(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 383 242**

(51) Int. CI.:
H04L 12/58 (2006.01)
H04L 29/06 (2006.01)
H04W 4/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09174366 .6**
(96) Fecha de presentación: **28.10.2009**
(97) Número de publicación de la solicitud: **2317709**
(97) Fecha de publicación de la solicitud: **04.05.2011**

(54) Título: **Autenticación e identificación automáticas de usuario para aplicación de mensajería instantánea móvil**

(45) Fecha de publicación de la mención BOPI:
19.06.2012

(45) Fecha de la publicación del folleto de la patente:
19.06.2012

(73) Titular/es:
RESEARCH IN MOTION LIMITED
295 Phillip Street
Waterloo, Ontario N2L 3W8, CA

(72) Inventor/es:
Lee, Dalsu;
Khvan, Kateryna;
Lo, Ken;
Manolescu, Andreea y
Hung, Michael

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Autenticación e identificación automáticas de usuario para aplicación de mensajería instantánea móvil.

CAMPO TÉCNICO

La presente tecnología se refiere en general a comunicaciones inalámbricas y, en particular, a identificación y autenticación de usuario para dispositivos de comunicaciones inalámbricas.

ANTECEDENTES

Los dispositivos de comunicaciones inalámbricas proporcionan una panoplia de funciones y aplicaciones que hace que estos dispositivos sean crecientemente populares. Para algunas aplicaciones tales como, por ejemplo, e-mail, agenda, calendario, la sincronización cliente-servidor asegura que los mensajes, contactos y citas del usuario sean registrados en el servidor, permitiendo de ese modo una fácil recuperación de estos datos en el caso de que el usuario conmute a un nuevo dispositivo o barra los datos del dispositivo. Para otras aplicaciones, en las que los datos del dispositivo no están registrados en un servidor, estos datos son vulnerables de modo que pueden perderse si el usuario realiza un barrido de datos en el dispositivo o conmuta a un nuevo dispositivo.

Por ejemplo, esto es un problema con mensajería de PIN puesto que esta forma de mensajería instantánea utiliza el identificador único de dispositivo (PIN) como dirección de transporte y no retransmite datos a través de un servidor. En cambio, los mensajes de PIN son comunicados directamente desde un dispositivo a otro a través de la red inalámbrica sin ser enrutados a través de un servidor de mensajería. Una agenda de contactos (una lista de PINs por cada uno de los contactos del usuario), opciones de usuario u otra información de ese tipo para la aplicación de mensajería de PIN, están así expuestas a perderse si el usuario conmuta a un nuevo dispositivo o hace un barrido de datos en el dispositivo. Aunque se conoce en el estado de la técnica interponer un servidor y registrar el usuario en el servidor creando un inicio de sesión de cuenta de usuario o ID de usuario, esta solución conduce a fatiga de contraseña y a la práctica insegura de reutilización de contraseñas. En consecuencia, sigue existiendo una necesidad de una técnica que conserve los datos de dispositivo cuando un dispositivo es conmutado o barrido sin exacerbar el problema de fatiga de contraseña.

El documento US 2008/0216153 A1 divulga sistemas, aparatos y métodos para facilitar la autenticación y las identificaciones para dispositivos de red. Un identificador que ya esté afiliado a un dispositivo se utiliza como nombre de usuario en un proceso de autenticación. Una contraseña y una clave de autenticación son generadas en base a al menos el nombre de usuario, y la contraseña y la clave de autenticación son proporcionadas al dispositivo. Durante el intento de acceso a un servicio de red por parte del dispositivo, el nombre de usuario, la contraseña y la clave de autenticación son intercambiados de alguna manera para determinar la autenticidad del dispositivo.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Las características y ventajas adicionales de la presente tecnología resultaran evidentes a partir de la descripción detallada que sigue, tomada en combinación con los dibujos anexos, en los que:

La Figura 1 es una representación esquemática de un ejemplo de dispositivo de comunicaciones inalámbricas en el que puede ser implementada la presente tecnología;

La Figura 2 es una representación esquemática de una pluralidad de dispositivos de comunicaciones inalámbricas conectados a un servidor de mensajería instantánea, servidor de e-mail y servidor de aplicaciones a través de redes inalámbricas y de Internet;

La Figura 3 representa esquemáticamente un servidor de mensajería instantánea (servidor de mensajería) como ejemplo de un servidor de aplicación móvil que puede implementar la presente tecnología para identificar y autenticar automáticamente usuarios del dispositivo;

La Figura 4 es un diagrama de flujo que compendia algunas de las etapas principales de un método de identificación y autenticación automática de un usuario de una aplicación móvil;

La Figura 5 es un diagrama de flujo que compendia algunas de las etapas principales de un método de registro automático de un usuario de una aplicación móvil en un servidor;

La Figura 6 es un diagrama que representa un modelo de datos para la cuenta de usuario en el que un ID de registro se ha asociado a un PIN y a una dirección de e-mail;

La Figura 7 representa un flujo de mensaje para un protocolo de autenticación de acuerdo con una implementación de esta nueva tecnología, y

La Figura 8 representa un método de actualización de información de Pin cuando un usuario conmuta a un nuevo dispositivo que tiene un nuevo PIN de acuerdo con una implementación de esta nueva tecnología, y

Se apreciará que a través de los dibujos anexos se han identificado las mismas características con iguales números de referencia.

DESCRIPCIÓN DETALLADA

En general, la presente tecnología proporciona una forma innovadora de que un servidor identifique y autentique automáticamente un usuario de una aplicación móvil tal como, por ejemplo, una aplicación de mensajería

instantánea que se ejecuta en un dispositivo de comunicaciones inalámbricas. El dispositivo comunica al servidor un identificador único de dispositivo (por ejemplo, un número de PIN, ESN, IMEI u otro código o número que identifique unívocamente el dispositivo inalámbrico) y una dirección de e-mail (que está enlazada con el dispositivo). El servidor asocia el identificador único de dispositivo y la dirección de e-mail con un identificador de registro. El identificador de registro, la dirección de e-mail y el identificador único de dispositivo forman así un triplete que puede ser usado para identificar y autenticar al usuario incluso aunque el usuario cambie el identificador único de dispositivo (por ejemplo, al conmutar dispositivos) o cambie su dirección de e-mail. Esta técnica permite con ello la creación de una cuenta (ID y contraseña de usuario) en el servidor para registrar datos relacionados con la aplicación. Por ejemplo, en el contexto específico de una aplicación de mensajería instantánea, los contactos (listas de contactos), opciones, perfiles, etc. (que constituyen los datos relacionados con la aplicación) pueden ser registrados en el servidor y recuperados cuando se precise accediendo a la cuenta con el uso del nuevo protocolo de identificación y autenticación automáticas. Esto elimina la necesidad de que el usuario recuerde e introduzca un ID y una contraseña de usuario para acceder a su cuenta en el servidor. En consecuencia, esta nueva tecnología permite que los datos de dispositivo (que en otro caso se perderían si el dispositivo fuera barrido o conmutado), sean conservados mediante almacenamiento de estos datos de dispositivo en una cuenta en un servidor. Los datos pueden ser recuperados de manera fácil y sin problemas empleando la nueva técnica de identificación y autenticación automáticas para acceder a los datos de la cuenta en el servidor sin que se requiera que el usuario introduzca un ID de inicio de sesión o una contraseña.

De ese modo, un aspecto principal de la presente tecnología consiste en un método para la identificación y la autenticación automáticas de un usuario de una aplicación móvil que se ejecuta en un dispositivo de comunicaciones inalámbricas. El método llevado a cabo por el servidor entraña recibir desde el dispositivo de comunicaciones inalámbricas un identificador único de dispositivo y una dirección de e-mail del usuario correspondientes al dispositivo de comunicaciones inalámbricas, asociar un identificador de registro con el identificador único de dispositivo y la dirección de e-mail, generar un signo de autenticación, y comunicar el signo de autenticación y el identificador de registro al dispositivo de comunicaciones inalámbricas.

Otro aspecto principal de la presente tecnología consiste en un método para registrar automáticamente un usuario de una aplicación móvil que se ejecuta en un dispositivo de comunicaciones inalámbricas con un servidor. El método llevado a cabo por el dispositivo de comunicaciones inalámbricas conlleva determinar una dirección de e-mail del usuario correspondiente al dispositivo de comunicaciones inalámbricas, comunicar al servidor un identificador único de dispositivo y la dirección de e-mail para permitir que un identificador de registro almacenado en el servidor sea asociado con el identificador único de dispositivo y con la dirección de e-mail, y recibir un signo de autenticación y el identificador de registro desde el servidor.

Todavía otro aspecto principal de la presente tecnología consiste en un dispositivo de comunicaciones inalámbricas que tiene un procesador acoplado operativamente a una memoria para determinar una dirección de email del usuario y un identificador único de dispositivo correspondientes al dispositivo de comunicaciones inalámbricas, y un transceptor de radiofrecuencia para comunicar el identificador único de dispositivo y la dirección de e-mail a un servidor con el fin de permitir que el servidor asocie un identificador de registro con el identificador único de dispositivo y con la dirección de e-mail, recibiendo el transceptor desde el servidor el identificador de registro y un signo de autenticación.

Incluso otro aspecto adicional principal de la presente tecnología consiste en un servidor de aplicación móvil que tiene una conexión de red para recibir desde un dispositivo de comunicaciones inalámbricas un identificador único de dispositivo y una dirección de email del usuario correspondientes al dispositivo de comunicaciones inalámbricas, una memoria para almacenar un identificador de registro, un procesador acoplado operativamente a la memoria para asociar el identificador de registro con el identificador único de dispositivo y con la dirección de e-mail, para generar un signo de autenticación y para comunicar por medio de e-mail el signo de autenticación y el identificador de registro al dispositivo de comunicaciones inalámbricas.

Los detalles y los particulares de estos aspectos de la tecnología van a ser descritos a continuación, a título de ejemplo, con referencia a los dibujos anexos.

DISPOSITIVO

La Figura 1 es una representación esquemática de un ejemplo de un dispositivo 100 de comunicaciones inalámbricas en el que puede ser implementada la presente tecnología. El término “dispositivo de comunicaciones inalámbricas” se entiende que abarca una amplia gama de dispositivos celulares y móviles tales como, por ejemplo, teléfonos inteligentes, teléfonos celulares, teléfonos por satélite, asistentes digitales personales (PDAs) con capacidad inalámbrica, tabletas de computación con capacidad inalámbrica, ordenadores portátiles con capacidad inalámbrica, etc.

Según se ha mostrado esquemáticamente en la Figura 1, el dispositivo 100 de comunicaciones inalámbricas incluye un microprocesador (mencionado en lo que sigue como un “procesador”) 110, acoplado operativamente a una memoria (Memoria Flash 120 y/o RAM 130). El dispositivo 100 tiene una interfaz de usuario 140 que incluye un

visualizador (por ejemplo, una pantalla LCD) 150, un teclado/teclado numérico 155. Un mando rotatorio/bola de seguimiento 160 puede haberse previsto opcionalmente como parte de la interfaz de usuario. Alternativamente, la interfaz de usuario 140 puede incluir una pantalla táctil en lugar de un teclado/teclado numérico. El dispositivo 100 de comunicaciones inalámbricas incluye un chipset 170 de transceptor de radiofrecuencia (RF) para transmitir y recibir inalámbricamente comunicaciones de datos y voz, por ejemplo a través de una red celular. Las comunicaciones inalámbricas pueden ser llevadas a cabo utilizando CDMA, GSM o cualquier otro estándar o protocolo de comunicaciones adecuado. Un micrófono 180 y un altavoz 182 han sido previstos para comunicaciones de voz, aunque éstos no sean necesarios para implementar la presente técnica de autenticación dado que ésta no incluye comunicaciones de voz.

Según se ha representado además en la Figura 1, el dispositivo 100 de comunicaciones inalámbricas puede incluir un chipset 190 de Sistema de Posicionamiento Global (GPS) (u otro subsistema de determinación de posición), para determinar la posición actual del dispositivo a partir de las señales de radiofrecuencia emitidas por una pluralidad de satélites orbitales de GPS.

En el nuevo dispositivo de comunicaciones inalámbricas, el procesador y la memoria actúan a efectos de determinar una dirección de e-mail y un identificador único de dispositivo correspondientes al dispositivo de comunicaciones inalámbricas. Por ejemplo, el dispositivo busca su propio PIN u otro identificador único de dispositivo. El dispositivo identifica también la dirección de e-mail del usuario (es decir, la dirección de e-mail del usuario que la aplicación de e-mail del dispositivo del usuario utiliza para enviar y recibir correo electrónico desde el dispositivo). El transceptor de radiofrecuencia comunica a continuación el identificador único de dispositivo y la dirección de e-mail a un servidor, con el fin de facilitar que el servidor asocie un identificador de registro con el identificador único de dispositivo y con la dirección de e-mail. Este registro del usuario da como resultado que se cree un signo de autenticación. El registro crea de manera efectiva una cuenta en el servidor actuando el signo de autenticación como la contraseña y el ID de registro como el ID de usuario. El transceptor recibe de nuevo desde el servidor el identificador de registro y un signo de autenticación.

El dispositivo de comunicaciones inalámbricas se registra de ese modo a sí mismo automáticamente en el servidor enviando su identificador único de dispositivo (por ejemplo, su PIN) y la dirección de e-mail usada por el dispositivo. Una vez que se ha registrado debidamente, el dispositivo puede así firmar en un servidor automáticamente sin necesitar que el usuario recuerde e introduzca un ID y una contraseña de usuario. En otras palabras, una vez registrado, el dispositivo puede interactuar automáticamente con el servidor identificándose y autenticándose a sí mismo automáticamente con el servidor sin la intervención o activación de entrada del usuario. Esto elimina los problemas asociados a “fatiga de contraseña”, es decir la necesidad de tener que recordar e introducir una contraseña.

En la aplicación específica de mensajería de PIN, es decir la mensajería instantánea, en la que los dispositivos utilizan sus identificadores únicos de dispositivo como direcciones de transporte, esta nueva tecnología de autenticación puede ser utilizada para acceder automáticamente a los datos relacionados con Pin almacenados en una cuenta de usuario en un servidor. Se puede acceder a estos datos después de haber conmutado los dispositivos o después de haber hecho un barrido de datos en un dispositivo. En cualquier caso, la técnica de autenticación puede ser usada para acceder a, y recuperar, datos registrados relacionados con PIN (por ejemplo, para recuperar listas de contactos, opciones, perfiles, etc., en el dispositivo).

Convencionalmente, cuando un usuario conmuta dispositivos o hace un barrido de datos en un dispositivo, toda la información relacionada con el PIN (por ejemplo, listas de contacto, opciones, perfiles, etc.) se pierde. Esta nueva tecnología de autenticación hace que sea posible acceder automáticamente a los datos registrados almacenados en una cuenta de usuario en un servidor con el fin de recuperar los datos en el dispositivo. El acceso a los datos registrados se realiza automáticamente en el sentido de que el usuario no es incitado a introducir una contraseña o un ID de inicio de sesión para identificarse a sí mismo o para ser autenticado como el propietario correcto de la cuenta. De ese modo, cuando un usuario conmuta a un nuevo dispositivo con un nuevo PIN o realiza un barrido de datos en un dispositivo existente, el nuevo dispositivo o dispositivo barrido puede recuperar la información almacenada en relación con el Pin desde la cuenta del usuario sin que se requiera que el usuario recuerde e introduzca una contraseña.

La técnica que antecede requiere en primer lugar que se cree una cuenta o un registro en el servidor (por ejemplo, en el servidor de mensajería instantánea). La creación de la cuenta puede ser iniciada por el usuario o automática. Por ejemplo, cuando el usuario de un nuevo dispositivo comunica en primer lugar con el servidor de mensajería instantánea, el dispositivo puede enviar automáticamente sus nuevos PIN y dirección de e-mail al servidor. Alternativamente, el dispositivo puede interrogar al usuario en cuanto a su autorización para crear tal cuenta. En cualquier caso, la creación de una cuenta conlleva comunicar el PIN y la dirección de e-mail del dispositivo al servidor, después de lo cual son asociados el PIN y la dirección de e-mail con una cuenta o un ID de registro. A continuación, el servidor puede reconocer al usuario automáticamente a partir de la dirección de e-mail únicamente. En otras palabras, la dirección de e-mail enlaza al usuario con un determinado ID de registro (cuenta). Una vez que se ha creado una cuenta o un registro, se puede utilizar para almacenar o registrar información relacionada con el

PIN tal como, por ejemplo, listas de contactos, agendas de contactos, perfiles de usuario, opciones, preferencias, etc.

Una vez que la cuenta ha sido creada, se puede acceder a la cuenta mediante el dispositivo comunicando simplemente al servidor que alberga la cuenta el identificador de registro y el signo de autenticación, los cuales actúan como ID de inicio de sesión y contraseña, respectivamente. Cualquier nuevo dato que sea registrado (nuevo contacto o información de agenda, opciones de ajuste, perfiles modificados, etc.), puede ser registrado periódicamente mediante acceso a la cuenta de usuario. El acceso a la cuenta de usuario se realiza utilizando la técnica de identificación y autenticación automáticas, es decir, sin que se requiera que el usuario introduzca ningún ID de inicio de sesión o contraseña. Los datos almacenados en la cuenta de usuario pueden ser recuperados si se borran de la memoria del dispositivo. Los datos pueden ser recuperados accediendo a la cuenta utilizando la misma técnica de identificación y autenticación (es decir, iniciando sesión con el uso del ID de registro y el signo de autenticación).

Si se realiza un barrido de datos en el dispositivo o si el usuario conmuta el antiguo dispositivo a un nuevo dispositivo, el ID de registro y el signo de autenticación no están ya más disponibles en el dispositivo. En ese caso, el acceso a la cuenta de usuario en el servidor resulta aún posible. El dispositivo debe comunicar su identificador único de dispositivo (por ejemplo, el PIN) si está aún disponible en el dispositivo, y/o la dirección de e-mail que fue utilizada para crear la cuenta. Con el reconocimiento ya sea del identificador único de dispositivo o de la dirección de e-mail, el servidor puede identificar la cuenta que pertenece al usuario. Una vez que la cuenta ha sido identificada, los datos se pueden recuperar en el dispositivo en que se realizó el barrido o ser descargados en el nuevo dispositivo.

La Figura 2 representa esquemáticamente un ejemplo de una red en la que puede ser implementada la presente tecnología. En la red de este ejemplo, los dispositivos 100 de comunicaciones inalámbricas comunican a través de redes inalámbricas 202 que tienen torres 202 de estaciones de base. Las redes inalámbricas 202 están conectadas a Internet para permitir que los dispositivos de comunicaciones inalámbricas naveguen por la Web, intercambien e-mails, etc. Los clientes con los dispositivos 100 de comunicaciones inalámbricas comunican a través de un cortafuegos 206 y de un servidor 208 de negocio con diversos servidores (por ejemplo, el servidor 210 de e-mail, el servidor 212 de aplicaciones y el servidor 214 de mensajería instantánea). Cada uno de estos servidores 210, 212, 214 puede estar conectado a su almacén de datos respectivo o base de datos 216, 218 y 220. Convencionalmente, los mensajes de PIN son intercambiados directamente entre dispositivos a través de la red inalámbrica sin ser demorados a través del servidor de negocio. El PIN sirve como identificador único de dispositivo y también como dirección de transporte. Utilizando la nueva tecnología que se divulga en la presente memoria, el dispositivo se registra automáticamente en el servidor de mensajería instantánea proporcionando una dirección de e-mail y el PIN (u otro identificador único de dispositivo). El servidor de mensajería instantánea asocia el identificador de registro (ID de registro) con la dirección de e-mail y el PIN (u otro identificador único de dispositivo) y dota al dispositivo de un signo de autenticación junto con el ID de registro. Los contactos, agendas de contacto y otros tales como la información, pueden ser almacenados (registrados) en el servidor de mensajería instantánea asociados a una cuenta de usuario identificada por el ID de registro y la dirección de e-mail, y de ese modo pueden ser restaurados o recuperados en caso de que el usuario realice un barrido de datos en su dispositivo o conmute a un nuevo dispositivo con un nuevo PIN. Esto va a ser desarrollado a continuación.

SERVIDOR DE APLICACIÓN MÓVIL

Un aspecto de esta nueva tecnología consiste en un servidor de aplicación móvil tal como, por ejemplo, un servidor 214 de mensajería instantánea que interactúa con el dispositivo 100, según se muestra a título de ejemplo en la Figura 3, para identificar y autenticar al usuario utilizando la dirección de e-mail y el PIN del dispositivo (u otro identificador único de dispositivo). Este servidor de aplicación móvil identifica y autentica al usuario sin que se necesite que el usuario introduzca un ID de usuario o una contraseña. Puesto que el usuario no tiene que recordar o introducir una contraseña, esta solución ayuda a mitigar el problema creciente de “fatiga de contraseña”, y también obvia la práctica insegura de reutilizar la misma contraseña para conectarse a diferentes aplicaciones.

Según se ha representado esquemáticamente en la Figura 3, un servidor de aplicación móvil tal como, por ejemplo, un servidor 214 de mensajería instantánea (“servidor de mensajería”) tiene una conexión de red 215 para recibir desde el dispositivo 100 de comunicaciones inalámbricas un identificador único de dispositivo (por ejemplo, un PIN) y una dirección de e-mail correspondientes al dispositivo de comunicaciones inalámbricas. El servidor 214 posee una memoria 214b para almacenar un identificador de registro. El servidor 214 posee también un procesador 214a acoplado operativamente a la memoria para asociar el identificador de registro con el identificador único de dispositivo ((por ejemplo, el PIN) y con la dirección de e-mail. El procesador y la memoria actúan para generar también un signo de autenticación. La conexión de red 215 es la utilizada para comunicar vía e-mail el signo de autenticación y el identificador de registro al dispositivo 100 de comunicaciones inalámbricas. Específicamente, en el sistema presentado a título de ejemplo en la Figura 3, el e-mail es comunicado a través de Internet 204 y de la red inalámbrica 200 al dispositivo 100. Según se muestra en la Figura 3, la memoria 214b se utiliza para almacenar tripletes de datos (ID de registro, dirección de e-mail y PIN) para una pluralidad de usuarios. La memoria o el almacenamiento de datos puede ser local o remoto respecto al servidor.

MÉTODOS

Un método de identificar y autenticar automáticamente a un usuario de una aplicación móvil tal como, por ejemplo, una aplicación de mensajería instantánea, con un servidor de aplicación móvil (por ejemplo, un servidor de mensajería instantánea) puede ser llevado a cabo según se ha representado en la Figura 4. Según se muestra en la Figura 4, el método (que es llevado a cabo por el servidor) conlleva una etapa 300 de recepción de PIN (u otro identificador único de dispositivo) y dirección de e-mail en el servidor de mensajería instantánea. A continuación, en la etapa 310, el Pin y la dirección de e-mail son asociados por el servidor a un identificador de registro (o ID de registro). El ID de registro, en una implementación, puede ser generado con anterioridad a la recepción de la dirección de e-mail y del PIN. En otra implementación, el ID de registro puede ser generado tras la recepción del PIN y de la dirección de e-mail. En cualquier caso, el ID de registro es enlazado con (asociado a) la dirección de e-mail y el PIN. Este ID de registro es funcionalmente equivalente a un ID de usuario. Un signo de autenticación (que es funcionalmente equivalente a una contraseña) es generado a continuación para el ID de registro (ID de usuario) en la etapa 320. El ID de registro y el signo de autenticación son comunicados a continuación al dispositivo en la etapa 330. En ese punto, se constituye la cuenta de usuario (el usuario es registrado). El ID de registro realiza el papel del ID de usuario mientras que el signo de autenticación realiza el papel de la contraseña. Para interactuar con el servidor, el usuario no necesita introducir ningún ID de usuario ni contraseña. El dispositivo se identifica y autentica automáticamente a sí mismo proporcionando su ID de registro (como el equivalente funcional de un ID de inicio de sesión) y el signo de autenticación (como el equivalente funcional de una contraseña).

La Figura 5 representa un método complementario (llevado a cabo por el dispositivo) en el que el dispositivo se registra a sí mismo automáticamente en un servidor sin necesitar que el usuario del dispositivo recuerde e introduzca un ID de usuario y una contraseña. En este método, en la etapa 340, el dispositivo determina una dirección de e-mail correspondiente al dispositivo de comunicaciones inalámbricas. Por ejemplo, el dispositivo puede estar configurado de modo que el e-mail procedente de un servidor de e-mail sea empujado hasta el dispositivo. La dirección de e-mail es identificada a continuación como enlazada a ese dispositivo particular de comunicaciones inalámbricas. Se debe apreciar que el dispositivo de comunicaciones inalámbricas puede estar enlazado a más de una dirección de e-mail. En la etapa 350, el dispositivo de comunicaciones inalámbricas comunica al servidor un identificador único de dispositivo y la dirección de e-mail. Esto permite que un identificador de registro almacenado en el servidor sea asociado al identificador único de dispositivo y a la dirección de e-mail. A continuación, en la etapa 360, el dispositivo recibe un signo de autenticación y el identificador de registro desde el servidor. Estos ID y signo de registro pueden ser utilizados después para permitir que el dispositivo interactúe con el servidor sin necesitar que el usuario introduzca un ID de inicio de sesión o una contraseña.

La Figura 6 es un diagrama que representa un modelo de datos para la cuenta de usuario en el que un ID de registro (identificador 600 de registro) está asociado a un PIN (u otro identificador 610 único de dispositivo) y a una dirección de e-mail 620. El ID de registro, el PIN y la dirección de e-mail forman un triplete de datos. Mientras el ID de registro y la dirección de e-mail se mantengan sin cambios, el usuario puede adquirir un nuevo dispositivo con un nuevo PIN y ser aún reconocible por el servidor de aplicación móvil como el mismo usuario. La información de usuario (por ejemplo, listas de contactos, agendas de contactos, perfiles, opciones, etc.) puede ser así restaurada desde la cuenta del usuario en el servidor hasta el dispositivo. Esto no sólo es útil cuando un usuario conmuta a un nuevo dispositivo, sino también en casos en los que un usuario hace un barrido de datos en un dispositivo.

La Figura 7 presenta un ejemplo de un flujo de mensaje para un protocolo de autenticación de acuerdo con una implementación particular. En la implementación particular representada en la Figura 7, un cliente 700 de mensajería con el dispositivo de comunicaciones inalámbricas, comunica con el servidor 214 de mensajería para procesar un nuevo registro. Una petición de autenticación 710, que incluye un PIN de dispositivo encriptado y una dirección de e-mail encriptada, es enviada desde el cliente hasta el servidor durante una sesión de mensajería instantánea. El servidor de mensajería genera un signo de autenticación de e-mail y lo codifica con una clave de sesión (por ejemplo, desde KeyNego). Un e-mail de autenticación 720, que incluye un signo de autenticación de e-mail encriptado, es enviado a continuación de nuevo al cliente de mensajería con el dispositivo a través de e-mail (en vez de cómo mensaje instantáneo). El cliente de mensajería intercepta el e-mail y descodifica el signo de autenticación utilizando la clave de sesión (por ejemplo, KeyNego). A continuación, una petición de autenticación 730 que contiene el PIN del dispositivo, la dirección de e-mail y el signo de autenticación, es comunicada desde el dispositivo de retorno al servidor. Cuando el servidor recibe la autenticación junto con el PIN y la dirección de e-mail apropiados, se satisface el hecho de que el signo de autenticación ha sido enviado al dispositivo correcto. En ese punto, el servidor devuelve una respuesta de autenticación 740 al cliente de mensajería del dispositivo. Una vez que este procedimiento ha sido completado, el dispositivo tiene las credenciales (ID de registro y signo de autenticación) para acceder automáticamente a la cuenta de usuario en el servidor con el fin de registrar o restaurar datos. En otras palabras, las funciones de registro y restauración pueden ser llevadas a cabo sin ninguna intervención del usuario (por ejemplo, sin necesitar que el usuario introduzca un ID de inicio de sesión o una contraseña). Por ejemplo, si un usuario añade una nueva persona de contacto para mensajería instantánea, la información de contacto para esa nueva persona de contacto (por ejemplo, el PIN de la nueva persona de contacto) es almacenada en el dispositivo. El dispositivo puede registrar automáticamente la información acerca del nuevo contacto accediendo a la cuenta del

usuario en el servidor y almacenando esa información en esa cuenta. Este registro automático se realiza conectando con la cuenta utilizando el ID y el signo de registro.

La Figura 8 representa esquemáticamente, a título de ejemplo, un método de actualización de la información de PIN cuando un usuario conmuta a un nuevo dispositivo. En este escenario, el usuario que conmuta a un nuevo dispositivo con un nuevo PIN desea notificar todos estos contactos/agendas de contacto que su PIN ha cambiado. En vez de enviar mensajes de actualización individuales, se puede utilizar la técnica que sigue para diseminar el nuevo PIN por todos los contactos/agendas de contactos almacenadas en una cuenta de usuario en el servidor. Este diagrama de la Figura 8 ilustra así un ejemplo específico de cómo un nuevo dispositivo con un nuevo identificador único de dispositivo (por ejemplo, un nuevo PIN de dispositivo) puede diseminar automáticamente el identificador único de dispositivo (por ejemplo, el nuevo PIN) a todos los contactos (agendas de contactos) cuando el nuevo dispositivo conecta con la red por primera vez. Según se muestra en la etapa 801, el dispositivo 100 comunica su nuevo identificador único de dispositivo (por ejemplo, el nuevo PIN) al servidor de aplicación móvil (por ejemplo, el servidor 214) de mensajería. Este servidor de aplicación móvil (por ejemplo, el servidor 214 de mensajería) acusa recibo (etapa 802) del nuevo PIN respondiendo al dispositivo 100. Tras la recepción por el dispositivo 100 de esta confirmación o acuse de recibo del nuevo PIN, el usuario del dispositivo no necesita hacer nada más, puesto que el servidor de aplicación móvil (por ejemplo, el servidor 214 de mensajería) asegura que todos los contactos están al tanto del nuevo PIN. En la etapa 803, el servidor 214 de mensajería guarda el nuevo PIN en una base de datos 800 de transacciones, conectada al o accesible de otro modo desde el servidor 214. La base de datos 800 de transacciones salva los detalles de la transacción actualizada hasta que la transacción (actualización) se ha completado en cuyo momento el nuevo PIN puede ser retirado de la base de datos 800 de transacciones. Pero con anterioridad a la retirada del nuevo PIN desde la base de datos de transacciones, el servidor de aplicación móvil (por ejemplo, el servidor 214 de mensajería) identifica todos los contactos (agendas de contactos) asociados al usuario y comunica a continuación (etapa 804) el nuevo PIN a cada uno de esos contactos o agendas de contactos (es decir, envía la información del nuevo PIN como actualización de PIN a cada dispositivo asociado a un contacto o una agenda de contactos). El servidor 214 de mensajería espera un acuse de recibo desde cada contacto o agenda de contactos. Una vez que se ha recibido un acuse de recibo (etapa 805) por cada contacto al que se envió una actualización, el servidor de mensajería retira el nuevo PIN de la base de datos de transacciones. Si todos los contactos no han respondido con el acuse de recibo, entonces el servidor de mensajería empieza a enviar comunicaciones adicionales (intermitentes) al contacto que no haya respondido en un intervalo ajustablemente predeterminado hasta que el contacto responde con el acuse de recibo del nuevo PIN (nuevo identificador único de dispositivo). Solamente entonces (cuando todos los contactos han confirmado la recepción del PIN actualizado) el servidor de mensajería retira el nuevo PIN de la base de datos de transacciones (en la etapa 806). La base de datos de transacciones asegura así que cualquier contacto o agenda de contactos que esté temporalmente fuera de rango o cuyo dispositivo esté temporalmente interrumpido, recibirá eventualmente la notificación del nuevo PIN.

En otras palabras, el servidor de mensajería instantánea u otro servidor de aplicación móvil está configurado para recibir un nuevo identificador único de dispositivo (por ejemplo, un PIN) desde un nuevo dispositivo, acusar recibo del nuevo identificador único de dispositivo desde el nuevo dispositivo, guardar el nuevo identificador único de dispositivo en una base de datos de transacciones accesible por el servidor, identificar al usuario en base a uno o ambos de entre el identificador de registro y la dirección de e-mail, identificar contactos asociados al usuario, comunicar el nuevo identificador único de dispositivo a los contactos hasta que el servidor haya recibido los acuses de recibo desde todos los contactos, y retirar el nuevo identificador único de dispositivo desde la base datos.

Las etapas de método que anteceden pueden ser implementadas como instrucciones codificadas en un producto de programa de ordenador. En otras palabras, el producto de programa de ordenador consiste en un medio legible con ordenador cuyo código de software está grabado para llevar a cabo las etapas que anteceden cuando el producto de programa de ordenador es cargado en la memoria y ejecutado en el microprocesador del dispositivo de comunicaciones inalámbricas.

Esta nueva tecnología ha sido descrita en términos de implementaciones y configuraciones específicas que solamente se pretende que constituyan ejemplos. El alcance del derecho exclusivo reclamado por el Solicitante se pretende que solamente esté limitado por tanto por las reivindicaciones anexas.

REIVINDICACIONES

1.- Un método para la identificación y autenticación automáticas de un usuario de una aplicación móvil que se ejecuta en un dispositivo de comunicaciones inalámbricas, comprendiendo el método:

recibir desde el dispositivo de comunicaciones inalámbricas un identificador único de dispositivo y una dirección de e-mail correspondientes al usuario del dispositivo de comunicaciones inalámbricas (300);
asociar un identificador de registro con el identificador único de dispositivo y la dirección de e-mail (310);
generar un signo de autenticación (320), y
comunicar el signo de autenticación y el identificador de registro al dispositivo de comunicaciones inalámbricas (300) para permitir que el usuario del dispositivo de comunicaciones inalámbricas sea consiguientemente identificado y autenticado utilizando el identificador de registro y el signo de autenticación.

2.- El método según se reivindica en la reivindicación 1, en el que la aplicación móvil es una aplicación de mensajería instantánea en comunicación con un servidor de mensajería instantánea.

3.- El método según se reivindica en la reivindicación 2, en el que la recepción del identificador único de dispositivo y de la dirección de e-mail comprende recibir una petición de autenticación que incluye un identificador único de dispositivo encriptado y una dirección de e-mail encriptada a través de una sesión de mensaje instantáneo desde el dispositivo hasta el servidor de mensajería instantánea.

4.- El método según se reivindica en la reivindicación 3, en el que comunicar el signo de autenticación y el identificador de registro comprende transmitir un e-mail de autenticación que incluye un signo de autenticación encriptado.

5.- El método según se reivindica en la reivindicación 4, en el que transmitir el e-mail de autenticación comprende:

transmitir el e-mail de autenticación en un formato predeterminado para permitir que la aplicación de mensajería instantánea que se ejecuta en el dispositivo intercepte automáticamente el e-mail de autenticación y descodifique automáticamente el signo de autenticación.

6.- El método según se reivindica en la reivindicación 5, que comprende además:

recibir desde el dispositivo una petición de autenticación que incluye el identificador único de dispositivo, la dirección de e-mail y el signo de autenticación, y
transmitir una respuesta de autenticación hasta el dispositivo.

7.- El método según se reivindica en la reivindicación 2, que comprende además:

recibir en el servidor de mensajería instantánea un nuevo identificador único de dispositivo para un nuevo dispositivo;
comunicar un acuse de recibo del nuevo identificador único de dispositivo al nuevo dispositivo;
guardar el nuevo identificador único de dispositivo en una base de datos de transacciones accesible por parte del servidor;
comunicar el nuevo identificador único de dispositivo a otro dispositivo que el servidor lo ha identificado como un contacto del usuario en base al identificador de registro asociado al usuario;
recibir un acuse de recibo del nuevo identificador único de dispositivo por parte del contacto, y
retirar el identificador único de dispositivo desde la base de datos de transacciones.

8.- El método según se reivindica en la reivindicación 1, que comprende además:

crear una cuenta en un servidor asociando el identificador de registro con el identificador único de dispositivo y con la dirección de e-mail.

9.- El método según se reivindica en la reivindicación 8, en el que el acceso a la cuenta comprende comunicar ya sea solamente la dirección de e-mail a partir de la cual se ha determinado el identificador de registro para la cuenta o ya sea solamente el identificador único de dispositivo a partir del cual se ha determinado el identificador de registro para la cuenta.

10.- El método según se reivindica en la reivindicación 8, que comprende además:

acceder a la cuenta comunicando al servidor el identificador de registro y el signo de autenticación.

11.- Un método, llevado a cabo en un dispositivo de comunicaciones inalámbricas, para registrar automáticamente un usuario de una aplicación móvil que se ejecuta en el dispositivo de comunicaciones inalámbricas, en un servidor, comprendiendo el método:

determinar una dirección de e-mail correspondiente al usuario del dispositivo de comunicaciones inalámbricas (340);
comunicar al servidor un identificador único de dispositivo y la dirección de e-mail para permitir que un identificador de registro almacenado en el servidor sea asociado al identificador único de dispositivo y a la dirección de e-mail (350), y
recibir un signo de autenticación y el identificador de registro desde el servidor (360).

12.- El método según se reivindica en la reivindicación 11, en el que la aplicación móvil es una aplicación de mensajería instantánea, y el que el servidor es un servidor de mensajería instantánea.

13.- El método según se reivindica en la reivindicación 12, en el que comunicar el identificador único de dispositivo y la dirección de e-mail comprende transmitir una petición de autenticación que incluye un identificador único de dispositivo encriptado y una dirección de e-mail encriptada por medio de una sesión de mensaje instantáneo desde el dispositivo hasta el servidor de mensajería instantánea.

14.- El método según se reivindica en la reivindicación 13, en el que recibir el signo de autenticación y el identificador de registro comprende:

interceptar un e-mail de autenticación que incluye un signo de autenticación encriptado;
descodificar el signo de autenticación, y
transmitir de nuevo al servidor a través de la sesión de mensaje instantáneo una petición de autenticación que incluye el identificador único de dispositivo, la dirección de e-mail y el signo de autenticación.

15.- El método según se reivindica en la reivindicación 12, que comprende:

comunicar un nuevo identificador único de dispositivo al servidor de mensajería instantánea, y
recibir un acuse de recibo desde el servidor de mensajería instantánea que notifique al usuario del nuevo dispositivo que el nuevo identificador único de dispositivo va a ser distribuido por el servidor de mensajería instantánea a todos los contactos almacenados en el servidor de mensajería instantánea asociado a un identificador de registro para el usuario.

16.- Un dispositivo (100) de comunicaciones inalámbricas, que comprende:

un transceptor (170) de radiofrecuencia, y
un procesador (110) acoplado operativamente a una memoria (120, 130) que comprende instrucciones ejecutables con ordenador, las cuales, cuando son ejecutadas por el procesador, provocan que el procesador lleve a cabo las etapas de una cualquiera de las reivindicaciones 8 a 12.

17.- Un servidor (214) de aplicación móvil, que comprende:

una conexión de red (215) para recibir desde un dispositivo (100) de comunicaciones inalámbricas un identificador único de dispositivo y una dirección de e-mail correspondientes a un usuario del dispositivo de comunicaciones inalámbricas;
una memoria (214b) para almacenar un identificador de registro;
un procesador (214a) acoplado operativamente a la memoria para asociar el identificador de registro al identificador único de dispositivo y a la dirección de e-mail, para generar un signo de autenticación y para comunicar a través de e-mail el signo de autenticación y el identificador de registro al dispositivo de comunicaciones inalámbricas.

18.- El servidor de aplicación móvil según se reivindica en la reivindicación 17, en el que el identificador único de dispositivo y la dirección de e-mail son recibidos en una petición de autenticación durante una sesión de mensajería instantánea entre una aplicación de mensajería instantánea que se ejecuta en el dispositivo y el servidor de aplicación móvil que actúa como servidor de mensajería instantánea.

19.- El servidor de aplicación móvil según se reivindica en la reivindicación 18, en el que el servidor está configurado para esperar la recepción de una petición de autenticación que incluye el identificador único de dispositivo, la dirección de e-mail y el signo de autenticación, y para contestar con una respuesta de autenticación que confirme que confirme que la autenticación del usuario en el servidor ha sido completada con éxito.

20.- El servidor de aplicación móvil según se reivindica en la reivindicación 18, en el que el servidor está configurado para:

recibir un nuevo identificador único de dispositivo desde un nuevo dispositivo;
acusar recibo del nuevo identificador único de dispositivo desde el nuevo dispositivo;
guardar el nuevo identificador único de dispositivo en una base de datos de transacciones accesible por parte del servidor;
identificar al usuario en base a uno o ambos de entre el identificador de registro y la dirección de e-mail;
identificar contactos asociados al usuario;
comunicar el nuevo identificador único de dispositivo a los contactos hasta que el servidor haya recibido el acuse de recibo desde todos los contactos, y
retirar el nuevo identificador único de dispositivo de la base de datos.

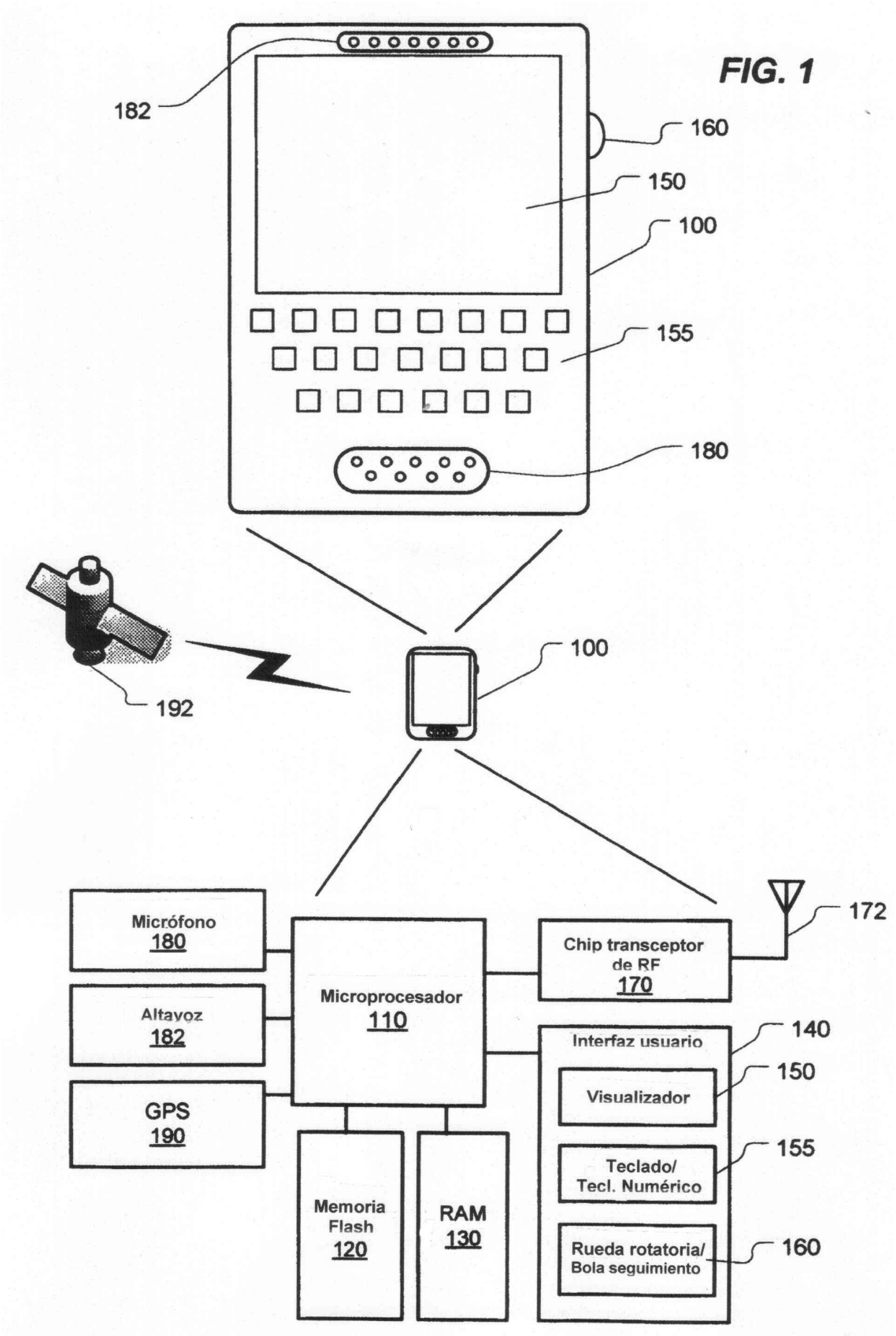
182
160
150
100
155
180
192
100
Micrófono
180
Altavoz
182
GPS
190
Microprocesador
110
Memoria
Flash
120
RAM
130
Chip transceptor
de RF
170
172
Interfaz usuario
140
Visualizador
150
Teclado/
Tecl. Numérico
155
Rueda rotatoria/
Bola seguimiento
160

FIG. 1

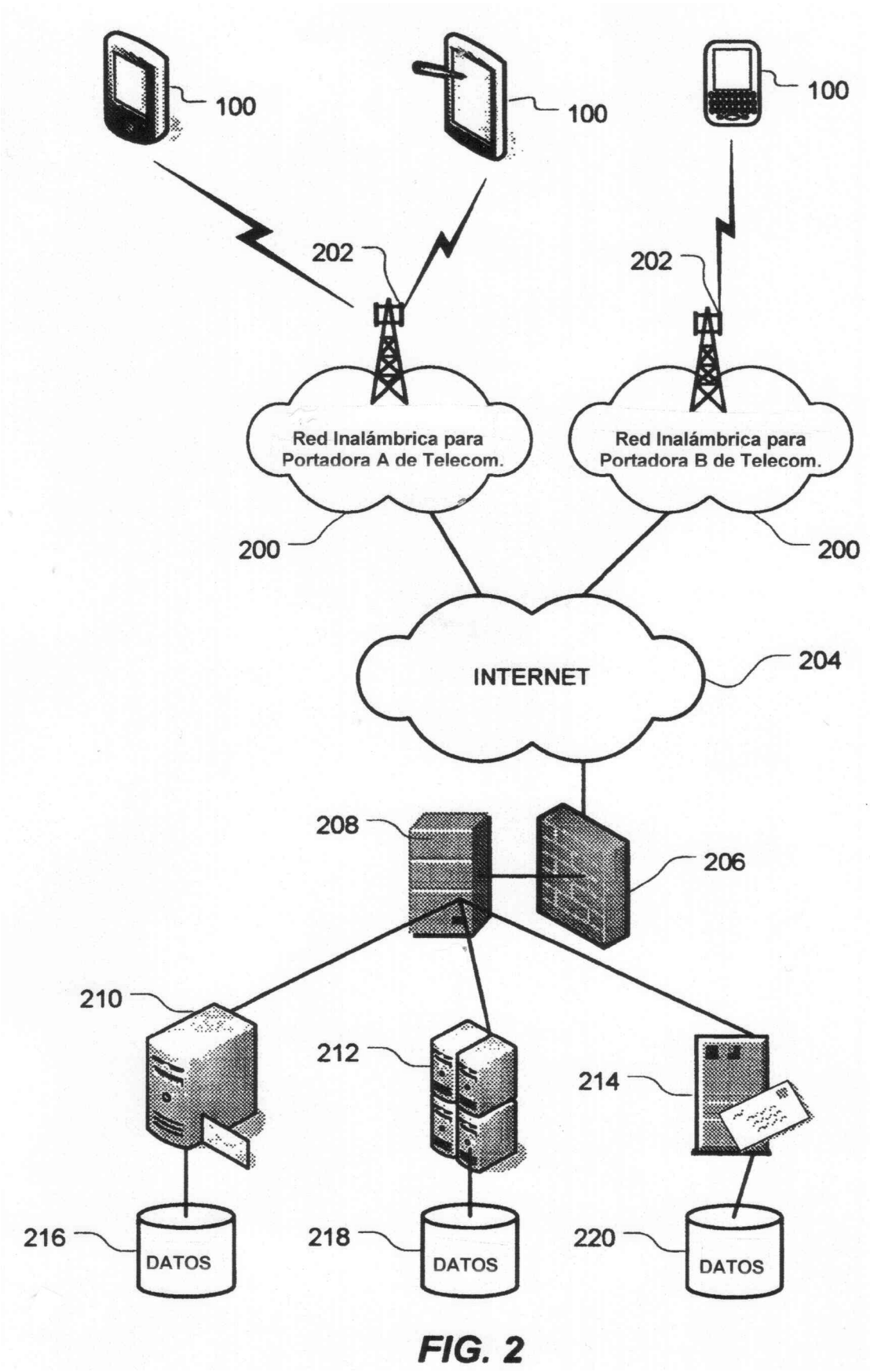
100
100
100
202
202
Red Inalámbrica para Portadora A de Telecom.
Red Inalámbrica para Portadora B de Telecom.
200
200
INTERNET
204
208
206
210
212
214
216
DATOS
218
DATOS
220
DATOS

FIG. 2

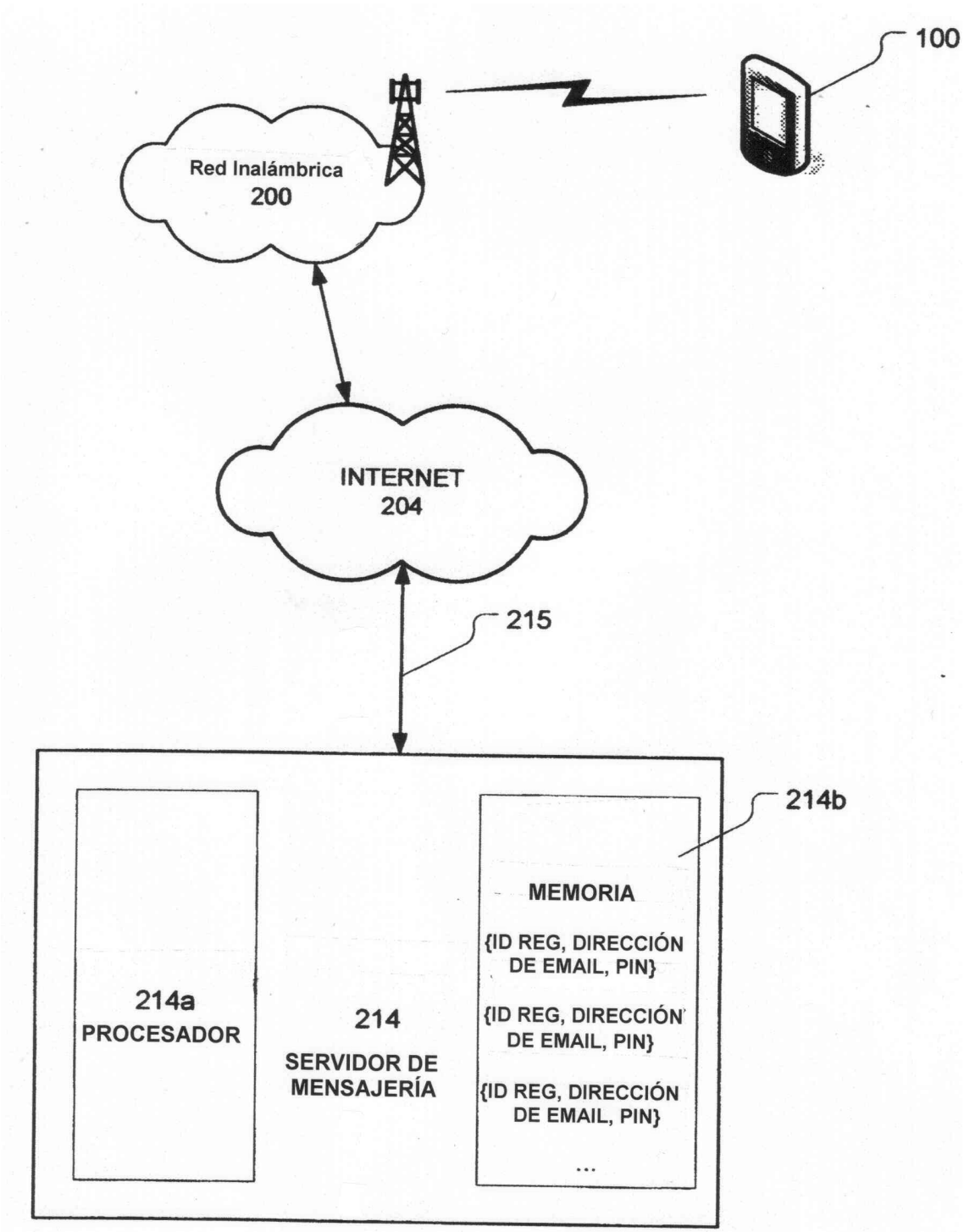
100
Red Inalámbrica
200
INTERNET
204
215
214b
MEMORIA
{ID REG, DIRECCIÓN DE EMAIL, PIN}
{ID REG, DIRECCIÓN DE EMAIL, PIN}
{ID REG, DIRECCIÓN DE EMAIL, PIN}
...
214a
PROCESADOR
214
SERVIDOR DE MENSAJERÍA

FIG. 3

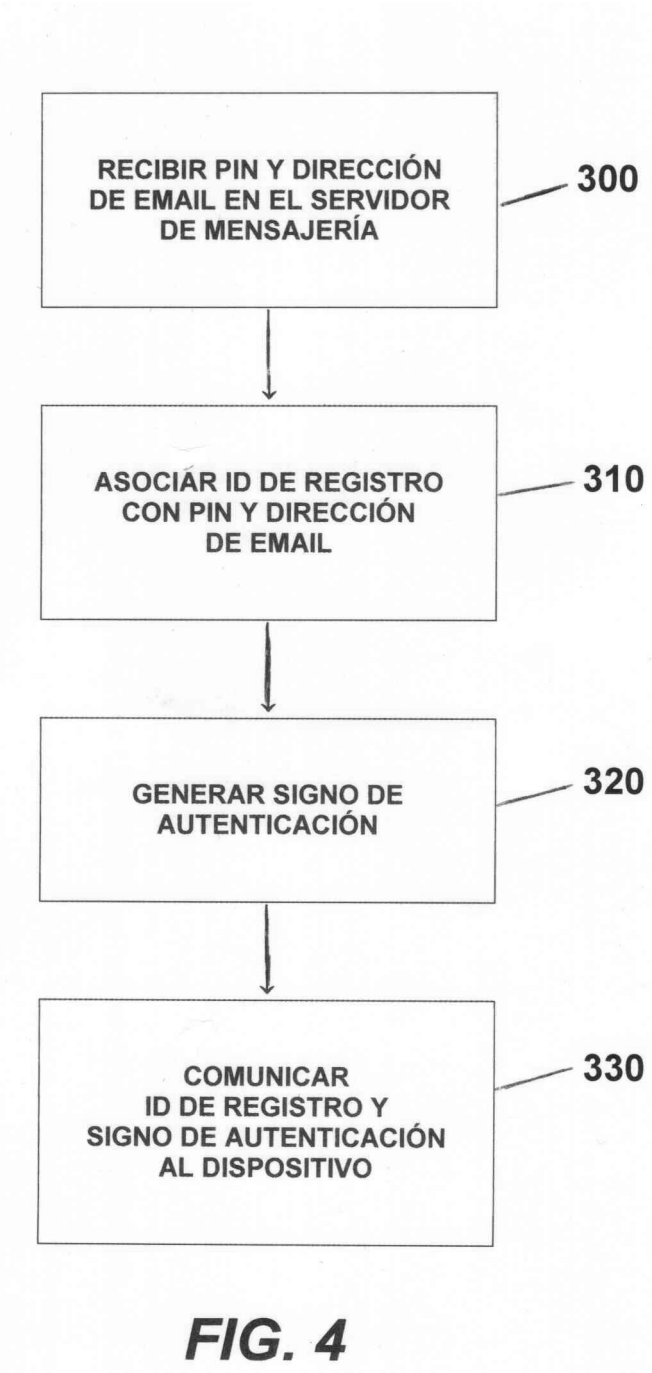
RECIBIR PIN Y DIRECCIÓN DE EMAIL EN EL SERVIDOR DE MENSAJERÍA
300
ASOCIAR ID DE REGISTRO CON PIN Y DIRECCIÓN DE EMAIL
310
GENERAR SIGNO DE AUTENTICACIÓN
320
COMUNICAR ID DE REGISTRO Y SIGNO DE AUTENTICACIÓN AL DISPOSITIVO
330

FIG. 4

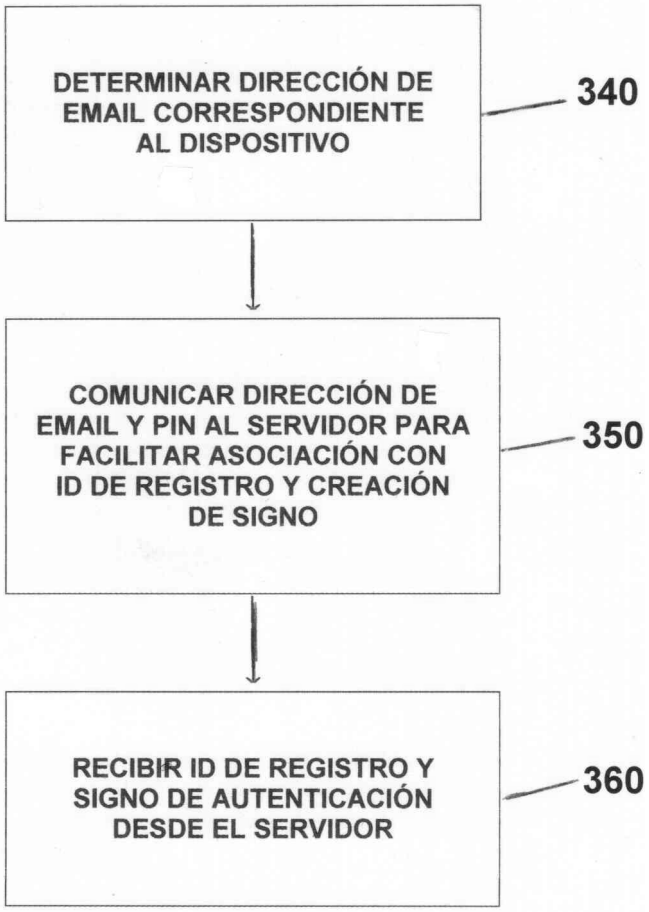
DETERMINAR DIRECCIÓN DE EMAIL CORRESPONDIENTE AL DISPOSITIVO
340
COMUNICAR DIRECCIÓN DE EMAIL Y PIN AL SERVIDOR PARA FACILITAR ASOCIACIÓN CON ID DE REGISTRO Y CREACIÓN DE SIGNO
350
RECIBIR ID DE REGISTRO Y SIGNO DE AUTENTICACIÓN DESDE EL SERVIDOR
360

FIG. 5

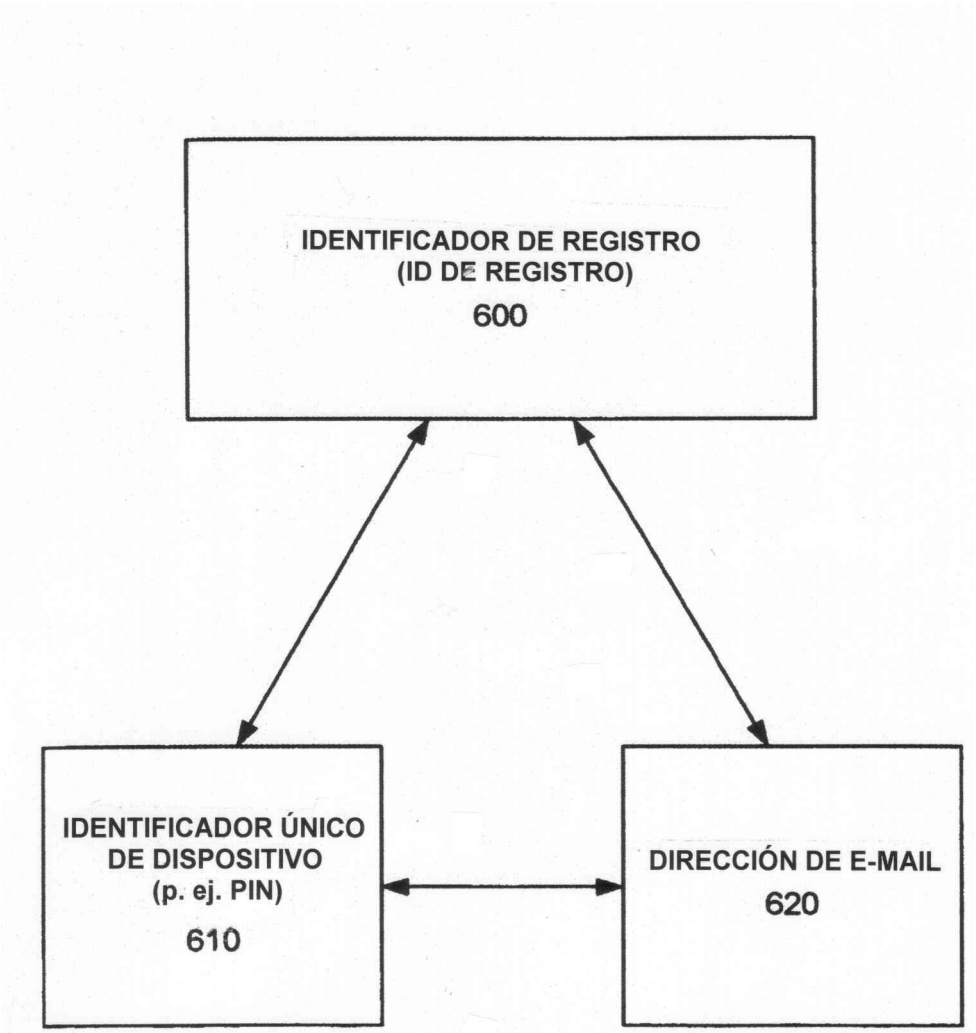
IDENTIFICADOR DE REGISTRO
(ID DE REGISTRO)
600
IDENTIFICADOR ÚNICO
DE DISPOSITIVO
(p. ej. PIN)
610
DIRECCIÓN DE E-MAIL
620

FIG. 6

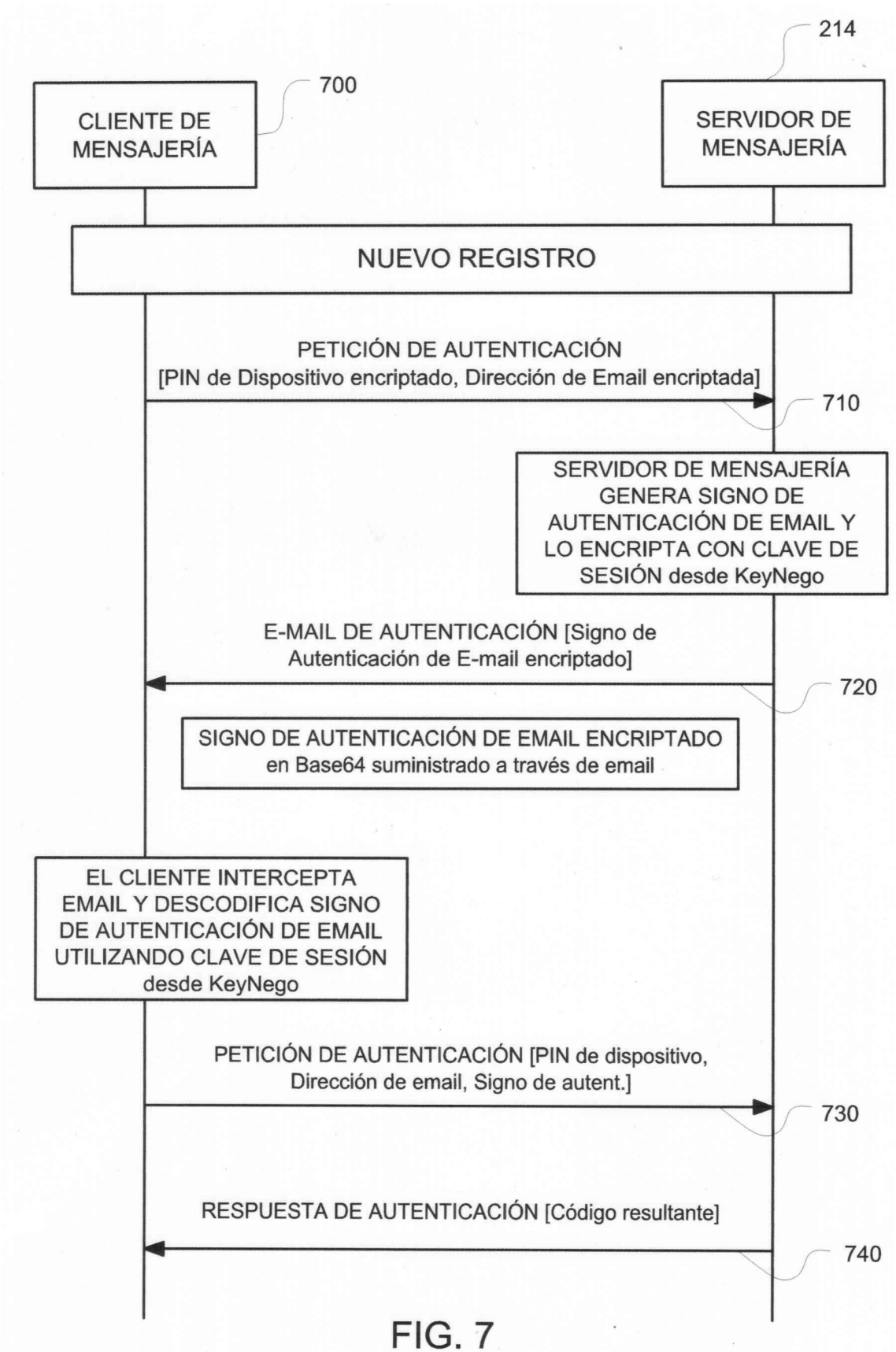
214
700
CLIENTE DE MENSAJERÍA
SERVIDOR DE MENSAJERÍA
NUEVO REGISTRO
PETICIÓN DE AUTENTICACIÓN [PIN de Dispositivo encriptado, Dirección de Email encriptada]
710
SERVIDOR DE MENSAJERÍA GENERA SIGNO DE AUTENTICACIÓN DE EMAIL Y LO ENCRIPTA CON CLAVE DE SESIÓN desde KeyNego
E-MAIL DE AUTENTICACIÓN [Signo de Autenticación de E-mail encriptado]
720
SIGNO DE AUTENTICACIÓN DE EMAIL ENCRIPTADO en Base64 suministrado a través de email
EL CLIENTE INTERCEPTA EMAIL Y DESCODIFICA SIGNO DE AUTENTICACIÓN DE EMAIL UTILIZANDO CLAVE DE SESIÓN desde KeyNego
PETICIÓN DE AUTENTICACIÓN [PIN de dispositivo, Dirección de email, Signo de autent.]
730
RESPUESTA DE AUTENTICACIÓN [Código resultante]
740

FIG. 7

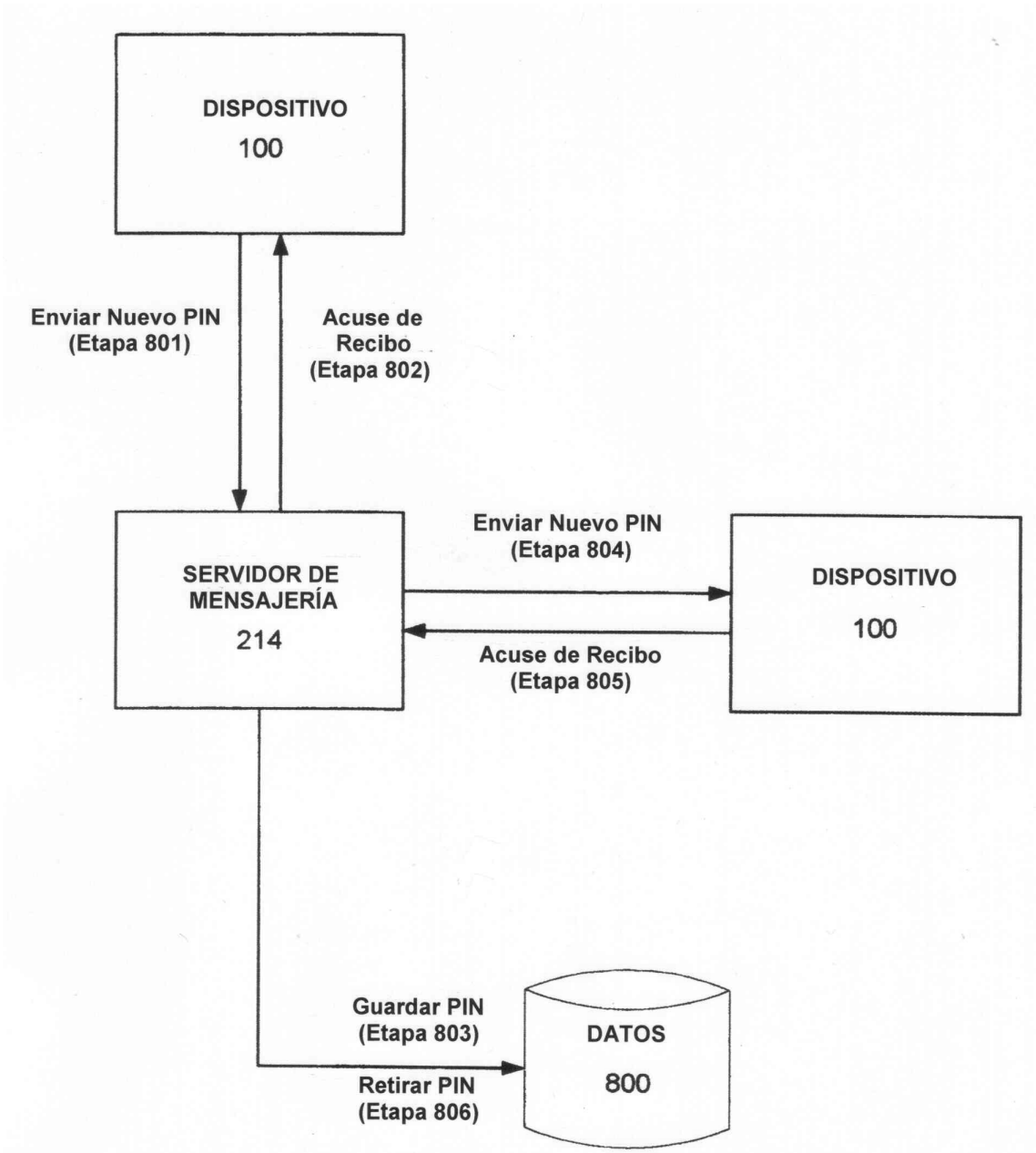
DISPOSITIVO
100
Enviar Nuevo PIN
(Etapa 801)
Acuse de
Recibo
(Etapa 802)
SERVIDOR DE
MENSAJERÍA
214
Enviar Nuevo PIN
(Etapa 804)
Acuse de Recibo
(Etapa 805)
DISPOSITIVO
100
Guardar PIN
(Etapa 803)
Retirar PIN
(Etapa 806)
DATOS
800

FIG. 8