patente US 2007/0143825 A1 y US 2014/0373104 A1 divulgan soluciones de seguridad adaptativas que proporcionan diferentes niveles de seguridad basados en la sensibilidad de los datos.

Un objeto de la presente invención es proporcionar una forma de autenticar el acceso a datos seguros que supere las desventajas de la técnica anterior, o al menos proporcione una alternativa útil.

Breve descripción de la invención

De acuerdo con un primer aspecto de la invención, se proporciona un método para proporcionar acceso a una pluralidad de almacenes de datos estructurados basados en una pluralidad de información de autenticación personal, el método comprende: en un sistema de protección de datos estructurado:

recibir una primera información de autenticación personal de la pluralidad de información de autenticación personal de un usuario;
al autenticar la primera información de autenticación personal, proporcionar acceso de usuario a un almacén de datos de primer nivel de la pluralidad de almacenes de datos estructurados, el almacén de datos de primer nivel almacena una pluralidad de pares de nombre de usuario/contraseña, cada par para acceder a un primero de una pluralidad de servidores;
una vez que se proporciona acceso de usuario al almacén de datos de primer nivel, el usuario recupera uno de los pares de nombre de usuario/contraseña en el almacén de datos de primer nivel y accede al

primer servidor utilizando el par de nombre de usuario/contraseña;
recibir una segunda información de autenticación personal de la pluralidad de información de autenticación personal del usuario;
al autenticar la segunda información de autenticación personal, y después de autenticar la primera información de autenticación personal, proporcionar acceso de usuario a un almacén de datos de segundo nivel de la pluralidad de almacenes de datos estructurados, el almacén de datos de segundo nivel almacena una pluralidad de pares de nombre de usuario/contraseña, cada par para acceder a un segundo de una pluralidad de servidores;
una vez que se proporciona acceso de usuario al almacén de datos de segundo nivel, el usuario recupera uno de los pares de nombre de usuario/contraseña en el almacén de datos de segundo nivel y accede al segundo servidor utilizando el par de nombre de usuario/contraseña;
recibir una tercera información de autenticación personal de la pluralidad de información de autenticación personal del usuario;
al autenticar la tercera información de autenticación personal, y después de autenticar la primera información de autenticación personal y la segunda información de autenticación personal, proporcionar acceso de usuario a un almacén de datos de tercer nivel de la pluralidad de almacenes de datos estructurados, el almacén de datos de tercer nivel almacena una pluralidad de pares de nombre de usuario/contraseña, cada par para acceder a un tercero de una pluralidad de servidores; y
una vez que se proporciona acceso de usuario al almacén de datos de tercer nivel, el usuario recupera uno de los pares de nombre de usuario/contraseña en el almacén de datos de tercer nivel y accede al tercer servidor utilizando el par de nombre de usuario/contraseña;

en donde la primera, segunda y tercera información de autenticación personal son de diferentes tipos entre sí, en donde los almacenes de datos de primer, segundo y tercer nivel son diferentes entre sí y almacenan diferentes pares de nombre de usuario/contraseña.

De acuerdo con un aspecto adicional, al menos una información de autenticación personal alfa de la pluralidad de información de autenticación personal puede ser un primer dato de tipo biométrico.

De acuerdo con un aspecto adicional, una información de autenticación personal beta de la pluralidad de información de autenticación personal puede ser un segundo dato de tipo biométrico que es diferente de los primeros datos de tipo biométrico.

De acuerdo con un aspecto adicional, una información de autenticación personal gamma de la pluralidad de autenticación personal puede ser un tercer tipo de datos, y el tercer tipo de datos puede ser diferente del primer tipo de datos y el segundo tipo de datos.

De acuerdo con un aspecto adicional, al menos uno de la pluralidad de almacenes de datos estructurados puede incluir datos de autenticación de terceros.

De acuerdo con un aspecto adicional, los datos de autenticación de terceros pueden incluir una contraseña.

De acuerdo con un aspecto adicional, al menos un almacén de datos de la pluralidad de almacenes de datos estructurados puede incluir al menos uno de: un archivo de datos, un número o una cadena de texto.

De acuerdo con un aspecto adicional, la pluralidad de información de autenticación personal puede incluir al menos uno de: datos de huellas dactilares, un código PIN, información de grabación de voz, datos de mensajes de voz, información de imágenes faciales, información de imágenes del iris o información de imágenes de la retina.

El método puede incluir además el paso de: mostrar una interfaz de usuario de almacén de datos que incluye información segura de al menos un almacén de datos de la pluralidad de almacenes de datos.

De acuerdo con un aspecto adicional, el paso de mostrar la interfaz de usuario del almacén de datos puede incluir además mostrar uno o más iconos asociados con la información segura incluida en el almacén de datos seleccionado de la pluralidad de almacenes de datos.

El método puede incluir, además: recibir una solicitud de cambio de almacén de datos para información segura previamente almacenada, la solicitud de cambio de almacén de datos incluyendo un nuevo almacén de datos; y asociar la información segura previamente almacenada con el nuevo almacén de datos.

El método puede incluir, además:

recibir un archivo de imagen de registro del sitio web;
reconocer texto en el archivo de imagen de registro del sitio web, incluida la información relacionada con el registro; y
asociar la información segura con un almacén de datos seleccionado de la pluralidad de almacenes de

datos a los que se ha autorizado el acceso.

De acuerdo con un aspecto adicional, la información relacionada con el registro puede incluir al menos uno de: un dominio de sitio web, un nombre comercial, un nombre de usuario, una contraseña, una sugerencia de contraseña, una pista de contraseña, una pregunta de restablecimiento, un icono o una respuesta de restablecimiento.

El método puede incluir, además:

mostrar una interfaz de usuario de actualización de almacén de datos que incluye información segura de un almacén seguro seleccionado de la pluralidad de almacenes de datos;
recibir información segura actualizada del usuario; y
asociar la información segura actualizada con el almacén de datos seleccionado.
De acuerdo con un aspecto adicional, al menos una de la pluralidad de información de autenticación personal puede comprender, además: recibir la al menos una de la pluralidad de información de autenticación personal desde un dispositivo cliente.

De acuerdo con un aspecto adicional, autenticar la primera información de autenticación personal o autenticar la segunda información de autenticación personal puede comprender, además:

enviar la al menos una información de autenticación personal de la pluralidad de información de autenticación personal a un servidor; y
recibir una confirmación de información de autenticación personal del servidor.

De acuerdo con un aspecto adicional, existe un sistema configurado para proporcionar un sistema de protección de datos estructurado a través de cualquier método del primer aspecto.

De acuerdo con un aspecto adicional, existe un programa informático configurado para proporcionar un sistema de protección de datos estructurado a través de cualquier método del primer aspecto. De acuerdo con un aspecto adicional, existe un medio legible electrónicamente configurado para almacenar un programa informático configurado para proporcionar un sistema de protección de datos estructurado a través de cualquier método del primer aspecto.

De acuerdo con un segundo aspecto de la invención, se proporciona un método que comprende, además: en el sistema estructurado de protección de datos:

recibir una primera información de configuración de autenticación personal;
guardar los primeros datos de autenticación guardados en función de la primera información de configuración de autenticación personal en un perfil de usuario;
recibir una segunda información de configuración de autenticación personal; y
guardar los segundos datos de autenticación guardados en función de la segunda información de configuración de autenticación personal en el perfil de usuario,
recibir una tercera información de configuración de autenticación personal; y
guardar la tercera información de configuración de autenticación personal como terceros datos de autenticación guardados en el perfil de usuario;

en donde la primera información de autenticación personal se autentica utilizando los primeros datos de autenticación guardados, la segunda información de autenticación personal se autentica utilizando los segundos datos de autenticación guardados y la tercera información de autenticación personal se autentica utilizando los terceros datos de autenticación guardados.

El método puede comprender, además:

recibir una primera información segura; y
asociar la primera información segura con un almacenamiento de datos alfa de la pluralidad de almacenes de datos.

El método puede comprender, además:

recibir una segunda información segura; y
asociar la segunda información segura con un almacenamiento de datos beta de la pluralidad de almacenes de datos.

De acuerdo con un aspecto adicional, una información de autenticación personal alfa de la pluralidad de información de autenticación personal puede ser un primer dato de tipo biométrico.

De acuerdo con un aspecto adicional, una segunda información de autenticación personal de la pluralidad de

información de autenticación personal puede ser un segundo dato de tipo biométrico que es diferente de los primeros datos de tipo biométrico.

De acuerdo con un aspecto adicional, una información de autenticación personal gamma de la pluralidad de información de autenticación personal puede ser un tercer tipo de datos, y el tercer tipo de datos puede ser diferente del primer tipo de datos y el segundo tipo de datos.

De acuerdo con un aspecto adicional, al menos uno de la pluralidad de almacenes de datos estructurados puede incluir datos de autenticación de terceros.

De acuerdo con un aspecto adicional, los datos de autenticación de terceros pueden incluir una contraseña.

De acuerdo con un aspecto adicional, al menos un almacén de datos de la pluralidad de almacenes de datos estructurados puede incluir al menos uno de: un archivo de datos, un número o una cadena de texto.

De acuerdo con un aspecto adicional, la pluralidad de información de autenticación personal puede incluir al menos uno de: datos de huellas dactilares, un código PIN, información de grabación de voz, datos de mensajes de voz, información de imágenes faciales, información de imágenes del iris o información de imágenes de la retina.

El método puede comprender, además:

recibir un archivo de imagen de registro del sitio web;
reconocer texto en el archivo de imagen de registro de sitio web que incluye información relacionada con el registro, la información relacionada con el registro que incluye al menos uno de: un dominio de sitio web, un nombre comercial, un nombre de usuario, una contraseña, una solicitud de contraseña, una pista de contraseña, una pregunta de restablecimiento, un icono o una respuesta de restablecimiento; y
asociar la información segura con un almacén de datos seleccionado de la pluralidad de almacenes de datos a los que se ha autorizado el acceso.

De acuerdo con un aspecto adicional, recibir al menos una de la primera información de confirmación de autenticación personal, la segunda información de confirmación de autenticación personal o una tercera información de confirmación de autenticación personal puede comprender, además:

determinar un período de tiempo de espera de entrada del usuario; y
guardar el período de tiempo de espera de entrada del usuario con el perfil de usuario.

El método puede comprender, además:

recibir una solicitud de cambio de almacén de datos para información segura previamente almacenada, la solicitud de cambio de almacén de datos incluye un nuevo almacén de datos; y
asociar la información segura previamente almacenada con el nuevo almacén de datos.

De acuerdo con un aspecto adicional, existe un sistema configurado para configurar un sistema de protección de datos estructurado a través de cualquier método del segundo aspecto.

De acuerdo con un aspecto adicional, existe un sistema estructurado de protección de datos a través de cualquier método del segundo aspecto.

De acuerdo con un aspecto adicional, existe un medio legible electrónicamente que almacena un programa informático configurado para proporcionar un sistema de protección de datos estructurado a través de cualquier método del segundo aspecto.

Otros aspectos de la invención se describen en las reivindicaciones.

Breve descripción de los dibujos

Ahora se describirán realizaciones de la invención, solo a modo de ejemplo, con referencia a los dibujos adjuntos en los que:

Figura 1: muestra el sistema 100 de acuerdo con una realización de la invención;

Figura 2: muestra el sistema 200 de acuerdo con una realización de la invención;

Figura 3: muestra el sistema 300 de acuerdo con una realización de la invención;

Figura 4: muestra el método 400 de acuerdo con una realización de la invención;

Figura 5: muestra el almacén de datos estructurados 500 de acuerdo con una realización de la invención;

Figura 6: muestra el método 600 de acuerdo con una realización de la invención;

Figura 7: muestra el método 700 de acuerdo con una realización de la invención;

Figura 8: muestra el método 800 de acuerdo con una realización de la invención;

Figura 9: muestra la interfaz de usuario 900 de acuerdo con una realización de la invención;

Figura 10: muestra la interfaz de usuario 1000 de acuerdo con una realización de la invención;

Figura 11: muestra la interfaz de usuario 1100 de acuerdo con una realización de la invención; y

Figura 12: muestra el sistema 1200 de acuerdo con una realización de la invención.

Descripción detallada de la invención

La presente invención proporciona un método, sistema y programa informático para configurar y proporcionar acceso a una pluralidad de almacenes de datos estructurados basados en una pluralidad de información de autenticación personal.

La Figura 1 representa un sistema 100 de acuerdo con una realización. El sistema 100 incluye el dispositivo cliente 102. El sistema 100 puede incluir además el servidor de configuración 104, el servidor de terceros 106, Internet 108, el dispositivo biométrico 110, la base de datos de perfiles de usuario 114 y los almacenes de datos estructurados 116.

El dispositivo cliente 102 puede funcionar para configurar y proporcionar a un usuario acceso a una pluralidad de almacenes de datos estructurados en función de una pluralidad de información de autenticación personal, como se describe en relación con las Figuras 4 a 12. El servidor de configuración 104 puede funcionar además para facilitar la configuración y proporcionar acceso a una pluralidad de almacenes de datos estructurados en función de una pluralidad de información de autenticación personal, como se describe en relación con las Figuras 4 a 12.

Cada uno del dispositivo cliente 102, el servidor de configuración 104, el servidor de terceros 106 y el dispositivo biométrico 110 puede incluir un dispositivo de procesamiento 200, como se ilustra en la Figura 2. El dispositivo de procesamiento 200 incluye un procesador 202, una memoria 204 y una interfaz de comunicación 206. En los ejemplos, el dispositivo de procesamiento 200 puede incluir además una pantalla 208.

El procesador 202 puede configurarse para ejecutar instrucciones informáticas que, cuando se ejecutan en el sistema 100, realizan una parte o todos los métodos descritos en relación con las Figuras 4 a 12. En realizaciones, el procesador 202 puede incluir un solo procesador o cualquier número múltiple de procesadores, como entenderán los expertos en la técnica.

La memoria 204 puede ser un medio legible electrónicamente o un medio legible por ordenador configurado para almacenar instrucciones de programa informático. En ejemplos, la memoria 204 puede incluir un medio no transitorio.

Las instrucciones de programa informático almacenadas, cuando se ejecutan en el procesador 202, pueden realizar una parte o todos los métodos descritos en relación con las Figuras 4 a 12.

En ejemplos, el procesador 202 y la memoria 204 pueden incorporarse en un conjunto de chips personalizado, tal como un sistema en un chip. Por ejemplo, el procesador 202 y la memoria 204 pueden incorporarse en un chip Snapdragon, Tegra, Mali-400, Cortex, Samsung Exynos, Intel Atom, Apple o Motorola personalizado, o cualquier otro tipo de chip conocido por los expertos en la técnica.

En ejemplos, partes de los métodos descritos en relación con las Figuras 4 a 12 pueden almacenarse o ejecutarse fuera del sistema 100. Por ejemplo, una parte de los métodos descritos en relación con las Figuras 4 a 12 puede almacenarse o ejecutarse en una combinación de un servidor y una instalación de almacenamiento en la nube a través de Internet 108.

La interfaz de comunicaciones 206 puede configurarse para comunicarse con dispositivos externos al dispositivo cliente 102 o al servidor de configuración 104. Por ejemplo, la interfaz de comunicaciones 206 puede comunicarse con cualquiera de los dispositivos biométricos 110, la base de datos de perfiles de usuario 114 o los almacenes de datos estructurados 116.

En ejemplos, la interfaz de comunicaciones 206 puede incluir interfaces cableadas o inalámbricas. La interfaz de comunicaciones 206 puede incluir un estándar inalámbrico de corto alcance o de baja potencia, como Bluetooth, Bluetooth LE, zigbee o comunicación de campo cercano (NFC). La interfaz de comunicaciones 206 puede incluir además WIFI, 3G, 4G, Ethernet o cualquier otra comunicación conocida por los expertos en la técnica. En ejemplos, el dispositivo de procesamiento 200 puede solicitar, enviar o recibir información, guardar información o enviar o recibir mensajes desde un dispositivo remoto a través de Internet 108.

En ejemplos, el dispositivo cliente 102 puede ser un dispositivo informático portátil o móvil tal como un teléfono inteligente, una tableta, un reloj inteligente o un dispositivo portátil. En ejemplos adicionales, el dispositivo cliente 102 puede ser un aparato informático tal como un televisor inteligente, una consola de videojuegos, un ordenador portátil o de escritorio, o una pieza de hardware doméstico habilitada para aplicaciones.

En ejemplos, el dispositivo cliente 102 puede recibir entradas de uno o más dispositivos de entrada integrados. En ejemplos adicionales, sin embargo, el dispositivo cliente 102 puede estar conectado a cualquier combinación de dispositivos de entrada externos, incluyendo uno o más dispositivos biométricos 110.

El dispositivo cliente 102 o el dispositivo biométrico 110 pueden incluir cualquier combinación de instrumentos de entrada operables para recibir información de un ser humano, un animal o un entorno. En ejemplos, el dispositivo cliente 102 o el dispositivo biométrico 110 pueden incluir un escáner de huellas digitales tal como un dispositivo táctil capacitivo, un dispositivo ultrasónico u óptico.

En ejemplos, el dispositivo cliente 102 o el dispositivo biométrico 110 pueden incluir un dispositivo de escaneo facial, tal como una imagen óptica, imagen térmica o dispositivo de escaneo 3D.

En ejemplos, el dispositivo cliente 102 o el dispositivo biométrico 110 pueden incluir un escáner ocular. En ejemplos, el escáner ocular puede incluir un escáner de iris o un escáner de retina usando un dispositivo de imágenes visible, infrarrojo y/o infrarrojo cercano.

En ejemplos, el dispositivo cliente 102 o el dispositivo biométrico 110 pueden incluir un detector de voz tal como un dispositivo de reconocimiento de voz o un dispositivo de reconocimiento de frases, que puede incluir un dispositivo de micrófono.

En ejemplos adicionales, el dispositivo cliente 102 o el dispositivo biométrico 110 pueden incluir cualquier otro dispositivo biométrico o biomonitor capaz de autenticar la identidad de un usuario, como entenderán los expertos en la técnica.

La Figura 1 incluye un servidor de configuración 104. El servidor de configuración 104 puede ser operable para ejecutar instrucciones, o para recuperar y guardar datos en una base de datos. En ejemplos, el servidor de configuración 104 puede incluir un único servidor o múltiples servidores en una arquitectura distribuida. En ejemplos, el servidor de configuración 104 puede admitir una base de datos relacional, una base de datos NoSQL, una base de datos distribuida o cualquier otra base de datos conocida por los expertos.

La Figura 3 representa el sistema 300, de acuerdo con una realización. El sistema 300 puede facilitar la configuración y proporcionar acceso a una pluralidad de almacenes de datos estructurados en función de una pluralidad de información de autenticación personal. El sistema 300 incluye la aplicación cliente 302. El sistema 300 puede incluir además la aplicación del servidor de configuración 304, la aplicación del servidor de terceros 306 y la aplicación biométrica 310.

El servidor de configuración 304 puede configurarse para recibir entradas de la aplicación cliente 302 para facilitar la configuración y proporcionar acceso a una pluralidad de almacenes de datos estructurados en función de una pluralidad de información de autenticación personal.

La aplicación cliente 302 puede comunicarse con la aplicación de servidor de terceros 306.

La aplicación cliente 302 puede comunicarse con la aplicación biométrica 310.

En ejemplos, la aplicación cliente 302, la aplicación de servidor de configuración 304, la aplicación de servidor de terceros 306 y la aplicación biométrica 310 pueden funcionar cada una en dispositivos separados. Por ejemplo, la aplicación cliente 302 puede operar en el dispositivo cliente 102; la aplicación servidor de configuración 304 puede operar en el servidor de configuración 102; la aplicación servidor de terceros 306 puede operar en el servidor de terceros 106; y la aplicación biométrica 310 puede operar en el dispositivo biométrico 110.

En ejemplos adicionales, sin embargo, las funciones de cualquiera de la aplicación cliente 302, la aplicación de servidor de configuración 304, la aplicación de servidor de terceros 306 y la aplicación biométrica 310 pueden distribuirse a través de dispositivos informáticos adicionales. Por ejemplo, la aplicación de servidor de configuración 304 puede operar a través de un grupo de servidores distribuidos.

La Figura 4 representa el método 400, una realización de ejemplo que puede ejecutarse dentro de cualquier combinación de la aplicación cliente 302 o la aplicación del servidor de configuración 304. El método 400 puede proporcionar acceso a una pluralidad de almacenes de datos estructurados en función de una pluralidad de información de autenticación personal.

La Figura 5 representa una pluralidad de ejemplo de almacenes de datos estructurados 500. Un almacén de datos es un repositorio físico o virtual para almacenar y administrar persistentemente una o más colecciones de datos. En ejemplos, un almacén de datos puede ser un archivo simple, una base de datos o cualquier otro repositorio conocido por los expertos en la técnica.

Como se puede ver en la Figura 5, la pluralidad de ejemplos de almacenes de datos estructurados 500 incluye el almacén de datos de primer nivel 502, el almacén de datos de segundo nivel 504 y el almacén de datos de tercer nivel 506. El almacenamiento de datos de tercer nivel 506 está configurado para ser accedido después de obtener acceso al almacenamiento de datos de segundo nivel 504, y tanto el tercer como el segundo almacenamiento de datos 506 y 504 están configurados para ser accedidos después de obtener acceso al almacenamiento de datos de primer nivel 502.

Un usuario que desee acceder a un almacén de datos dentro de los almacenes de datos estructurados 500 debe autenticarse antes de obtener el acceso. La autenticación es el proceso de confirmar la identidad de un usuario utilizando la información de autenticación personal proporcionada por el usuario. Por ejemplo, un usuario que desee acceder al primer almacén de datos 402 puede autenticarse en un primer nivel.

En ejemplos, la información de autenticación personal puede incluir datos de huellas dactilares. Los datos de huellas dactilares pueden incluir datos recibidos de un escáner de huellas dactilares. Los datos de huellas dactilares pueden incluir datos sin procesar, como un archivo de imagen bidimensional, o datos procesados, como información de extracción de características, una suma de verificación de imágenes o información de hash.

En ejemplos, la información de autenticación personal puede incluir información de grabación de voz desde un dispositivo de reconocimiento de voz. La información de grabación de voz puede ser independiente del texto. La información de grabación de voz puede incluir datos sin procesar, como un archivo de audio, o datos procesados, que pueden incluir impresiones de voz o información de extracción de características. La información de grabación de voz se puede utilizar para autenticar la voz de un usuario.

En ejemplos, la información de autenticación personal puede incluir datos de mensajes de voz de un dispositivo de reconocimiento de frases. Los datos de los mensajes de voz dependen del texto y pueden incluir datos sin procesar, como un archivo de audio, o datos procesados. Los datos del mensaje de voz se pueden usar para autenticar a un hablante.

En ejemplos, la información de autenticación personal puede incluir información de imagen facial de un dispositivo de escaneo facial. La información de la imagen facial puede incluir datos sin procesar, como un archivo de imagen, o datos procesados que incluyen información de extracción de características, una suma de verificación de imágenes o información de hash. La información de la imagen facial se puede utilizar para autenticar a un usuario en función de una o más características faciales.

En ejemplos, la información de autenticación personal puede incluir datos de imágenes oculares utilizando un escáner ocular. Por ejemplo, la información de autenticación personal puede incluir información de la imagen del iris o información de la imagen de la retina. Los datos de imágenes oculares pueden incluir datos sin procesar, como datos de imágenes, o datos procesados que incluyen información de extracción de características, una suma de verificación de imágenes o información de hash.

Por ejemplo, la información de autenticación personal puede incluir datos de contraseña o una contraseña.

En ejemplos, la información de autenticación personal puede incluir datos de código pin. Por ejemplo, la información de autenticación personal puede incluir un código de acceso o un patrón de pantalla de bloqueo.

Los ejemplos proporcionados de información de autenticación personal en este documento no pretenden ser limitativos. Los expertos en la técnica entenderán fácilmente que cualquier tipo de información capaz de autenticar a un usuario puede usarse como información de autenticación personal para proporcionar acceso a un almacén de datos. Por ejemplo, se puede usar cualquier tipo de información biométrica que pueda usarse razonablemente para identificar a un usuario.

Cuando se configura un almacén de datos para acceder después de obtener acceso a otro almacén de datos, un usuario debe autenticar ambos almacenes de datos antes de obtener acceso al almacén de datos más interno. Por ejemplo, cuando se configura un almacenamiento de datos de segundo nivel 504 para acceder después de obtener acceso al almacenamiento de datos de primer nivel 502, como se ilustra en la Figura 5, un usuario debe

autenticarse en el almacenamiento de datos de primer nivel 502 y el almacenamiento de datos de segundo nivel 504 antes de obtener acceso al almacenamiento de datos de segundo nivel 504.

Aunque el ejemplo de almacén de datos estructurados 500 incluye tres almacenes de datos estructurados, esto no pretende ser limitante. En ejemplos, los almacenes de datos estructurados 500 pueden incluir dos, tres o cualquier número de almacenes de datos.

En ejemplos adicionales, es posible que no se configure un almacenamiento de datos de tercer nivel 506 para acceder después de obtener acceso al almacenamiento de datos de segundo nivel 504. Por ejemplo, el almacén de datos de tercer nivel 506 puede configurarse para acceder solo después de obtener acceso al almacén de datos de primer nivel 502.

El método 400 comienza con el paso 402, se recibe una primera información de autenticación personal 402 de la pluralidad de información de autenticación personal.

En ejemplos, la información de autenticación personal recibida puede recibirse desde un dispositivo biométrico integrado en el dispositivo cliente 102, o externo al dispositivo cliente 102, tal como el dispositivo biométrico 110.

El método 400 continúa con el paso 404. En el paso 404, al autenticar la primera información de autenticación personal 402, se proporciona acceso a un almacén de datos de primer nivel de la pluralidad de almacenes de datos estructurados. Por ejemplo, se puede proporcionar acceso al almacenamiento de datos de primer nivel 502.

El método 400 continúa con el paso 406. En el paso 406, se recibe una segunda información de autenticación personal de la pluralidad de datos de inicio de sesión.

El método 400 continúa con el paso 408. En el paso 408, al autenticar la segunda información de autenticación personal, y después de autenticar la primera información de autenticación personal, se proporciona acceso a un almacenamiento de datos de segundo nivel de la pluralidad de almacenes de datos estructurados. Por ejemplo, se puede proporcionar acceso al almacenamiento de datos de segundo nivel 504.

Al permitir el acceso al almacenamiento de datos de primer nivel 502 al autenticar la primera información de autenticación personal 402, y permitir el acceso al almacenamiento de datos de segundo nivel 504 al autenticar tanto la primera información de autenticación personal 402 como la segunda información de autenticación personal 404, esto puede permitir que un usuario establezca diferentes niveles de seguridad para la información.

Por ejemplo, un usuario puede colocar información menos sensible en el almacén de datos de primer nivel e información con un mayor nivel de sensibilidad en el almacén de datos de segundo nivel. Cuando un usuario desea acceder solo a la información menos sensible en el almacén de datos de primer nivel, el usuario no accederá, por lo tanto, también a la información más sensible en el almacén de datos de segundo nivel.

En ejemplos, el método 400 puede incluir pasos adicionales. Por ejemplo, el método 400 continúa con los pasos 410 y 412. En el paso 410, se puede recibir una tercera información de autenticación personal de la pluralidad de datos de inicio de sesión.

En ejemplos, el método 400 puede continuar con el paso 412. En el paso 412, al autenticar la tercera información de autenticación personal 410, y después de autenticar la primera información de autenticación personal 402 y la segunda información de autenticación personal 406, se puede proporcionar acceso a un almacén de datos de tercer nivel de la pluralidad de almacenes de datos estructurados. Por ejemplo, se puede proporcionar acceso al almacenamiento de datos de tercer nivel 506.

Cuando se configura el almacén de datos de tercer nivel 506 para acceder después de obtener acceso a los almacenes de datos de primer y segundo nivel 502 y 504, los tres niveles del almacén de datos deben autenticarse para que un usuario obtenga acceso al almacén de datos de tercer nivel 506. Esto puede proporcionar a un usuario un almacenamiento de datos de mayor seguridad para la información que el usuario considere demasiado sensible para acceder a la información contenida en los almacenes de datos de primer y segundo nivel 502 y 504. También puede permitir al usuario acceder a datos menos confidenciales sin acceder también a los datos de mayor sensibilidad.

Al proporcionar acceso a una pluralidad de almacenes de datos estructurados basados en una pluralidad de información de autenticación personal, un usuario puede proteger la información de acuerdo con la sensibilidad percibida de los datos por el usuario. Esto puede permitir que un usuario se sienta mejor en el control de su información.

En ejemplos, puede haber niveles adicionales de almacenes de datos con información de autenticación personal respectiva que debe autenticarse para que un usuario obtenga acceso, como entenderán los expertos en la técnica.

En ejemplos, una información de autenticación personal alfa de la pluralidad de información de autenticación personal puede ser un primer dato de tipo biométrico. Los datos de tipo biométrico son datos que requieren una entrada biométrica de un usuario. Por ejemplo, los datos de tipo biométrico pueden incluir, de modo no limitativo, datos de huellas dactilares, datos de voz, datos de imágenes oculares o datos de imágenes faciales.

El uso de datos de tipo biométrico como información de autenticación personal puede permitir a un usuario evitar la dificultad de inventar y recordar una contraseña segura para proteger el almacenamiento de información de primer nivel. Debido a que un usuario no puede simplemente olvidar su información biométrica, la información biométrica de autenticación personal puede reducir la necesidad de restablecer las contraseñas. Los datos de tipo biométrico también pueden ser más seguros que las contraseñas. Esto puede permitir que un usuario acceda de manera consistente y segura a la información en el primer almacén de datos.

En ejemplos, una información de autenticación personal beta de una pluralidad de información de autenticación personal puede ser un segundo dato de tipo biométrico que es diferente de los primeros datos de tipo biométrico.

El uso de un primer tipo de datos biométricos para la primera información de autenticación personal y un segundo tipo de datos biométricos para la segunda información de autenticación personal puede permitir que un usuario acceda fácilmente al almacenamiento de datos de segundo nivel sin necesidad de inventar y recordar contraseñas.

En ejemplos, una información de autenticación personal gamma de la pluralidad de información de autenticación personal puede ser un tercer tipo de datos, y el tercer tipo de datos es diferente del primer tipo de datos y el segundo tipo de datos. Por ejemplo, la tercera información de autenticación personal puede ser un tercer tipo de datos biométricos.

Por ejemplo, la primera información de autenticación personal puede incluir datos de huellas dactilares o un código pin, la segunda información de autenticación personal puede incluir información de grabación de voz o datos de mensajes de voz, y la tercera información de identificación personal recibida puede incluir datos de reconocimiento facial o de reconocimiento ocular.

Al asignar un tipo de datos diferente a cada nivel de almacén de datos, puede ser posible proporcionar seguridad adicional para la información almacenada en el almacén de datos estructurado más interno, el almacén de datos de tercer nivel en el ejemplo proporcionado.

En ejemplos, al menos uno de la pluralidad de almacenes de datos estructurados incluye datos de autenticación de terceros. Los datos de autenticación de terceros pueden identificar repositorios o sitios web seguros de terceros, nombres de usuario o sugerencias de nombres de usuario, contraseñas o sugerencias de contraseñas, preguntas, respuestas o sugerencias de recuperación de contraseñas, o cualquier otra información relacionada con la obtención de información segura de un servidor de terceros 106.

En ejemplos, los datos de autenticación de terceros pueden incluir una contraseña.

En ejemplos, al menos un almacén de datos de la pluralidad de almacenes de datos estructurados puede incluir al menos uno de: un archivo de datos, un número o una cadena de texto.

Por ejemplo, el al menos un almacén de datos de la pluralidad de almacenes de datos estructurados puede incluir documentos que incluyen cualquier combinación de texto, imagen, video o audio. El al menos un almacén de datos de la pluralidad de almacenes de datos estructurados puede incluir además cualquier otro tipo de datos, tal como un número o una cadena de texto.

Al permitir que un usuario guarde cualquier combinación de archivos de datos, números o cadenas de texto en cualquiera de la pluralidad de almacenes de datos, puede ser posible proteger los datos o proteger las contraseñas de servidores de terceros, incluidos los datos seguros dentro del almacén de datos estructurados.

En ejemplos, al menos una información de autenticación personal de la pluralidad de información de autenticación personal se puede recibir dentro de un período de tiempo de espera de entrada del usuario.

Por ejemplo, el período de tiempo de espera de entrada del usuario se puede establecer durante un paso de configuración. Más adelante, cuando un usuario intenta obtener acceso a un almacén de datos, se puede determinar la cantidad de tiempo que se tarda en proporcionar la información de autenticación y compararla con el período de tiempo de espera de entrada del usuario. Si se tarda demasiado en introducir la información de autenticación personal, es posible que el usuario no esté autenticado.

Por ejemplo, si la información de autenticación personal incluye un patrón de pantalla de bloqueo para un teléfono inteligente, y el usuario que intenta autenticarse tarda 5 segundos en ingresar el patrón, pero el período de tiempo de espera de entrada del usuario es de solo 2 segundos, esto puede indicar que el usuario posterior que intenta obtener acceso a un almacén de datos no es el usuario original.

Al proporcionar un período de tiempo de espera de entrada del usuario, esto puede permitir la incorporación de un nivel de habilidad en el proceso de autenticación del usuario. Esto puede proporcionar un proceso de autenticación más sólido.

En ejemplos, el método 400 puede continuar con el paso 412. En el paso 412, se puede mostrar una interfaz de usuario del almacén de datos que incluye información segura de al menos un almacén de datos de la pluralidad de almacenes de datos.

En ejemplos, mostrar la interfaz de usuario del almacén de datos puede incluir además mostrar uno o más iconos asociados con la información segura incluida en el almacén de datos seleccionado de la pluralidad de almacenes de datos.

Por ejemplo, las Figuras 9, 10 y 11 representan ejemplos de interfaces de usuario de almacenamiento de datos 900, 1000 y 1100, respectivamente.

Como se puede ver en la interfaz de usuario del almacén de datos 900, se pueden mostrar iconos 902 que representan información segura disponible en el almacén de datos de segundo nivel.

Al seleccionar un icono de sitio web 902, la interfaz de usuario del almacén de datos representa una visualización de ejemplo de la información segura asociada con el icono de sitio web seleccionado 902.

Por ejemplo, la interfaz de usuario del almacén de datos 1000 muestra un sitio web, "uefa.com", un nombre de usuario, alex321@yahoo.com, y una contraseña, "footbal16".

Las interfaces de usuario del almacén de datos 900 y 1000 pueden permitir que un usuario solo vea la información segura que el usuario desea ver. Esto puede evitar que otros vean otra información segura en lugares públicos, por ejemplo.

Un tercer ejemplo se proporciona en la interfaz de usuario del almacén de datos 1100. La interfaz de usuario del almacén de datos 1100 incluye iconos 1102 que se muestran junto a sitios web, nombres de usuario y contraseñas. Esto puede permitir que un usuario vea toda la información en un almacén de datos de un solo vistazo.

Al permitir que un usuario determine qué información segura se guarda en cada almacén de datos, proporcionar un acceso fácil y seguro a esa información y permitir que el usuario vea toda la información segura de un vistazo en la interfaz de usuario del almacén de datos, es posible que un usuario se sienta en control de su información segura.

En ejemplos, el método 400 puede incluir además los pasos del método 600. El método 600 puede incluir el paso 602. La solicitud de cambio de almacén de datos 602 puede recibirse para información segura previamente almacenada, la solicitud de cambio de almacén de datos incluye un nuevo almacén de datos. Una solicitud de cambio de almacén de datos 602 es una solicitud para cambiar el almacén de datos en el que se guarda la información segura previamente almacenada.

En ejemplos, una interfaz de usuario de almacén de datos puede proporcionar una manera fácil para que un usuario genere una solicitud de cambio de almacén de datos 602. Por ejemplo, la interfaz de usuario del almacén de datos 1000 representa un selector de nivel del almacén de datos 1002. Un usuario puede determinar que la información previamente almacenada relacionada con un inicio de sesión en el sitio web de la Unión de Asociaciones Europeas de Fútbol (UEFA) debe guardarse en un nuevo almacén de datos o en un almacén de datos de primer nivel 502. Al realizar el cambio con el selector de nivel de almacén de datos 1002, un usuario puede guardar presionando el botón guardar 1004 para generar la solicitud de cambio de almacén de datos 602.

El método 600 puede incluir además el paso 604. En el paso 604, la información segura almacenada previamente puede asociarse con el nuevo almacenamiento de datos.

La solicitud de cambio de almacenamiento de datos 602 permite que un usuario tenga el control de sus datos. Él o ella puede cambiar el almacén de datos, y la autenticación relacionada requerida, para acceder a la información segura almacenada anteriormente.

El método 600 puede incluir además el paso 606. En el paso 606, se puede recibir un archivo de imagen de registro de sitio web.

Un archivo de imagen de registro de sitio web 606 es una imagen de un sitio web donde un usuario se está registrando para recibir acceso seguro, o reconfigurando su acceso seguro. Por ejemplo, el archivo de imagen de registro del sitio web 606 puede ser una captura de pantalla de un usuario que se registra para vincularse.

En ejemplos, el archivo de registro del sitio web 606 puede ser una captura de pantalla.

El método 600 puede incluir además el paso 608. En el paso 608, se puede reconocer texto en el archivo de imagen de registro del sitio web que incluye información relacionada con el registro. Por ejemplo, el texto puede reconocerse usando reconocimiento óptico de caracteres, o cualquier otro protocolo conocido por los expertos en la técnica.

En ejemplos, la información segura puede incluir al menos uno de: un dominio de sitio web, un nombre comercial, un nombre de usuario, una contraseña, una sugerencia de contraseña, una pista de contraseña, una pregunta de restablecimiento de contraseña, un icono o una respuesta de restablecimiento de contraseña.

El método 600 puede incluir además el paso 610. En el paso 610, la información segura puede asociarse con un almacén de datos seleccionado de la pluralidad de almacenes de datos a los que se ha autorizado el acceso. El almacén de datos seleccionado puede ser determinado por el usuario.

Esto puede permitir que un usuario ingrese información en un almacén de datos sin necesidad de volver a escribirla. Esto puede permitir que se mantenga información más precisa en un almacén de datos.

El método 600 puede incluir además el paso 612. En el paso 612, se puede mostrar una interfaz de usuario de actualización de almacén de datos que incluye información segura de un almacén seguro seleccionado de la pluralidad de almacenes de datos.

El método 600 puede incluir además el paso 614. En el paso 614, se puede recibir información segura actualizada del usuario desde la interfaz de usuario de actualización del almacén de datos. Por ejemplo, la interfaz de usuario de actualización del almacén de datos puede permitir que un usuario edite la información segura.

El método 600 puede incluir además el paso 616. En el paso 616, la información segura actualizada puede asociarse con el almacén de datos seleccionado.

Los pasos 612, 614 y 616 pueden permitir que un usuario actualice la información mantenida en un almacén de datos.

En ejemplos, los pasos de los métodos 400 y 600 se pueden ejecutar en una aplicación cliente 302. En ejemplos adicionales, sin embargo, los pasos de los métodos 400 y 600 se pueden ejecutar en la aplicación cliente 302 y el servidor de configuración 304.

Por ejemplo, la Figura 12 representa el sistema 1200. El sistema 1200 incluye la aplicación cliente 302 y el servidor de configuración 304.

En ejemplos, al menos una de la pluralidad de información de autenticación personal puede recibirse desde un dispositivo cliente. Por ejemplo, el mensaje 1202 puede enviarse desde la aplicación cliente 302 a la aplicación del servidor de configuración 304, incluida la información de autenticación personal recibida de un usuario.

En ejemplos, al menos una información de autenticación personal de la pluralidad de información de autenticación personal se puede enviar a un servidor, y se puede recibir una confirmación de información de autenticación personal del servidor. Una confirmación de información de autenticación personal es un mensaje que confirma que la información de autenticación personal autentica a un usuario. Por ejemplo, el mensaje 1204 puede enviarse desde la aplicación de servidor 304 a la aplicación de cliente 302.

La Figura 7 representa una realización adicional del método 700 de la solicitud. El método 700 se puede utilizar para configurar el acceso a un almacén de datos estructurados. El método 700 comienza con el paso 702. En el paso 702, se recibe una primera información de configuración de autenticación personal.

Una primera información de configuración de autenticación personal es la información recibida cuando un usuario configura el acceso a un almacén de datos. Por ejemplo, si el almacén de datos de primer nivel requerirá información de autenticación personal de huellas dactilares, la primera información de configuración de autenticación personal 702 incluye datos de huellas dactilares iniciales.

El método 700 continúa con el paso 704. En el paso 704, los primeros datos de autenticación guardados en función de la primera información de configuración de autenticación personal 702 se guardan en un perfil de usuario. Los datos de autenticación guardados son los que se utilizarán para autenticar la información de autenticación personal recibida posteriormente.

En ejemplos, por ejemplo, cuando la información de autenticación es una contraseña, los primeros datos de autenticación guardados pueden ser los mismos que la primera información de configuración de autenticación personal.

En ejemplos adicionales, sin embargo, los primeros datos de autenticación guardados pueden ser diferentes de la primera información de configuración de autenticación personal. Por ejemplo, si la primera información de configuración de autenticación personal 702 incluye una imagen, tal como una imagen de huella dactilar, los primeros datos de autenticación guardados pueden incluir una o más características derivadas de la imagen de huella dactilar. Alternativamente, la primera información de configuración de autenticación personal 702 puede incluir un hash de la imagen.

El perfil de usuario incluye los datos de autenticación guardados, que se pueden utilizar para autenticar a un usuario.

El método 700 continúa con el paso 706. En el paso 706, se recibe una segunda información de configuración de autenticación personal.

El método 700 continúa con el paso 708. En el paso 708, los segundos datos de autenticación guardados en función de la segunda información de configuración de autenticación personal se guardan en el perfil de usuario. Autenticar la primera información de autenticación personal de una pluralidad de informaciones de autenticación para proporcionar acceso a un almacén de datos de primer nivel de la pluralidad de almacenes de datos estructurados incluye usar los primeros datos de autenticación guardados, y autenticar una segunda información de autenticación personal de la pluralidad de informaciones de autenticación para proporcionar acceso a un almacén de datos de segundo nivel de la pluralidad de almacenes de datos estructurados incluye usar los segundos datos de autenticación guardados, después de autenticar la primera información de autenticación personal.

Al permitir que un usuario guarde datos de autenticación personal en un perfil de usuario, es posible configurar el almacén de datos estructurados 500 para que tenga los mismos beneficios discutidos con respecto a las Figuras 4, 5 y 6.

En ejemplos, el método 700 puede incluir pasos adicionales. Por ejemplo, el método 700 puede incluir el paso 710. En el paso 710, se puede recibir una tercera información de configuración de autenticación personal.

El método 700 puede incluir además el paso 712. En el paso 712, la tercera información de configuración de autenticación personal se puede guardar, ya que los terceros datos de autenticación guardados se pueden guardar en el perfil de usuario. La autenticación de la tercera información de autenticación personal de la pluralidad de información de autenticación para proporcionar acceso a un almacén de datos de tercer nivel de la pluralidad de almacenes de datos estructurados puede incluir el uso de los terceros datos de autenticación guardados, después de autenticar la primera información de autenticación personal y la segunda información de autenticación personal.

En ejemplos, el método 700 puede incluir pasos adicionales. Por ejemplo, el método 700 puede incluir cualquiera de los pasos del método 800.

En ejemplos, el método 800 puede incluir los pasos 802 y 804. En el paso 802, se puede recibir una primera información segura.

En el paso 804, la primera información segura puede asociarse con un almacenamiento de datos alfa de la pluralidad de almacenes de datos. Por ejemplo, el almacén de datos alfa puede ser un almacén de datos de primer nivel 502, un almacén de datos de segundo nivel 504 o un almacén de datos de tercer nivel 506.

En ejemplos, el método 800 puede incluir los pasos 806 y 808. En el paso 806, se puede recibir una segunda información segura.

En el paso 808, la segunda información segura puede asociarse con un almacenamiento de datos beta de la pluralidad de almacenes de datos. Por ejemplo, el almacén de datos beta puede ser un almacén de datos de primer nivel 502, un almacén de datos de segundo nivel 504 o un almacén de datos de tercer nivel 506.

En ejemplos, una información de autenticación personal alfa de la pluralidad de información de autenticación personal puede ser un primer dato de tipo biométrico.

En ejemplos, una información de autenticación personal beta de la pluralidad de información de autenticación personal puede ser un segundo dato de tipo biométrico que es diferente de los primeros datos de tipo biométrico.

En ejemplos, una gamma de la pluralidad de información de autenticación personal puede ser un tercer tipo de datos, y el tercer tipo de datos puede ser diferente del primer tipo de datos y el segundo tipo de datos.

En ejemplos, al menos uno de la pluralidad de almacenes de datos estructurados puede incluir datos de autenticación de terceros.

En ejemplos, los datos de autenticación de terceros pueden incluir una contraseña.

En ejemplos, al menos un almacén de datos de la pluralidad de almacenes de datos estructurados puede incluir al menos uno de: un archivo de datos, un número o una cadena de texto.

En ejemplos, la pluralidad de información de autenticación personal puede incluir al menos uno de: datos de huellas dactilares, un código pin, información de grabación de voz, datos de mensajes de voz, información de imágenes faciales, información de imágenes del iris o información de imágenes de la retina.

En ejemplos, el método 700 puede incluir además los pasos 606, 608 y 610 del método 600.

En ejemplos, recibir al menos una de la primera información de confirmación de autenticación personal, la segunda información de confirmación de autenticación personal o una tercera información de confirmación de autenticación personal puede incluir además los pasos 810 y 812 del método 800.

En el paso 810, se puede determinar un período de tiempo de espera de entrada del usuario.

En el paso 812, el período de tiempo de espera de entrada del usuario se puede guardar con el perfil de usuario.

Al proporcionar acceso estructurado a información segura en almacenes de datos estructurados, puede ser posible proporcionar acceso seguro a información de varios niveles de sensibilidad, lo que permite a un usuario sentir que su información está segura y que tiene el control de dónde se guarda.

Si bien la presente invención se ha ilustrado mediante la descripción de las realizaciones de la misma, y si bien las realizaciones se han descrito con considerable detalle, no es la intención del solicitante restringir o limitar de ninguna manera el alcance de las reivindicaciones adjuntas a dicho detalle.

## REIVINDICACIONES

**1.** Un método para proporcionar acceso a una pluralidad de almacenes de datos estructurados basados en una pluralidad de información de autenticación personal, el método comprende: en un sistema de protección de datos estructurado:

recibir una primera información de autenticación personal de la pluralidad de información de autenticación personal de un usuario;
al autenticar la primera información de autenticación personal, proporcionar acceso de usuario a un almacén de datos de primer nivel de la pluralidad de almacenes de datos estructurados, el almacén de datos de primer nivel almacena una pluralidad de pares de nombre de usuario/contraseña, cada par para acceder a un primero de una pluralidad de servidores;
una vez que se proporciona acceso de usuario al almacén de datos de primer nivel, el usuario recupera uno de los pares de nombre de usuario/contraseña en el almacén de datos de primer nivel y accede al primer servidor utilizando el par de nombre de usuario/contraseña;
recibir una segunda información de autenticación personal de la pluralidad de información de autenticación personal del usuario;
al autenticar la segunda información de autenticación personal, y después de autenticar la primera información de autenticación personal, proporcionar acceso de usuario a un almacén de datos de segundo nivel de la pluralidad de almacenes de datos estructurados, el almacén de datos de segundo nivel almacena una pluralidad de pares de nombre de usuario/contraseña, cada par para acceder a un segundo de una pluralidad de servidores;
una vez que se proporciona acceso de usuario al almacén de datos de segundo nivel, el usuario recupera uno de los pares de nombre de usuario/contraseña en el almacén de datos de segundo nivel y accede al segundo servidor utilizando el par de nombre de usuario/contraseña;
recibir una tercera información de autenticación personal de la pluralidad de información de autenticación personal del usuario;
al autenticar la tercera información de autenticación personal, y después de autenticar la primera información de autenticación personal y la segunda información de autenticación personal, proporcionar acceso de usuario a un almacén de datos de tercer nivel de la pluralidad de almacenes de datos estructurados, el almacén de datos de tercer nivel almacena una pluralidad de pares de nombre de usuario/contraseña, cada par para acceder a un tercero de una pluralidad de servidores; y
una vez que se proporciona acceso de usuario al almacén de datos de tercer nivel, el usuario recupera uno de los pares de nombre de usuario/contraseña en el almacén de datos de tercer nivel y accede al tercer servidor utilizando el par de nombre de usuario/contraseña;

en donde la primera, segunda y tercera información de autenticación personal son de diferentes tipos entre sí, en donde los almacenes de datos de primer, segundo y tercer nivel son diferentes entre sí y almacenan diferentes pares de nombre de usuario/contraseña.

**2.** Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en donde una información de autenticación personal alfa de la pluralidad de información de autenticación personal es un primer dato de tipo biométrico.

**3.** Un método como se reivindica en la reivindicación 2, en donde una información de autenticación personal beta de la pluralidad de información de autenticación personal es un segundo dato de tipo biométrico que es diferente de los primeros datos de tipo biométrico.

**4.** Un método como se reivindica en la reivindicación 3, en donde una información de autenticación personal gamma de la pluralidad de información de autenticación personal es un tercer tipo de datos, y el tercer tipo de datos es diferente del primer tipo de datos y el segundo tipo de datos.

**5.** Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en donde al menos uno de la pluralidad de almacenes de datos estructurados incluye datos de autenticación de terceros.

**6.** Un método de acuerdo con la reivindicación 5, en donde los datos de autenticación de terceros incluyen una contraseña.

**7.** Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en donde la pluralidad de información de autenticación personal incluye al menos uno de: datos de huellas dactilares, un código pin, información de grabación de voz, datos de mensajes de voz, información de imágenes faciales, información de imágenes del iris o información de imágenes de la retina.

**8.** Un método como se reivindica en cualquiera de las reivindicaciones anteriores, que comprende además: mostrar una interfaz de usuario de almacén de datos que incluye información segura de al menos un almacén de datos de la pluralidad de almacenes de datos.

**9.** Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en donde recibir al menos una de la pluralidad de información de autenticación personal comprende, además: recibir la al menos una de la pluralidad de información de autenticación personal desde un dispositivo cliente.

**10.** Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en donde la autenticación de la primera información de autenticación personal o la autenticación de la segunda información de autenticación personal comprende, además:

enviar la al menos una información de autenticación personal de la pluralidad de información de autenticación personal a un servidor; y
recibir una confirmación de información de autenticación personal del servidor.

**11.** Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el período de tiempo de espera del usuario se almacena con un perfil de usuario.

**12.** Un método de conformidad con cualquiera de las reivindicaciones anteriores, en donde un tiempo para ingresar la al menos una información de autenticación personal se compara con el período de tiempo de espera de entrada del usuario para determinar la autenticación.

**13.** Un método tal como se reivindica en cualquiera de las reivindicaciones anteriores, que comprende, además: en el sistema estructurado de protección de datos:

recibir una primera información de configuración de autenticación personal;
guardar los primeros datos de autenticación guardados en función de la primera información de configuración de autenticación personal en un perfil de usuario;
recibir una segunda información de configuración de autenticación personal; y
guardar los segundos datos de autenticación guardados en función de la segunda información de configuración de autenticación personal en el perfil de usuario,
recibir una tercera información de configuración de autenticación personal; y
guardar la tercera información de configuración de autenticación personal como terceros datos de autenticación guardados en el perfil de usuario;
en donde la primera información de autenticación personal se autentica utilizando los primeros datos de autenticación guardados, la segunda información de autenticación personal se autentica utilizando los segundos datos de autenticación guardados y la tercera información de autenticación personal se autentica utilizando los terceros datos de autenticación guardados.

**14.** Un sistema estructurado de protección de datos configurado para realizar el método de cualquiera de las reivindicaciones anteriores.

**DIBUJOS**

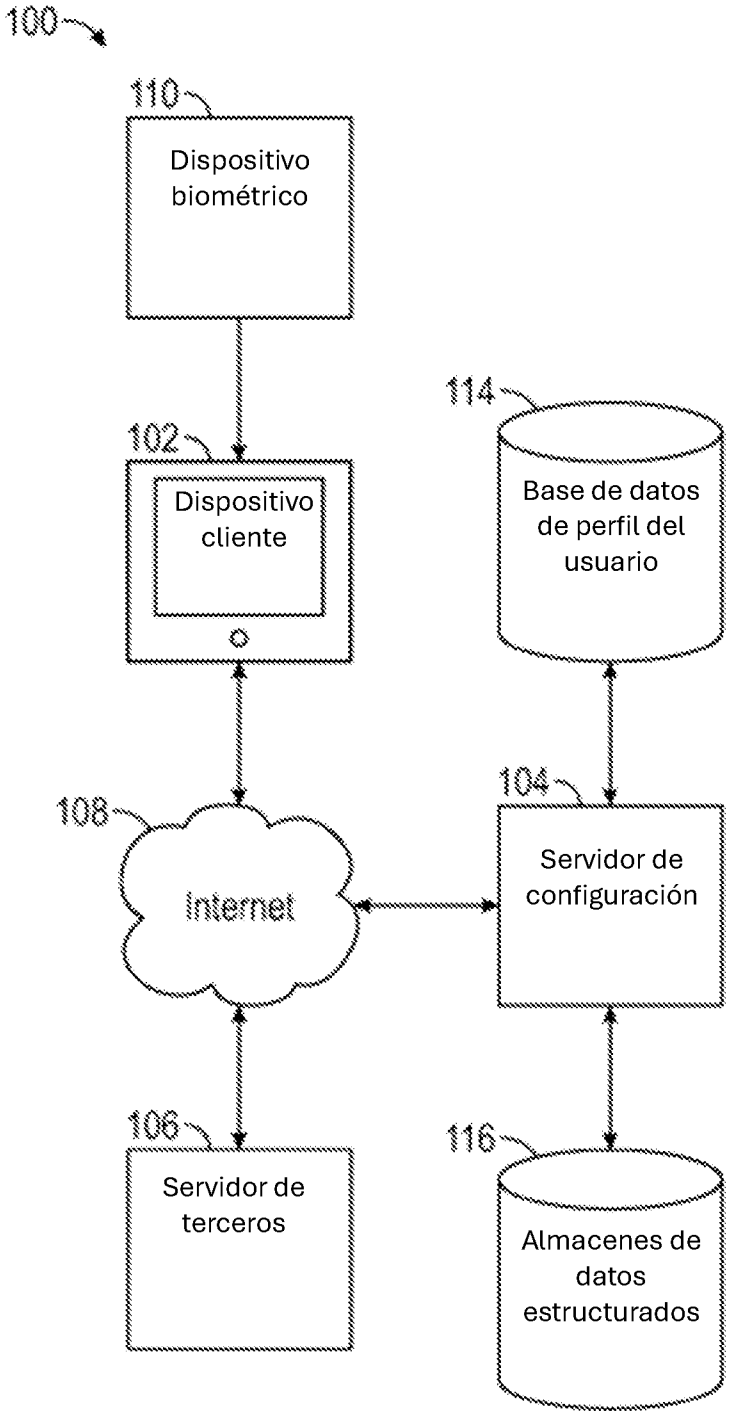


FIG. 1

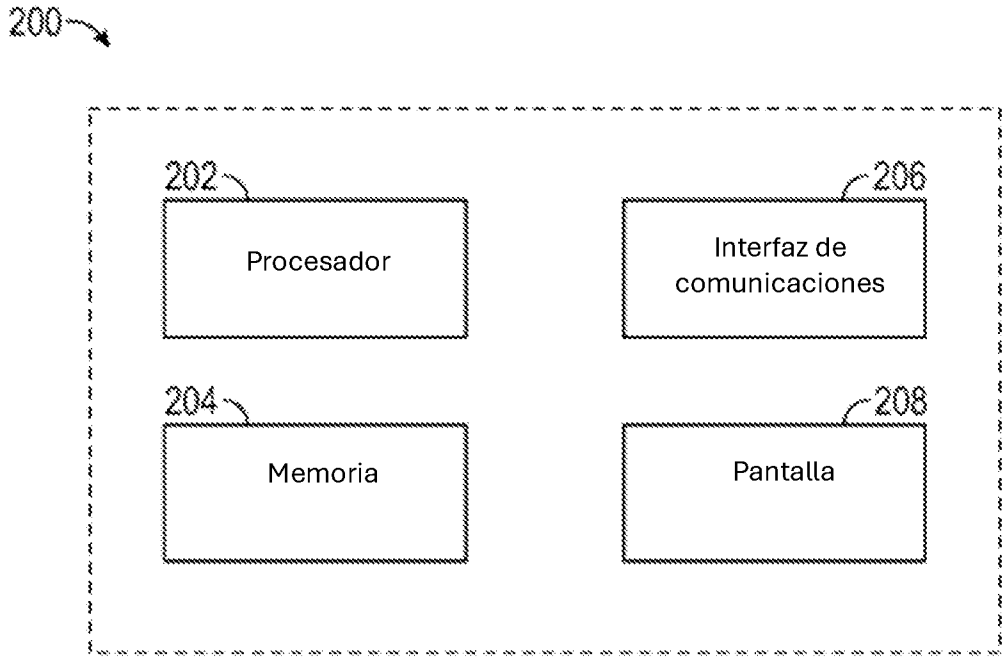
200
202
Procesador
206
Interfaz de comunicaciones
204
Memoria
208
Pantalla

FIG. 2

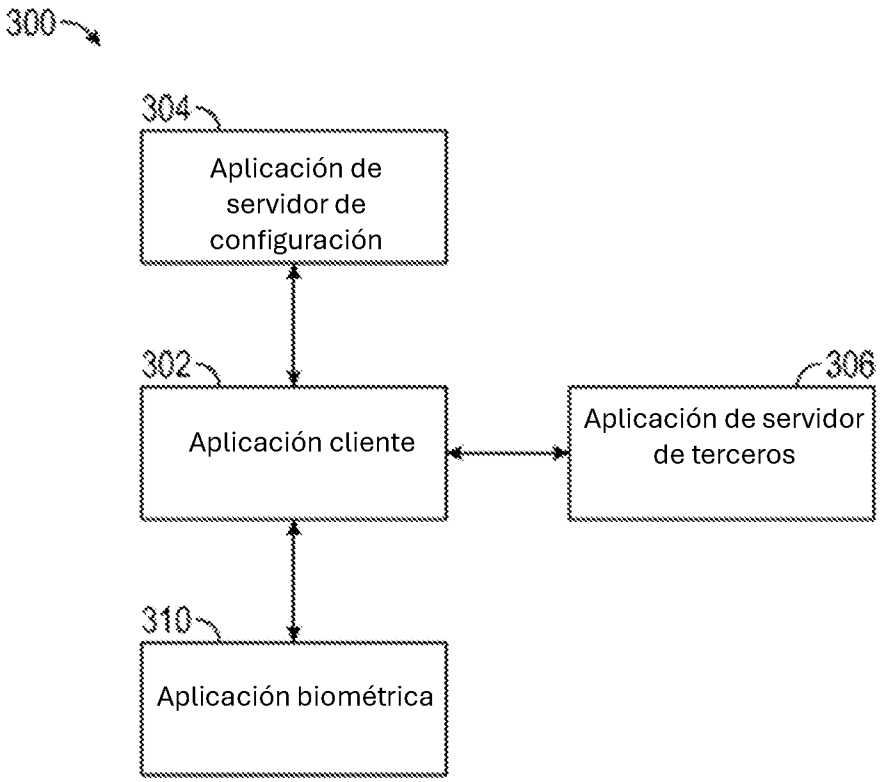
300
304
Aplicación de servidor de configuración
302
Aplicación cliente
306
Aplicación de servidor de terceros
310
Aplicación biométrica

FIG.3

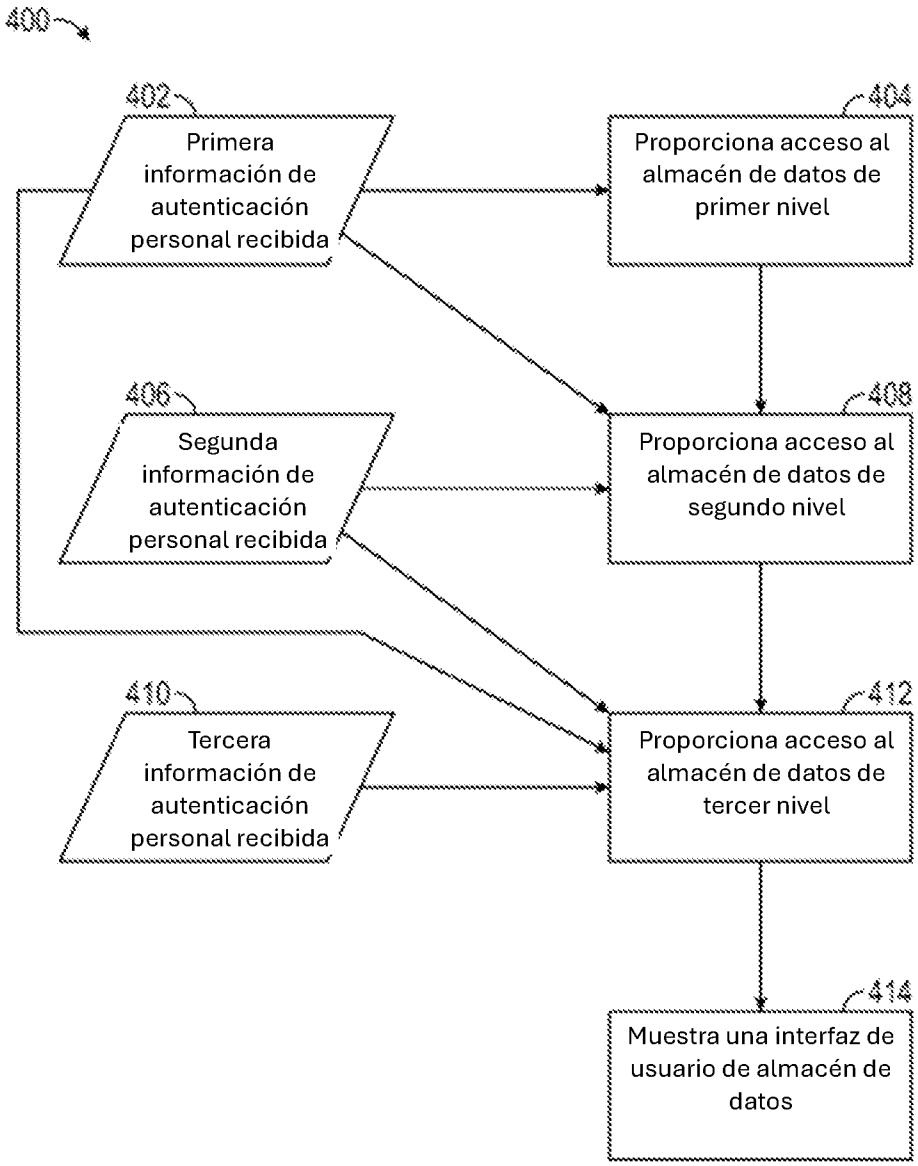
400
402
Primera información de autenticación personal recibida
404
Proporciona acceso al almacén de datos de primer nivel
406
Segunda información de autenticación personal recibida
408
Proporciona acceso al almacén de datos de segundo nivel
410
Tercera información de autenticación personal recibida
412
Proporciona acceso al almacén de datos de tercer nivel
414
Muestra una interfaz de usuario de almacén de datos

FIG. 4

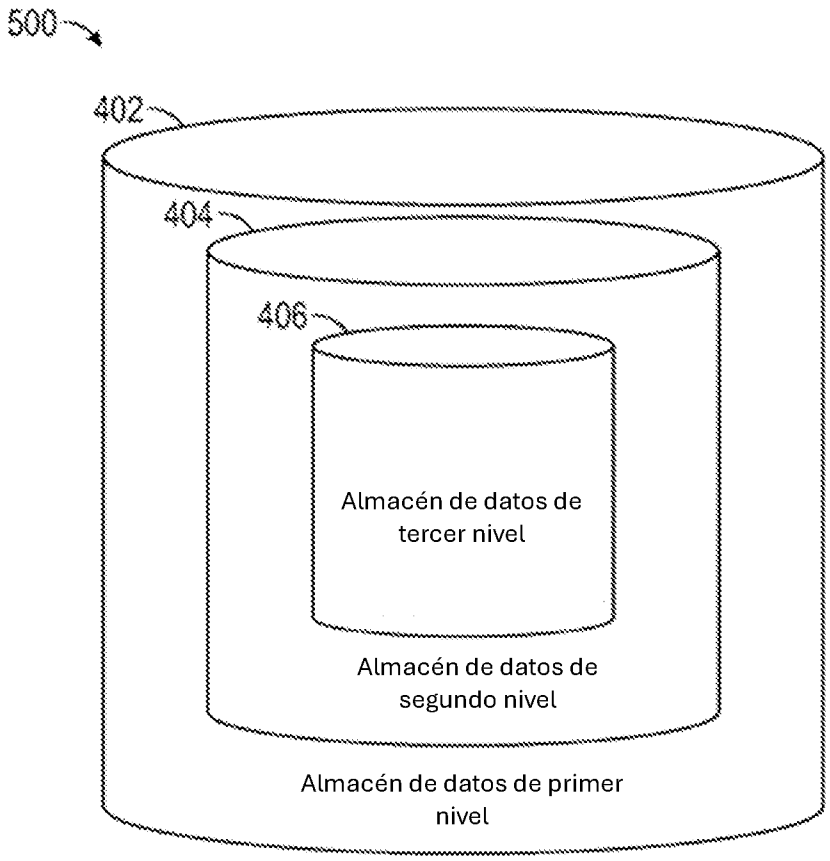
500
402
404
406
Almacén de datos de tercer nivel
Almacén de datos de segundo nivel
Almacén de datos de primer nivel

FIG. 5

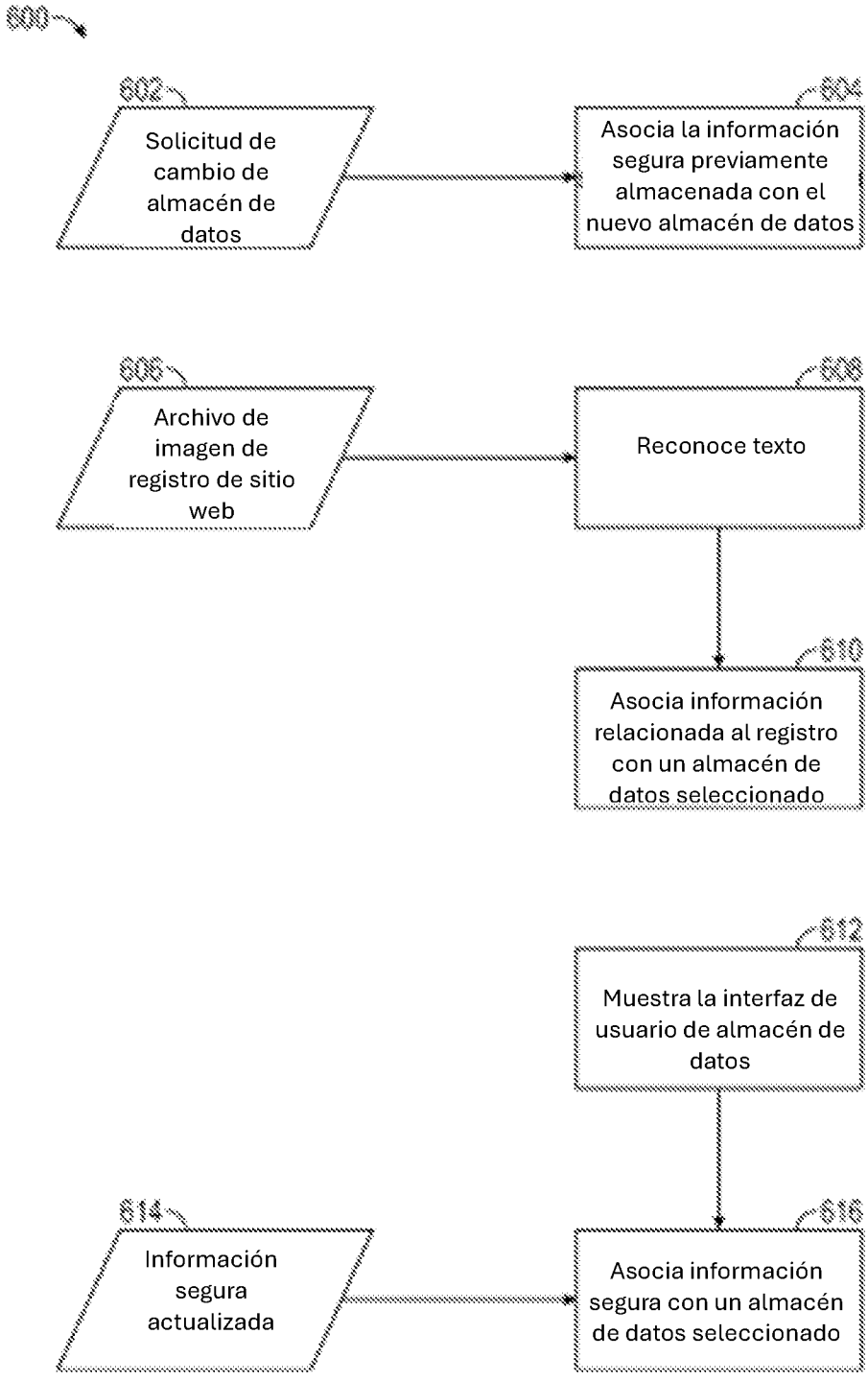
600
602
Solicitud de cambio de almacén de datos
604
Asocia la información segura previamente almacenada con el nuevo almacén de datos
606
Archivo de imagen de registro de sitio web
608
Reconoce texto
610
Asocia información relacionada al registro con un almacén de datos seleccionado
612
Muestra la interfaz de usuario de almacén de datos
614
Información segura actualizada
616
Asocia información segura con un almacén de datos seleccionado

FIG.6

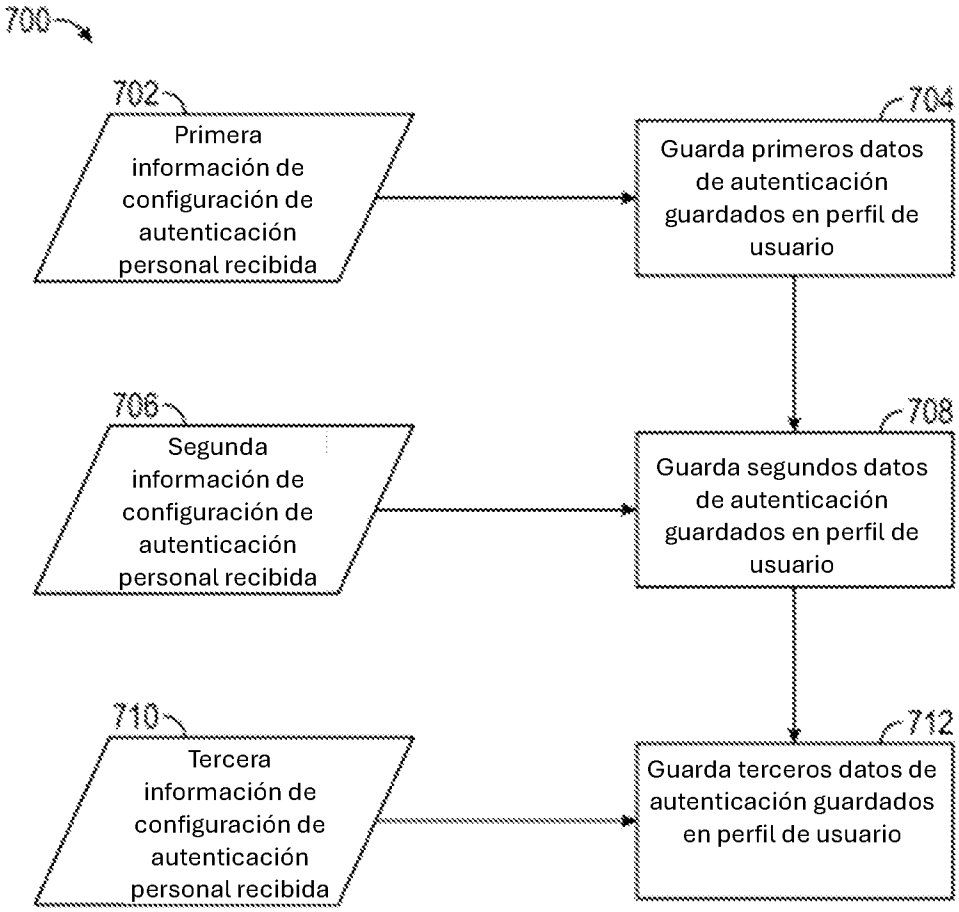
700
702
Primera información de configuración de autenticación personal recibida
704
Guarda primeros datos de autenticación guardados en perfil de usuario
706
Segunda información de configuración de autenticación personal recibida
708
Guarda segundos datos de autenticación guardados en perfil de usuario
710
Tercera información de configuración de autenticación personal recibida
712
Guarda terceros datos de autenticación guardados en perfil de usuario

FIG.7

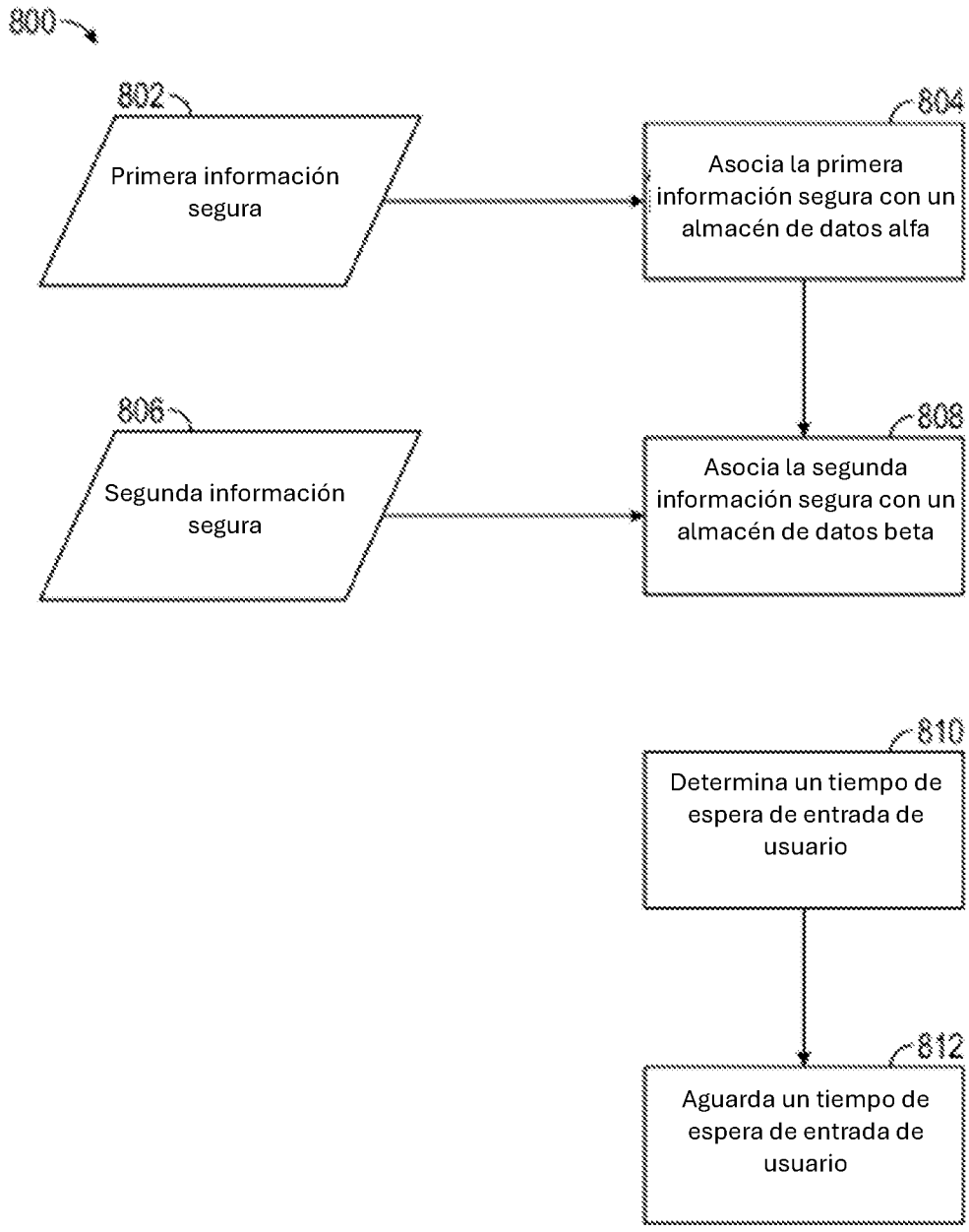
800
802
Primera información segura
804
Asocia la primera información segura con un almacén de datos alfa
806
Segunda información segura
808
Asocia la segunda información segura con un almacén de datos beta
810
Determina un tiempo de espera de entrada de usuario
812
Aguarda un tiempo de espera de entrada de usuario

FIG. 8

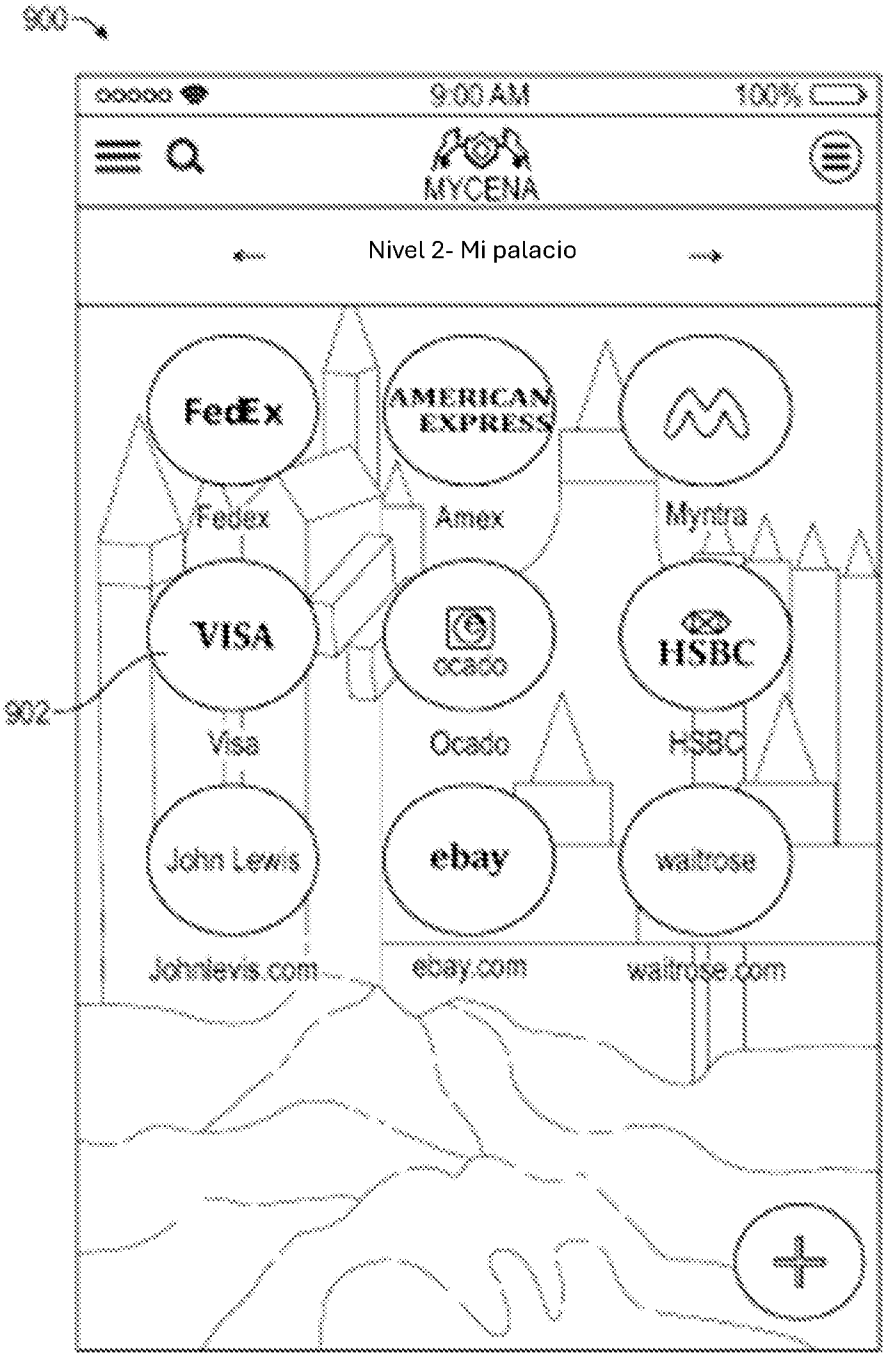
900
9:00 AM
100%
MYCENA
Nivel 2- Mi palacio
FedEx
Fedex
AMERICAN EXPRESS
Amex
Myntra
VISA
Visa
ocado
Ocado
HSBC
HSBC
John Lewis
Johnlewis.com
ebay
ebay.com
waitrose
waitrose.com
902

FIG. 9

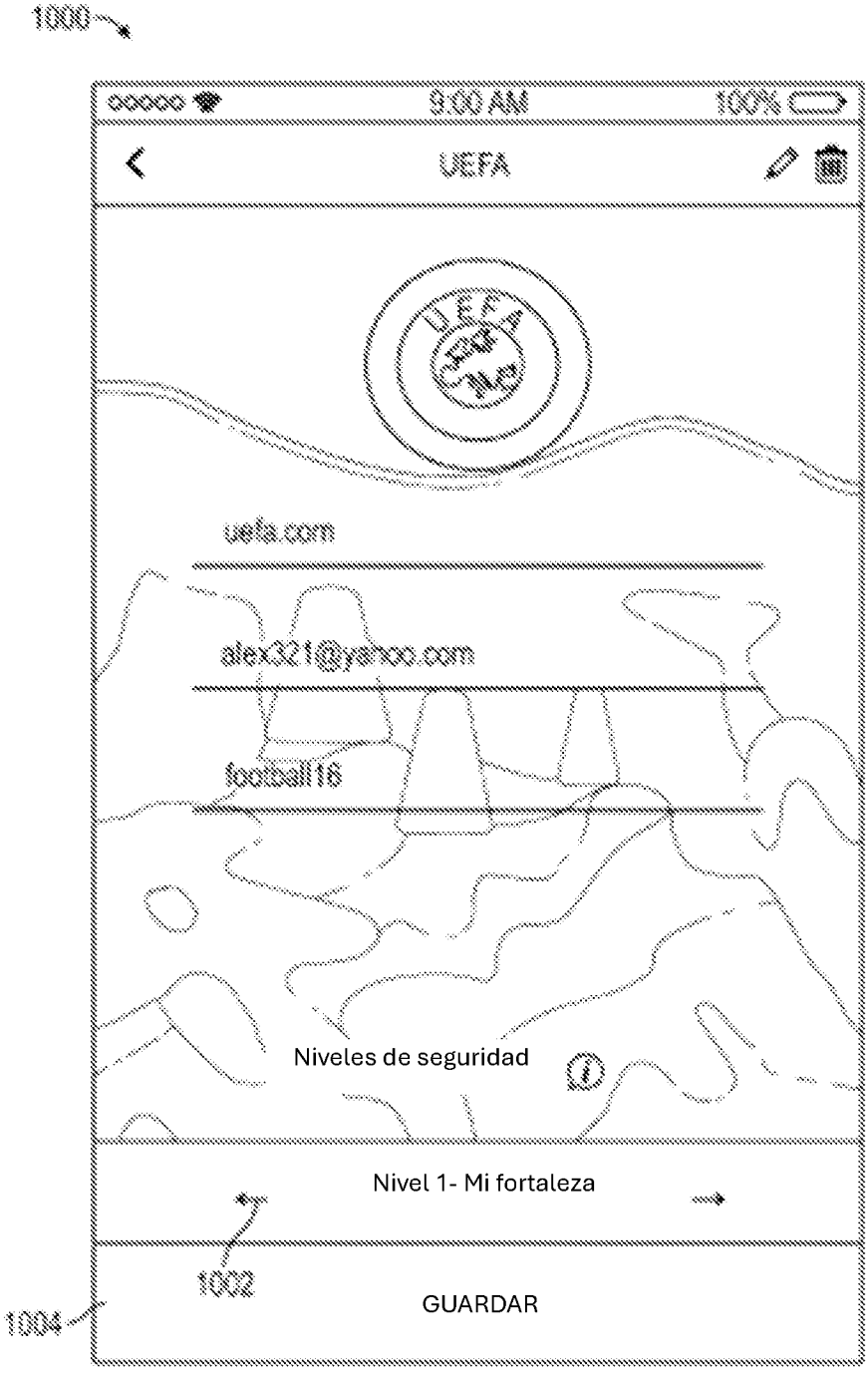
1000
9:00 AM
100%
UEFA
uefa.com
alex321@yahoo.com
football16
Niveles de seguridad
Nivel 1- Mi fortaleza
1002
GUARDAR
1004

FIG. 10

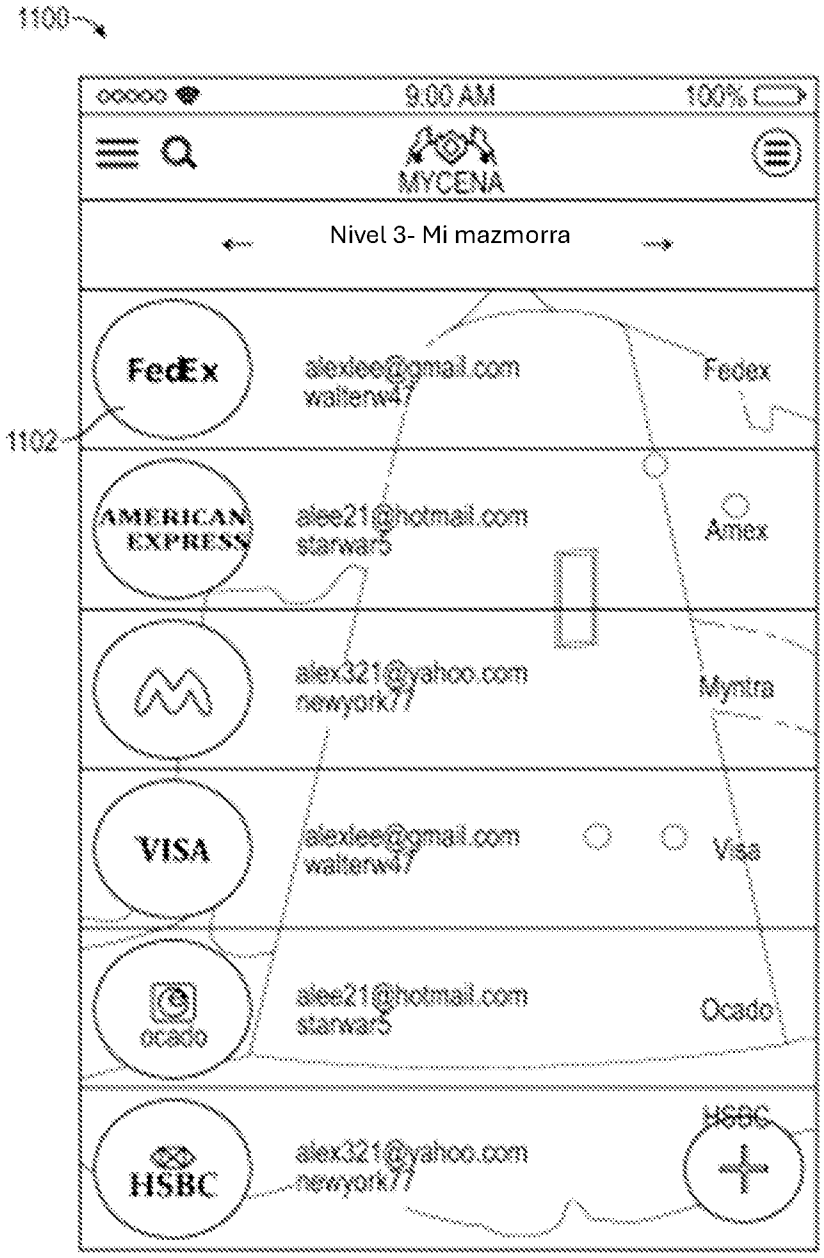
1100
9:00 AM
100%
MYCENA
Nivel 3- Mi mazmorra
1102
FedEx
alexlee@gmail.com
walleru47
Fedex
AMERICAN EXPRESS
alee21@hotmail.com
starwar3
Amex
alex321@yahoo.com
newyork77
Myntra
VISA
alexlee@gmail.com
walleru47
Visa
ocado
alee21@hotmail.com
starwar3
Ocado
HSBC
alex321@yahoo.com
newyork77
HSBC

FIG. 11

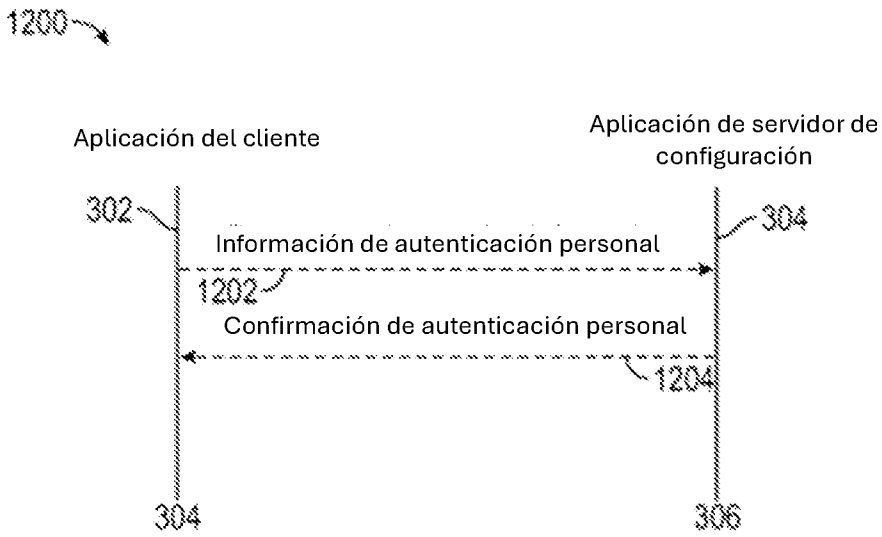
1200
Aplicación del cliente
Aplicación de servidor de configuración
302
304
Información de autenticación personal
1202
Confirmación de autenticación personal
1204
304
306

FIG. 12