(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 929 974**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/45 (2013.01)
G06F 21/44 (2013.01)
G06F 21/32 (2013.01)
H04W 12/06 (2011.01)
H04W 12/04 (2011.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.08.2016 PCT/AU2016/000275**

(87) Fecha y número de publicación internacional: **16.02.2017 WO17024335**

(96) Fecha de presentación y número de la solicitud europea: **12.08.2016 E 16834301 (0)**

(97) Fecha y número de publicación de la concesión europea: **03.08.2022 EP 3335142**

(54) Título: **Sistema de autenticación de dispositivo**

(30) Prioridad:

12.08.2015 AU 2015903231

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.12.2022

(73) Titular/es:

HAVENTEC PTY LTD (100.0%)
Level 27 1 Market Street
Sydney, NSW 2000, AU

(72) Inventor/es:

RICHARDSON, RIC, B.

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema de autenticación de dispositivo

Antecedentes

A lo largo de los años se han hecho muchos esfuerzos por simplificar el procedimiento de autenticación de la identidad de una persona. Un sistema, conocido como oAuth, permite a una persona autenticarse con un sitio pero luego compartir esas credenciales de autenticación con otros sitios y servicios usando tokens que caducan con el tiempo.

Una ventaja clave de esta estrategia es que es posible que solo se requiera que una persona autentique su identidad con un sitio, pero tenga acceso a varios sitios sin la inconveniencia de configurar y someterse a un procedimiento de autenticación aparte para cada sitio.

Una desventaja de este sistema es que normalmente no es posible usar la misma estrategia para autenticar a los usuarios que se conectan desde diferentes dispositivos al tiempo que usan la misma cuenta.

Si bien existen mecanismos conocidos para que un usuario comparta datos entre múltiples dispositivos digitales, tal como, por ejemplo, se describe en los documentos US 2011/0138018 a QUALCOMM Incorporated, actualmente no existe ningún mecanismo para que ese usuario provoque la autenticación consecuente en función de una autenticación inicial en un primer dispositivo.

Esta capacidad sería muy deseable en el sentido de que una autenticación en uno de los dispositivos de usuario para una cuenta de sitio podría usarse en múltiples dispositivos que el usuario tiene o usa.

Las realizaciones de la presente invención buscan abordar este problema o al menos proporcionar una alternativa útil.

El documento US 2007/136573 a Steinberg divulga ampliamente un sistema y un procedimiento de uso de dos o más mecanismos de autenticación de múltiples factores para autenticar partes en línea. El énfasis está en el uso de dos o más mecanismos de autenticación de múltiples factores.

El documento EP 2873192 describe procedimientos y sistemas para usar credenciales derivadas para autenticar un dispositivo en múltiples plataformas. El énfasis está en el uso de credenciales derivadas para autenticar un dispositivo en múltiples plataformas.

Notas

El término "que comprende" (y variaciones gramaticales de este) se usa en esta memoria descriptiva en el sentido inclusivo de "que tiene" o "que incluye", y no en el sentido exclusivo de "que consiste solo en '.

La discusión antes vista de la técnica anterior en los Antecedentes de la invención, no es una admisión de que cualquier información discutida en la misma sea citable en la técnica anterior o parte del conocimiento general común de los expertos en la materia en cualquier país.

Breve Descripción de la Invención

Definiciones:

Autenticación: En esta memoria descriptiva, autenticación se usa en el sentido de tomar medidas para identificar aún más un inicio de sesión de usuario, por lo general, pero no exclusivamente, en un entorno de servidor de cliente. Ejemplos de etapas incluyen el requisito de enviar un código de acceso que se ha identificado previamente como asociado con el inicio de sesión de usuario. En otras formas no exclusivas, se pueden requerir datos biométricos para llevar a cabo la etapa para identificar adicionalmente un inicio de sesión de usuario. La autenticación se establece a nivel de software, ya que implica necesariamente un nivel de selectividad en cuanto a qué datos o categorías de datos están disponibles para la comunicación posterior a la autenticación.

Confianza: En esta memoria descriptiva, confianza se refiere a una relación que puede establecerse entre dos dispositivos digitales con el fin de transmitir datos entre ellos. La confianza puede estar a nivel de hardware.

Las reivindicaciones adjuntas definen el alcance de protección. Cualquier ejemplo y descripción técnica de aparatos, productos y/o procedimientos en la descripción y/o dibujos no cubiertos por las reivindicaciones se presentan no como realizaciones de la invención, sino como técnica o ejemplos útiles para comprender la invención. Por consiguiente, en

una forma amplia de la invención, se proporciona un procedimiento de autenticación de un usuario con respecto a más de un dispositivo digital; dicho usuario tiene una cuenta en un servidor; dicho procedimiento comprende

a. el usuario efectúa una secuencia de inicio de sesión y una secuencia de autenticación en un primer dispositivo digital como se hace referencia y se registra en el servidor para autenticar así al usuario con respecto al primer dispositivo digital;
b. el usuario efectúa posteriormente una secuencia de inicio de sesión en un segundo dispositivo digital; el segundo dispositivo digital comunica la secuencia de inicio de sesión del usuario al servidor;
c. el servidor comunica una opción al segundo dispositivo digital para usar el primer dispositivo digital para efectuar la autenticación del usuario con respecto al segundo dispositivo digital;

d. tras la recepción de una solicitud del segundo dispositivo digital para efectuar la autenticación mediante el uso del primer dispositivo digital:
i. el servidor emite una ID única temporal para el segundo dispositivo digital;
ii. el servidor envía una solicitud de autenticación al primer dispositivo digital;
iii. la solicitud de autenticación incluye la transmisión de la ID única temporal emitida al segundo dispositivo digital;
iv. comunicar la ID única temporal desde el primer dispositivo digital al usuario para permitirle así al usuario determinar si está de acuerdo con la solicitud de autenticación;
v. el usuario comunica estar de acuerdo o de otro modo mediante comunicación efectuada desde el primer dispositivo digital al servidor.

En aun una forma amplia adicional de la invención, se proporciona un procedimiento para autenticar una sesión de usuario instigada por un usuario en un dispositivo digital con respecto a una identidad de inicio de sesión de usuario dada en un servidor; dicho procedimiento comprende:

a. autenticar un primer dispositivo digital para una primera identidad de inicio de sesión de usuario tal como se registra en el servidor;
b. comprometerse así a transferir datos protegidos entre el primer dispositivo digital y el servidor;
c. posteriormente autenticar un segundo dispositivo digital para dicha primera identidad de inicio de sesión de usuario tal como se registra en dicho servidor mediante las etapas de:
d. dicho usuario ingresa dicha primera identidad de inicio de sesión de usuario en dicho segundo dispositivo digital;
e. dicho segundo dispositivo digital es emitido por dicho servidor con un identificador temporal en respuesta a que dicho usuario ingrese dicha primera identidad de inicio de sesión de usuario en dicho segundo dispositivo digital;
f. dicho servidor a continuación transmite dicho identificador temporal a dicho primer dispositivo digital para comunicarse con dicho usuario mediante dicho primer dispositivo digital;
g. dicho usuario responde a dicha comunicación de dicho identificador temporal a dicho usuario mediante dicho primer dispositivo digital haciendo que dicho primer dispositivo digital comunique un comando de autorización de dicho segundo dispositivo digital a dicho servidor si se cumple una condición de respuesta;

por el cual se autoriza dicha primera identidad de inicio de sesión de usuario para dicho segundo dispositivo digital.

En aun otra forma amplia de la invención, se proporciona en un entorno donde un primer dispositivo puede comunicarse con un servidor sujeto a autenticación del dispositivo con respecto al servidor, un procedimiento de autenticación de un segundo dispositivo con respecto al servidor; dicho procedimiento comprende:

a. Previa solicitud, el servidor comunica un identificador al segundo dispositivo y al primer dispositivo;
b. Autenticar el segundo dispositivo al mismo nivel que el primer dispositivo sujeto a un etapa de confirmación.

En aun otra forma amplia de la invención, se proporciona un aparato para realizar la autenticación de al menos un segundo dispositivo con respecto a un entorno de servidor donde se ha realizado la autenticación de un primer dispositivo; el aparato incluye:

a. Una memoria que almacena al menos un primer identificador de inicio de sesión y un elemento de datos de autenticación asociados
b. Un procesador que genera un identificador temporal como una primera etapa para efectuar la autenticación de al menos el segundo dispositivo
a. Un transmisor que transmite el identificador temporal a al menos un segundo dispositivo y al primer dispositivo.
b. Un dispositivo de comparación que compara el identificador temporal del primer dispositivo y del segundo dispositivo y toma una decisión basada en la comparación en cuanto a si permite que el servidor autentique el segundo dispositivo con respecto al entorno del servidor.

Preferentemente, dicha condición de respuesta es una comparación positiva del identificador temporal comunicado por dicho primer dispositivo digital con el identificador temporal comunicado a dicho segundo dispositivo digital por dicho servidor.

Preferentemente, el identificador temporal es una secuencia alfanumérica.

Preferentemente, los datos protegidos son datos almacenados con respecto a dicho primer inicio de sesión de usuario en dicho servidor.

Preferentemente, los datos protegidos son datos de aplicación almacenados con respecto a dicho primer inicio de sesión de usuario en dicho servidor.

Preferentemente, la autenticación de dicho primer dispositivo digital se efectúa mediante la entrada de un identificador de inicio de sesión de usuario y datos de autenticación separados en dicho primer dispositivo digital.

Preferentemente, dichos datos de autenticación separados son una contraseña.

Preferentemente, dichos datos de autenticación separados son datos biométricos.

Preferentemente, la etapa de confirmación comprende comparar el identificador en el segundo dispositivo y el identificador en el primer dispositivo.

Preferentemente, la confirmación se efectúa si, y solo si, el identificador en el segundo dispositivo se corresponde con el identificador en el primer dispositivo

Preferentemente, el identificador es una secuencia alfanumérica.

Preferentemente, se puede establecer la autenticación para una sola sesión.

Preferentemente, la autenticación se puede establecer para un número limitado de sesiones

Preferentemente, la autenticación se puede establecer por un período indefinido

En aun otra forma amplia de la invención, se proporcionan medios codificados con código que, cuando son ejecutados por un procesador, realizan el procedimiento como se describió anteriormente.

Breve descripción de los dibujos

Las realizaciones de la presente invención se describirán ahora con referencia a los dibujos, donde:

Figura 1A - Ilustra un sistema de establecimiento de confianza de hardware de la técnica anterior.
Figura 1B - Ilustra los componentes principales de una realización de ejemplo.
La Figura 2 es un diagrama de flujo de las etapas efectuadas por el ejemplo de la Figura 1B.
La Figura 3 es un diagrama de bloques que ilustra la interacción entre un primer dispositivo digital y un segundo dispositivo digital operable según una realización del sistema de la presente invención.
La Figura 4 es un diagrama de bloques de la interacción de la Figura 3 como experimentada por parte de un usuario.

Descripción y Operación Detalladas

La Figura 1A ilustra esquemáticamente una disposición "Bluetooth" de la técnica anterior para establecer una conexión de datos entre dos dispositivos suficiente para establecer un nivel básico de confianza. Este sistema funciona directamente entre dos dispositivos y, en esencia, es un mecanismo para garantizar que los dos dispositivos entre los que se desea la comunicación se identifiquen inequívocamente con el fin de proporcionar confianza a nivel de hardware.

Realizaciones de la presente invención buscan proporcionar la capacidad de autenticar un segundo o más dispositivos con respecto a un entorno de servidor que depende de que la autenticación se haya establecido primero para un primer dispositivo con respecto al mismo entorno de servidor. En formas preferidas, pero no exclusivamente, el entorno del servidor se define por medio del inicio de sesión de usuario.

La Figura 1B describe los componentes principales de una realización de ejemplo de la presente invención.

Inicialmente, un usuario 10 establecería una conexión autenticada con un servidor 11 habilitado con la realización de ejemplo usando procedimientos de autenticación conocidos en la técnica.

Para autenticar al usuario 10 y el primer dispositivo digital del usuario 12, en este caso un teléfono inteligente, el usuario usa una aplicación habilitada para la web 17 para registrarse con el servidor 11. En este caso, este dispositivo 12 se registraría como el dispositivo de referencia o de confirmación principal de usuario.

La identidad 14 del dispositivo 12 se almacena con la cuenta de usuario 13 y se puede hacer referencia a la misma en el futuro cuando el usuario requiera dispositivos adicionales que tiene o usa para ser autenticado con el servidor 11.

La cuenta de usuario 13 también incluye una ID de cuenta o nombre o nombre de usuario 16 que se puede usar para identificar y nombrar de forma única al usuario de la cuenta.

Cuando el usuario 10 desea autenticarse usando un nuevo dispositivo 15, el usuario conecta el dispositivo 15 al servidor 11 a través de una red pública tal como la Internet 20 usando una aplicación tal como un navegador web 16 y luego ingresa su nombre de cuenta 16 para identificarse como el usuario 10 al servidor 11.

Luego, el servidor 11 notifica al usuario 10 que su segundo dispositivo aún no se reconoce como un dispositivo autenticado y le pregunta al usuario 10 si desea agregar el dispositivo a su cuenta 13.

Tras acordar proceder, al usuario se le presenta un botón para iniciar una solicitud desde el servidor 11 al dispositivo de confirmación principal del usuario 12 para verificar una conexión autenticada entre el usuario 10 y el servidor 11. Al usuario también se le presenta una identificación de dispositivo tal como un número de cuatro dígitos 18 que se puede usar para identificar el dispositivo.

Posteriormente, el segundo dispositivo digital 15 muestra una pantalla 21 que explica al usuario que necesitará obtener la autenticación de su dispositivo de confirmación para proceder con la autenticación de su nuevo dispositivo 15. También se les mostrará la ID temporal 21 preferentemente en forma de un número de cuatro dígitos que se genera nuevo cada vez que un nuevo dispositivo solicita la autenticación. Este número de cuatro dígitos es generado por el servidor 11 y se usa una vez para identificar el dispositivo solicitante 15 al dispositivo de confirmación 12 cuando se realiza una solicitud de autenticación.

El nuevo dispositivo 15 luego entra en un modo de espera para recibir una verificación de autenticación desde el servidor 11 después de que se haya usado el dispositivo de confirmación 12 para verificar su identidad.

Al mismo tiempo, se solicita al servidor 11 que inicie una conexión con el primer dispositivo de confirmación digital primario del usuario 12 para verificar y autorizar la solicitud de autenticación de usuario.

En el caso de un teléfono inteligente tal como un iPhone de Apple, se puede enviar un mensaje de notificación al dispositivo de usuario 12, que, a su vez, puede abrir la aplicación de usuario 17 para verificar la identidad del usuario.

Si la conexión de la aplicación 17 al servidor 11 es actual y no caducó, se muestra al usuario el número de cuatro dígitos que identifica el dispositivo solicitante y se le pide al usuario en la pantalla que autorice el nuevo dispositivo después de verificar la identidad del nuevo dispositivo.

Si la conexión de la aplicación 17 al servidor 11 no es actual y no ha caducado, se le pide al usuario que se autentique usando el dispositivo de confirmación 12. Posteriormente, se muestra al usuario el número de cuatro dígitos que identifica al dispositivo solicitante y se le pide al usuario en la pantalla que autorice el nuevo dispositivo después de verificar la identidad del nuevo dispositivo.

Una vez que el servidor 11 recibe una verificación de la identidad del nuevo dispositivo 15, el servidor permite que una sesión autenticada proceda entre el nuevo dispositivo 15 y el servidor 11.

La pantalla del nuevo dispositivo 15 notifica al usuario que la autenticación se ha completado con éxito y el acceso al sitio está habilitado. Adicionalmente, se añade una nueva identidad de dispositivo 19 a la cuenta del usuario 13 en el servidor 11.

La Figura 2 describe un procedimiento de control de ejemplo de la realización de ejemplo. El procedimiento implica que un usuario 40 utilice un dispositivo inicial, un servidor 41 con el cual el usuario desea conectarse y un segundo dispositivo 42 que el usuario desea autenticar con su cuenta en el servidor.

Inicialmente, un usuario establece una cuenta autenticada con el servidor 43 y el servidor almacena los detalles de la cuenta para autenticación futura 44.

Posteriormente, un usuario puede solicitar que un nuevo dispositivo sea autenticado por el usuario 45 para usar la misma cuenta en el servidor. Para identificarse con el servidor, el usuario introduce su nombre de usuario 46 y lo envía para su uso por el servidor.

El servidor luego confirma que el nombre de usuario es conocido, pero reconoce que el dispositivo que está siendo usado por el usuario no es conocido por el servidor 47. A continuación, el servidor le pregunta al usuario si desea usar las credenciales de autenticación de un dispositivo 48 existente para confirmar que el nuevo dispositivo es reconocido con la cuenta. Si el usuario está de acuerdo 49, entonces el servidor le da al dispositivo solicitante una identidad única temporal 50 que luego se muestra al usuario en la pantalla del nuevo dispositivo 51. El nuevo dispositivo luego pasa a un modo de espera 53 hasta que se responda a la solicitud de recibir una autenticación.

El servidor 41 luego envía una solicitud de autenticación 52 para el nuevo dispositivo al dispositivo de confirmación 40 que ya está autenticado y en uso o puede usar credenciales de autenticación existentes para establecer y autenticar y la identidad de los usuarios.

El dispositivo existente recibe la solicitud de autenticación junto con la identidad del dispositivo solicitante 54. Esta etapa es importante porque permite al usuario identificar correctamente el dispositivo que se está usando para solicitar una nueva autenticación.

El usuario luego confirma la identidad del dispositivo solicitante y permite que proceda la autenticación del nuevo dispositivo 55. Posteriormente, el servidor recibe la autorización para autenticar al usuario en el nuevo dispositivo 56 y el servidor comparte las credenciales de autenticación con el nuevo dispositivo 57.

Como resultado, el nuevo dispositivo recibe las credenciales de autenticación 58 y se permite que el nuevo dispositivo se utilice para acceder a la cuenta de usuario desde el nuevo dispositivo 59.

El resultado es un sistema de autenticación que permite que las credenciales autenticadas de un dispositivo conocido se compartan con un nuevo dispositivo para permitirle acceder a la misma cuenta y recursos.

Las Figuras 3 y 4 son diagramas de bloques que ilustran la interacción entre un primer dispositivo digital y un segundo dispositivo digital operable según una realización del sistema de la presente invención.

Con referencia a la Figura 3, donde los componentes similares están numerados como para realizaciones anteriores, excepto en la serie 100, se muestra un primer dispositivo digital 112 (ID 0) en comunicación con un servidor 111, por lo que un usuario 110 puede "iniciar sesión" a través de una aplicación que se ejecuta en el dispositivo digital 112 a una cuenta de usuario 113 en el servidor 111. Para que los datos o aplicaciones asociados con la cuenta de usuario 113 se comuniquen al dispositivo digital 112, el inicio de sesión de usuario debe ser autenticado por el servidor 111. En este caso, la etapa de autenticación es proporcionada por el usuario que ingresa un nombre de usuario 123 y una contraseña asociada 124. Si estos se corresponden, entonces se ha producido la autenticación y una sesión de usuario puede funcionar entre el primer dispositivo digital 112 y el servidor 111.

De acuerdo con una realización de la presente invención, si el usuario desea autenticar un segundo dispositivo digital 115 (ID 1) con respecto a la misma cuenta de usuario 113, esto puede efectuarse ingresando el mismo nombre de usuario 123 en una aplicación en un segundo dispositivo digital 115 para activar así una secuencia de inicio de sesión en el servidor 111.

Tal como se ilustra en la Figura 4, en uso, se puede pedir al usuario que elija si autenticarse a través de otro dispositivo, por ejemplo, a través de la casilla de selección 125.

En el caso de que el usuario elija autenticarse a través de otro dispositivo, el servidor 111 genera y emite una ID temporal 121 al segundo dispositivo digital 115. La ID temporal 121 luego se muestra en el segundo dispositivo digital 115 o se pone a disposición de otro modo para comunicación al usuario suficiente para que el usuario verifique el ID temporal 121 que se ha emitido para el segundo dispositivo digital 115.

Al mismo tiempo, posteriormente, el servidor 111 emite la misma ID temporal 121 al primer dispositivo digital

112. Nuevamente, el primer dispositivo digital 112 hace que la ID temporal 121 se muestre en el primer dispositivo digital 112 o que de otro modo esté disponible para comunicación al usuario suficiente para que el usuario verifique la ID temporal 121 que se ha emitido para el primer dispositivo digital 112.

Durante el uso, el usuario luego se coloca en una posición donde luego puede comparar la ID temporal 121 que aparece en o está asociada de otro modo con el segundo dispositivo digital 115 con la ID temporal 121 que aparece en o está asociada de otro modo con el primer dispositivo digital 112 durante un período de tiempo predeterminado. En una forma, si las dos ID temporales se corresponden, entonces se puede confirmar al primer dispositivo digital 112 que se ha producido una correspondencia y activar, mediante la casilla de verificación de elección 126, la transmisión de una señal de autorización 127 desde el primer dispositivo digital 112 al servidor 111.

Tras la recepción de la señal de autorización 127, el servidor hace que el inicio de sesión en el segundo dispositivo digital 115 se trate como autenticado, lo que permite al usuario acceder a los datos y servicios bajo esa cuenta de usuario de inicio de sesión 113 en el servidor 111.

Realizaciones alternativas

La realización de ejemplo muestra la confirmación de una autenticación que se produce entre un ordenador personal y un teléfono inteligente con el teléfono inteligente como dispositivo de confirmación. Una realización alternativa podría permitir que cualquier dispositivo que el usuario tenga u opere responda por cualquier dispositivo que el usuario desee agregar a su cuenta.

La realización de ejemplo usa un número de cuatro dígitos para identificar el dispositivo que solicita la autenticación. Una realización alternativa podría usar cualquier procedimiento para identificar el dispositivo solicitante de tal manera que garantice que un usuario del dispositivo de confirmación pueda estar razonablemente satisfecho en cuanto a la identidad del dispositivo solicitante.

La realización de ejemplo no especifica cómo la sesión autenticada entre el servidor y el

dispositivo de confirmación se comparte con el nuevo dispositivo. Una realización alternativa podría usar un token o una clave de sesión. En aun otra realización alternativa, datos de autenticación reales del dispositivo de confirmación podrían usarse en parte o por duplicado como un medio para permitir que un nuevo dispositivo establezca sus propias credenciales de autenticación. Por ejemplo, si se usó un PIN para autenticar un dispositivo de confirmación, entonces se podría usar un sistema que use el mismo PIN en el nuevo dispositivo para establecer las nuevas credenciales de autenticación.

La realización de ejemplo muestra un nuevo dispositivo que está siendo autenticado por un dispositivo previamente registrado para una sesión segura. Una realización alternativa podría permitir que se produzca la autenticación para su uso en una sesión única, un número limitado de sesiones o período de tiempo, o indefinidamente de forma permanente.

REIVINDICACIONES

1. Un procedimiento llevado a cabo por un servidor (41, 111) para autenticar un segundo dispositivo (42,115) que comprende:

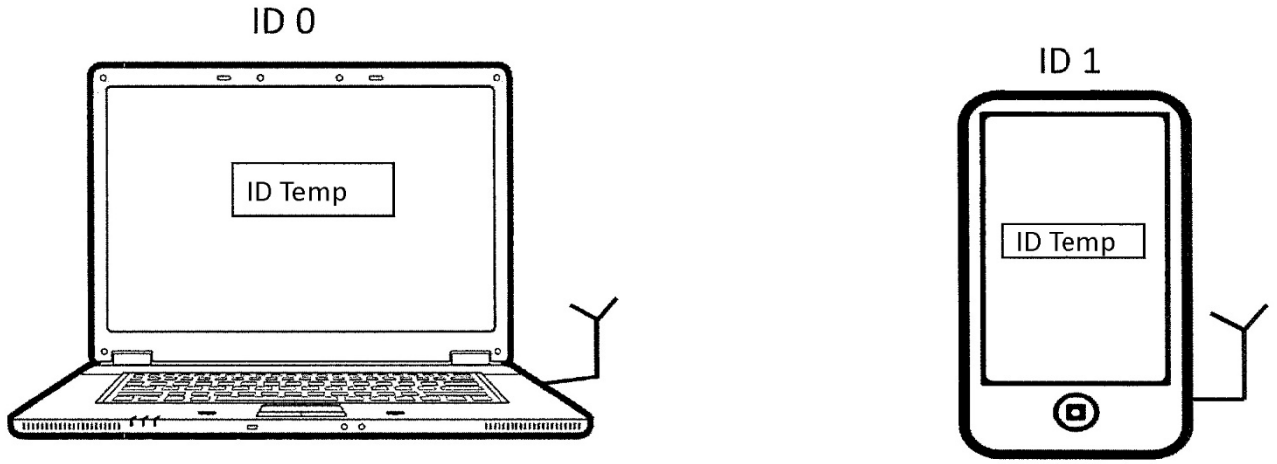
- recibir, desde un primer dispositivo (40, 112) que tiene una primera identidad de dispositivo, una solicitud para establecer una cuenta de usuario autenticada (113);
- almacenar los detalles de la cuenta de usuario que comprende la primera identidad de dispositivo y un nombre de usuario (123);
- recibir, del segundo dispositivo (42, 115), una solicitud para autenticar el segundo dispositivo (42, 115) para usar la cuenta de usuario (113), donde la solicitud comprende el nombre de usuario (123);
- enviar, al segundo dispositivo (42, 115), una solicitud para usar el dispositivo primario para confirmar la autenticación;
- recibir, del segundo dispositivo (42, 115), una aceptación (48, 49) para usar el primer dispositivo (40, 112);
- enviar, al segundo dispositivo (42, 115), un identificador único temporal (121);
- enviar, al primer dispositivo (40, 112), una solicitud de autenticación que comprende el identificador único temporal (121);
- recibir, del primer dispositivo (40, 112), una autorización para autenticar el segundo dispositivo (42, 115);
- enviar, al segundo dispositivo (42, 115), credenciales de autorización (57) del primer dispositivo (40, 112) para acceder a la cuenta de usuario (113).

2. El procedimiento de la reivindicación 1, donde el identificador único temporal es una secuencia alfanumérica.

3. El procedimiento de la reivindicación 1, donde la autenticación puede establecerse para una única sesión.

4. Medios codificados con código que, cuando son ejecutados por un procesador, realizan el procedimiento de cualquier reivindicación anterior.

5. Un servidor que comprende medios adaptados para realizar las etapas del procedimiento definido en la reivindicación 1.



Sistema de Confianza Bluetooth

1. ID 0 e ID 1 se identifican entre sí y establecen una comunicación temporal.

2. Para establecer confianza entre ID 0 e ID 1
   A: ID 0 genera y transmite ID Temp a ID 1
   B: ID Temp es mostrada en ID 1
   C: Si ID Temp en ID 0 es igual a ID Temp en ID 1, entonces confiar entre ID 0 e ID 1.

Técnica anterior

Figura 1A

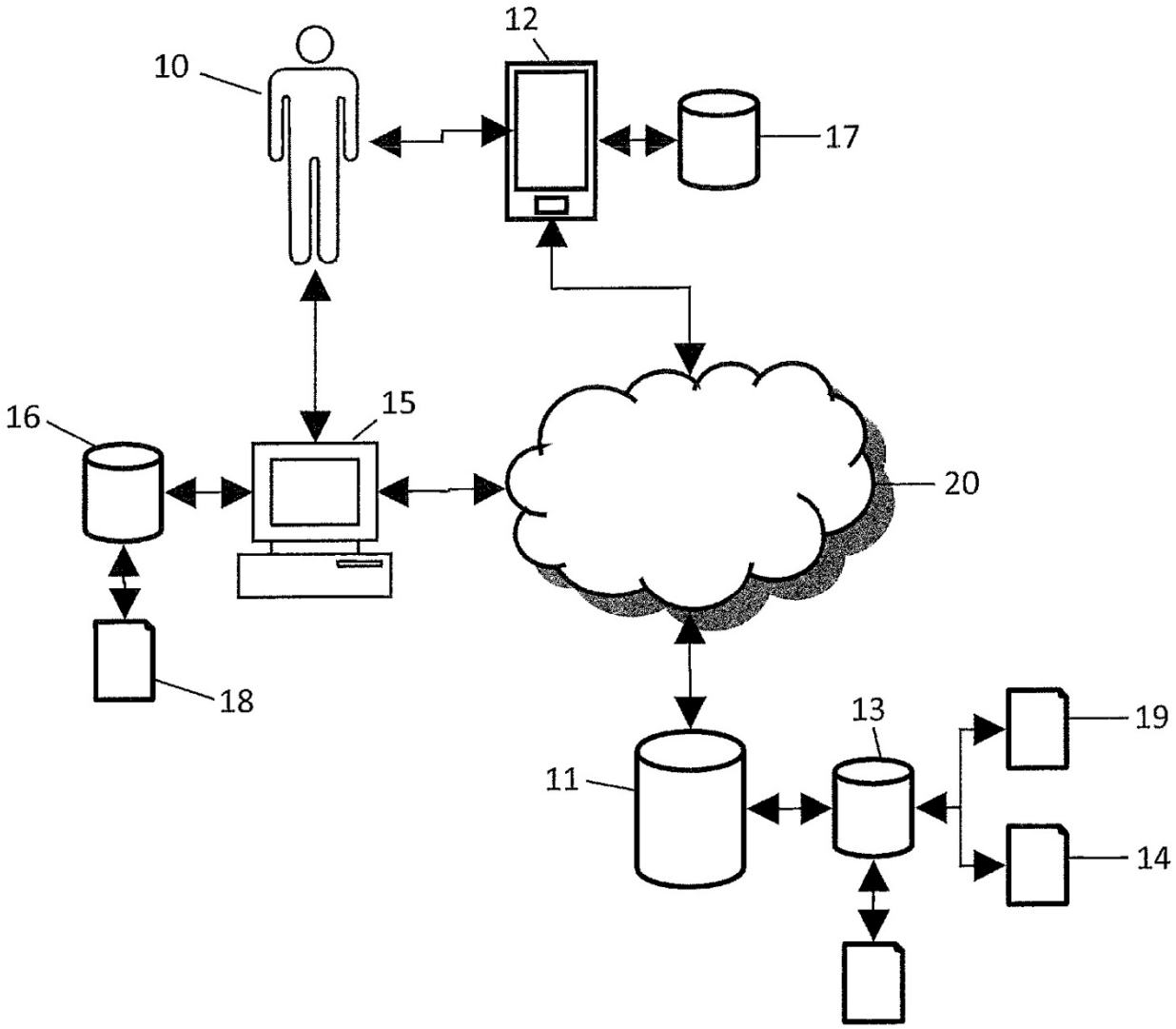


Figura 1B

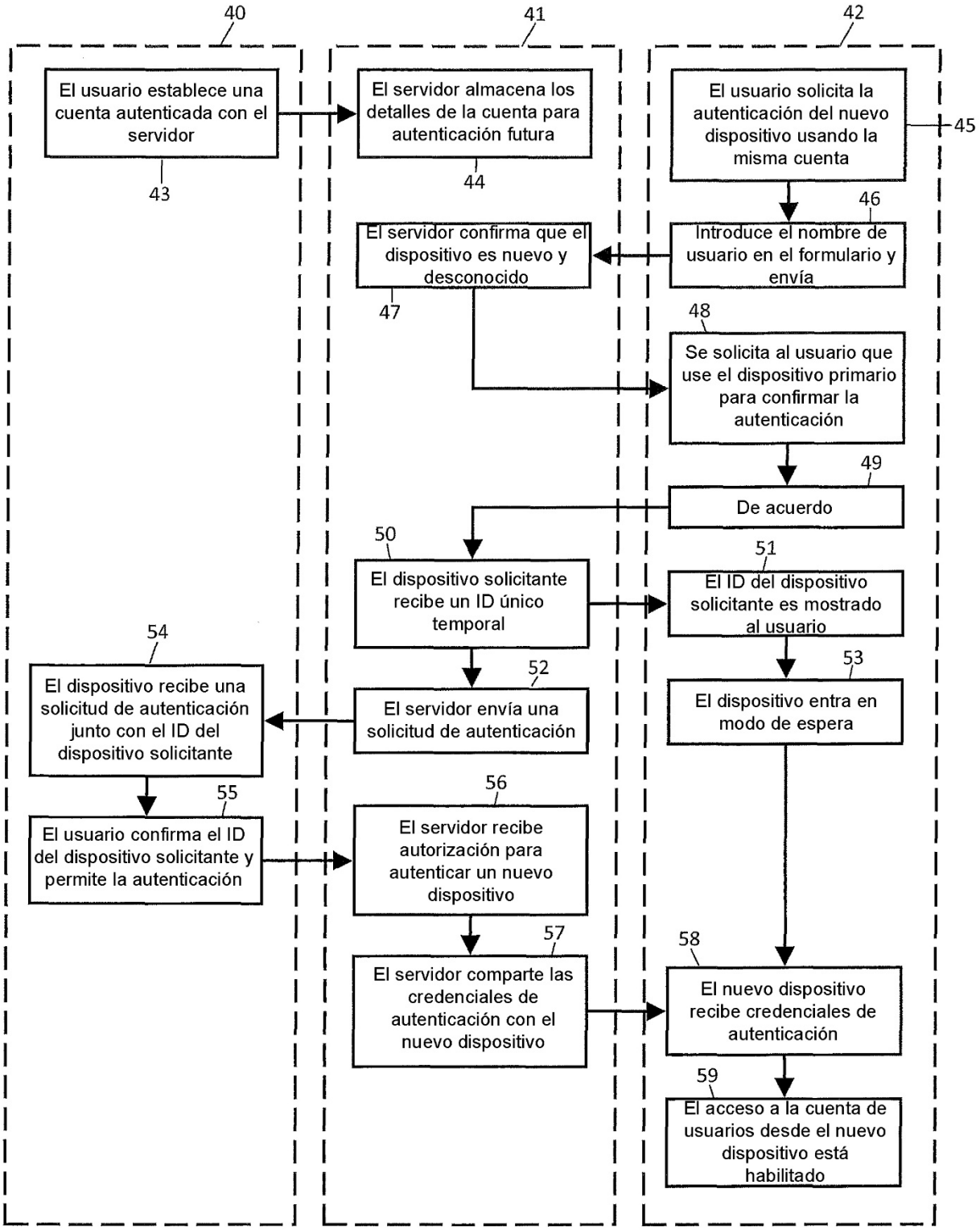
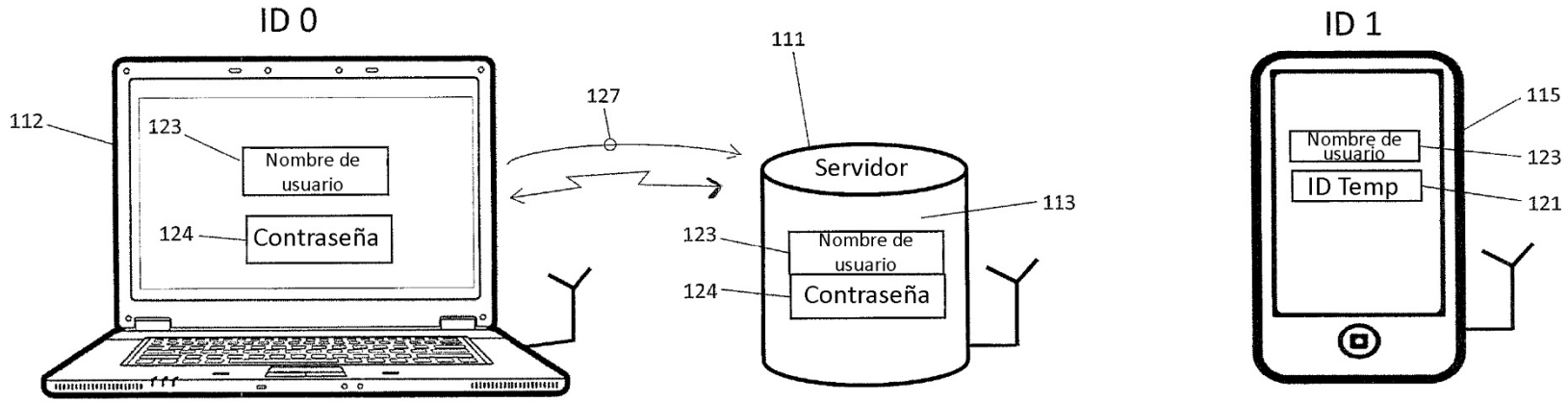

40
41
42
El usuario establece una cuenta autenticada con el servidor
43
El servidor almacena los detalles de la cuenta para autenticación futura
44
El usuario solicita la autenticación del nuevo dispositivo usando la misma cuenta
45
46
Introduce el nombre de usuario en el formulario y envía
El servidor confirma que el dispositivo es nuevo y desconocido
47
48
Se solicita al usuario que use el dispositivo primario para confirmar la autenticación
49
De acuerdo
50
El dispositivo solicitante recibe un ID único temporal
51
El ID del dispositivo solicitante es mostrado al usuario
53
El dispositivo entra en modo de espera
52
El servidor envía una solicitud de autenticación
54
El dispositivo recibe una solicitud de autenticación junto con el ID del dispositivo solicitante
55
El usuario confirma el ID del dispositivo solicitante y permite la autenticación
56
El servidor recibe autorización para autenticar un nuevo dispositivo
57
El servidor comparte las credenciales de autenticación con el nuevo dispositivo
58
El nuevo dispositivo recibe credenciales de autenticación
59
El acceso a la cuenta de usuarios desde el nuevo dispositivo está habilitado

Figura 2



1. INICIO DE SESIÓN para establecer la autenticación entre ID 0 y servidor para ese inicio de sesión

2. Establecer autenticación entre ID 1 y el servidor para ese inicio de sesión
   A: El servidor transmite ID Temp a ID 1
   B: El servidor transmite ID Temp a ID 0
   C: Si ID Temp en ID 0 es igual a ID Temp en ID 1, entonces autenticar entre ID 1 y el servidor para ese inicio de sesión.

Figura 3

ES 2 929 974 T3

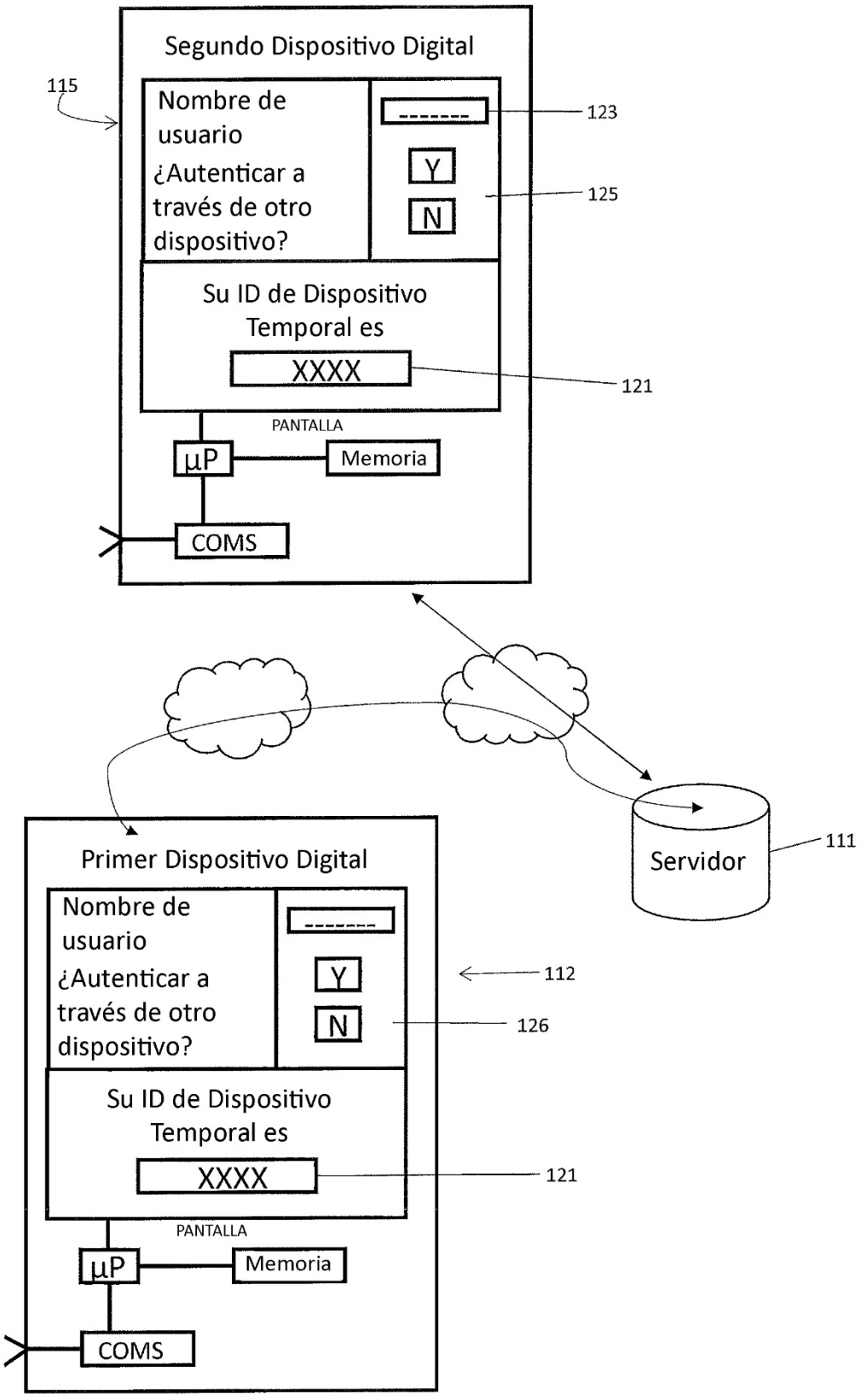

Segundo Dispositivo Digital
115
Nombre de usuario
¿Autenticar a través de otro dispositivo?
123
Y
N
125
Su ID de Dispositivo Temporal es
XXXX
121
PANTALLA
µP
Memoria
COMS
Servidor
111
Primer Dispositivo Digital
Nombre de usuario
¿Autenticar a través de otro dispositivo?
112
Y
N
126
Su ID de Dispositivo Temporal es
XXXX
121
PANTALLA
µP
Memoria
COMS

Figura 4