

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 540 105**

51 Int. Cl.:

**H04L 29/06** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **06.02.2009 E 09711546 (3)**

97 Fecha y número de publicación de la concesión europea: **08.04.2015 EP 2248322**

54 Título: **Métodos y aparato para el registro de dispositivos inalámbricos**

30 Prioridad:

**22.02.2008 US 30695 P**  
**09.06.2008 US 135256**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**08.07.2015**

73 Titular/es:

**TELEFONAKTIEBOLAGET L M ERICSSON**  
**(PUBL) (100.0%)**  
**164 83 Stockholm, SE**

72 Inventor/es:

**SALMELA, PATRIK y**  
**SLAVOV, KRISTIAN**

74 Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

**ES 2 540 105 T3**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Métodos y aparato para el registro de dispositivos inalámbricos

## 5 CAMPO TÉCNICO

La presente invención se refiere en general a los sistemas de comunicación inalámbrica, y en particular se refiere a métodos, aparatos y sistemas para el procesamiento de datos de registro para dispositivos inalámbricos para su uso en la descarga de credenciales de abonado de red tal como un Módulo de Identidad de Abonado Universal (DLUSIM - Universal Subscriber Identity Module, en inglés).

10

## ANTECEDENTES

Las tecnologías de las comunicaciones de Máquina a máquina (M2M – Machine to Machine, en inglés) permiten el despliegue de dispositivos inalámbricos que no requieren la interacción humana para operar. Los dispositivos M2M inalámbricos han sido desplegados o propuestos para una amplia gama de aplicaciones de telemetría y telemática. Algunas de estas aplicaciones incluyen monitorización de sistemas de distribución de utilidad, venta remota, sistemas de seguridad y gestión de flotas.

15

20

Uno de los retos para el despliegue de M2M inalámbrico es cómo permitir un eficiente “aprovisionamiento” de servicios. En particular, cada dispositivo M2M inalámbrico debe ser activado para su operación en una red particular. Se conocen varias técnicas para la activación y el aprovisionamiento de dispositivos inalámbricos, incluyendo las técnicas descritas en la Solicitud de Patente Europea EP 0 778 716 A2, titulada “Customer activation system for cellular network”, y la Patente de U.S. Nº 6.064.879 titulada “Mobile Communication Method, and Mobile Telephone Switching Station Customer Management System, and Mobile Unit for implementing the Same”. Con los teléfonos celulares 3G convencionales, el aprovisionamiento se consigue típicamente utilizando un Módulo de Identidad de Abonado Universal (USIM), una aplicación instalada en una Tarjeta de Circuitos Integrados Universal (UICC – Universal Integrated Circuit Card, en inglés) proporcionada por el operador de red inalámbrica. La USIM / UICC puede ser insertada en un dispositivo celular para conectar el dispositivo a una suscripción particular, permitiendo con ello que el usuario del dispositivo acceda a terminales suscritos a través de la red de su operador doméstico y, en muchos casos, mediante redes de asociados colaboradores. Aunque resulta razonablemente conveniente para consumidores individuales, este planteamiento para aprovisionamiento puede no resultar práctico para una aplicación M2M en la que una única entidad puede desplegar cientos de dispositivos inalámbricos a través de una amplia área geográfica. Por ejemplo, en algunos casos un dispositivo inalámbrico puede ser instalado durante la fabricación en un elemento de equipo mayor (por ejemplo, un coche), haciendo la posterior inserción de una tarjeta SIM no práctica o imposible. En otros casos, los dispositivos M2M pueden ser desplegados sobre una amplia área geográfica, de manera que ningún operador inalámbrico único puede proporcionar la cobertura necesaria. En tales casos, hacer coincidir los USIMs específicos para un operador adecuado con los dispositivos correctos puede resultar problemático. Finalmente, la reconfiguración de un dispositivo M2M, por ejemplo, para transferir el dispositivo a una suscripción con un operador diferente, puede resultar cara, especialmente cuando el dispositivo M2M está en una ubicación remota.

25

30

35

40

45

Debido a estos retos, la industria inalámbrica ha estado investigando recientemente la posibilidad de credenciales de suscripción descargables, por ejemplo, un USIM descargable (DLUSIM). En particular, el Proyecto de Colaboración de 3ª Generación (3GPP – 3rd Generation Partnership Project, en inglés) ha estado estudiando la factibilidad de utilizar tecnología DLUSIM para la gestión remota de dispositivos M2M inalámbricos. Un informe del 3GPP titulado “Technical Specification Group Services and System Aspects; Feasibility Study on Remote Management of USIM Application on M2M Equipment; (versión 8), 3GPP TR 33.812, está actualmente en desarrollo.

50

En un planteamiento en estudio, las credenciales de suscripción preliminares, por ejemplo, una Identidad de Abonado Móvil Internacional Preliminar y sus claves asociadas, etc., están programadas en cada dispositivo M2M inalámbrico. Estas credenciales preliminares pueden ser utilizadas para obtener acceso inicial a una red inalámbrica disponible con el propósito limitado de descargar credenciales de suscripción “permanentes”, tal como un USIM descargable. Las credenciales preliminares están asociadas con un servicio de registro, que facilita un acceso temporal a una red de 3GPP y la conexión a un servidor de aprovisionamiento asociado con un operador inalámbrico que ofrece los servicios deseados.

55

60

El planteamiento general es que un dispositivo M2M inalámbrico utilice las credenciales preliminares para ejecutar un método de conexión inicial a red a una red disponible, de acuerdo con los protocolos de red inalámbrica convencionales. Puede asumirse que la red a la cual se conecta el dispositivo es una red visitada, de manera que la conexión se efectúa de acuerdo con procedimientos de itinerancia. Una vez conectado a la red, el dispositivo M2M establece una conexión con un servidor de aprovisionamiento para la descarga de un USIM.

65

Aunque el procedimiento anterior permite una conexión inicial a una red de 3GPP, no proporciona una solución completa para el aprovisionamiento de dispositivos M2M inalámbricos. Así, es necesario un mecanismo para conectar un dispositivo M2M inalámbrico desplegado a una suscripción para servicios de red para móviles de un operador de red. En particular, se necesitan mecanismos para el registro de un dispositivo inalámbrico

recientemente desplegado con un operador deseado (u "Operador Doméstico") y para la actualización de ese registro cuando sea necesario.

COMPENDIO

5 La presente invención proporciona un sistema y métodos para la asociación de un dispositivo M2M inalámbrico "genérico", es decir, un dispositivo que no está pre-programado con credenciales de suscripción correspondientes a un operador particular, con un Operador Doméstico designado por el propietario del dispositivo. El sistema y métodos descritos facilitan asimismo la conexión automática de un dispositivo M2M recientemente activado a un servidor apropiado para la descarga de credenciales de suscripción para el Operador Doméstico.

10 El sistema descrito incluye un servidor de registro para el guardado de datos de registro electrónicos para una pluralidad de dispositivos inalámbricos y para dirigir a los dispositivos inalámbricos recientemente activados a un servidor para la descarga de credenciales de suscripción "permanentes", tal como un USIM descargable. El sistema descrito incluye asimismo un servidor de suscripción para la actualización de entradas a servidor de registro para reflejar una asociación entre un dispositivo inalámbrico que se suscribe y su correspondiente red doméstica. En algunas realizaciones, el servidor de suscripción puede estar asimismo configurado para la descarga de credenciales de suscripción para la suscripción de dispositivos inalámbricos.

20 De acuerdo con esto, un servidor de registro de ejemplo de acuerdo con algunas realizaciones de la invención comprende una unidad de almacenamiento configurada para el almacenamiento de una pluralidad de identificadores preliminares del dispositivo y correspondientes códigos de seguridad, donde cada identificador preliminar del dispositivo está asociado con un dispositivo inalámbrico. El servidor de registro comprende asimismo una interfaz de red, y una unidad de procesamiento para el procesamiento de solicitudes de actualización de registro. En algunas comunicaciones, la unidad de procesamiento está configurada para la recepción de una solicitud de actualización de registro a través de la interfaz de red, comprendiendo la solicitud de actualización de registro un primer identificador de dispositivo, un primer código de seguridad candidato y datos de la red doméstica para un primer dispositivo inalámbrico. La unidad de procesamiento autentica la solicitud de actualización de registro mediante la comparación del primer código de seguridad candidato con un código de seguridad almacenado correspondiente al primer identificador de dispositivo, y almacena los datos de la red doméstica en la unidad de almacenamiento en asociación con el primer identificador de dispositivo y el código de seguridad correspondiente. En algunas realizaciones, la unidad de procesamiento está asimismo configurada para la recepción de una solicitud de conexión a través de la interfaz de red desde el primer dispositivo inalámbrico correspondiente al primer identificador del dispositivo, y para enviar al menos una porción de los datos de la red doméstica al primer dispositivo inalámbrico a través de la interfaz de red. Esta porción puede incluir una dirección de red para su uso por parte del primer dispositivo inalámbrico en la descarga de credenciales de suscripción.

35 Un servidor de suscripción de ejemplo comprende una interfaz de red y una unidad de procesamiento configurada para recibir una solicitud de suscripción electrónica para un primer dispositivo inalámbrico a través de la interfaz de red, comprendiendo la solicitud de suscripción un identificador de dispositivo preliminar y un correspondiente código de seguridad para el primer dispositivo inalámbrico. El servidor de suscripción envía una solicitud de actualización de registro a un servidor de registro a través de la interfaz de red, comprendiendo la solicitud de actualización de registro el identificador de dispositivo preliminar, el correspondiente código de seguridad y datos de la red doméstica para el primer dispositivo inalámbrico, donde los datos de la red doméstica identifican una dirección de red para la descarga de credenciales de suscripción. El servidor de suscripción puede estar asimismo configurado para recibir una solicitud de descarga de credencial desde el primer dispositivo inalámbrico a través de la dirección de red, donde la solicitud de descarga de credencial es dirigida a la dirección de red identificada por los datos de la red doméstica, y para enviar las credenciales de suscripción al primer dispositivo inalámbrico para su uso en el acceso a los servicios de red.

50 Métodos correspondientes para el guardado de datos de registro electrónicos para dispositivos inalámbricos y para la actualización de los datos de registro se explican también.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

55 La Figura 1 ilustra una red de comunicación de acuerdo con una o más realizaciones de la invención.  
 La Figura 2 ilustra el flujo de información de registro y de credenciales de abonado de acuerdo con algunas realizaciones de la invención.  
 La Figura 3 es un diagrama de flujo lógico que ilustra un método de ejemplo para guardar datos de registro electrónicos para una pluralidad de dispositivos inalámbricos.  
 La Figura 4 es un diagrama de flujo lógico que ilustra un método de ejemplo para la actualización de la información del código de seguridad para un dispositivo inalámbrico en un sistema de registro.  
 La Figura 5 es un diagrama de flujo lógico que ilustra un método de ejemplo para la actualización de los datos de registro electrónicos para un dispositivo inalámbrico y la distribución de las credenciales de suscripción al dispositivo inalámbrico.  
 La Figura 6 es un diagrama de bloques de un servidor de registro de acuerdo con algunas realizaciones de la invención.

La Figura 7 es un diagrama de bloques de un servidor de suscripción de acuerdo con algunas realizaciones de la invención.

#### DESCRIPCIÓN DETALLADA

5 En la descripción que sigue se describen varios aspectos de la presente invención en relación con los estándares de red promulgados por el Proyecto de Colaboración de 3ª Generación (3GPP). Resultará evidente para los expertos en la materia que estas técnicas pueden ser aplicadas a otros sistemas inalámbricos en los que las credenciales de suscripción pueden ser descargadas a un dispositivo inalámbrico. Además, aunque la explicación que sigue se centra en los dispositivos M2M inalámbricos, que incluyen dispositivos sin interfaces humanas en absoluto, las técnicas explicadas en esta memoria son aplicables de manera más general, y pueden de hecho ser aplicadas a otros terminales inalámbricos, que incluyen aparatos para el consumidor. Finalmente, resultará evidente para los expertos en la materia que el término “terminal móvil”, tal como se utiliza en esta memoria, pretende incluir cualquiera de una amplia variedad de dispositivos de usuario final, que incluyen en particular cualquiera de los dispositivos denominados “Equipo de Usuario”, (UE), o “estación de telefonía móvil” por las diferentes especificaciones promulgadas por la Colaboración de 3ª Generación o por otros grupos de estandarización. De hecho, el término “terminal de telefonía móvil” incluye terminales inalámbricos adaptados para aplicaciones de máquina a máquina (M2M), así como terminales inalámbricos adaptados para comunicaciones inalámbricas mediante telefonía fija. Resultará así evidente para los expertos en la materia que los terminales móviles explicados en esta memoria pueden comprender radioteléfonos celulares con capacidad de comunicaciones de voz, capacidades de comunicaciones de datos, o ambas; dispositivos asistentes digitales personales (PDA – Personal Digital Assistant, en inglés) que incluyen capacidad de comunicaciones inalámbricas; ordenadores portátiles de regazo y/u ordenadores de mano convencionales u otros dispositivos que incluyen un transmisor receptor inalámbrico; y tarjetas y módulos de transmisor receptor inalámbrico adaptadas para su uso en dispositivos informáticos anfitriones, que pueden o no ser portátiles. Así, la siguiente descripción y los dibujos que se acompañan deben ser considerados como ilustrativos de la presente invención, y no limitativos.

La Figura 1 ilustra una red de comunicación de acuerdo con una o más realizaciones de la invención, e incluye un dispositivo M2M 110 inalámbrico, que está en el rango de al menos dos estaciones de base 120. En el sistema ilustrativo de la Figura 1, una estación de base 120 proporciona acceso a una primera red inalámbrica, la red de Operador “Visitada” 130, mientras que la otra proporciona acceso a una segunda red inalámbrica, la red de Operador “Doméstico” 140. Resultará evidente para los expertos en la materia que con el propósito de la siguiente explicación los términos “visitado” y “doméstico” resultan significativos sólo después de que el dispositivo M2M 110 es asociado con una suscripción proporcionada por el operador de la red de Operador Doméstico (es decir, el “Operador Doméstico”). De hecho, cuando un dispositivo M2M 110 se conecta a una red utilizando sus credenciales preliminares, su operador “doméstico” con el propósito de conexión a la red es el operador que proporciona el servicio de registro descrito en esta memoria, es decir, el operador que controla las credenciales preliminares.

Resultará evidente para los expertos en la materia que el dispositivo M2M 110 puede en algunas realizaciones ser un dispositivo inalámbrico de multi-modo y/o de multi-banda, de manera que soporta múltiples protocolos de comunicaciones y/u opera en múltiples bandas de frecuencia. Así, la red de Operador Visitado 130 y la red de Operador Doméstico 140 puede ofrecer acceso a red a través de redes de acceso por radio similares o completamente diferentes.

En cualquier caso, cada una de la red de Operador Visitado 130 y la red de Operador Doméstico proporcionan servicios de datos inalámbricos y acceso a la red de datos pública (PDN – Public Data Network, en inglés) 150, que puede ser la Internet. Así, en el sistema representado, cada red inalámbrica es capaz de proporcionar al dispositivo M2M 110 acceso a cualquier recurso accesible públicamente en la Internet, así como acceso a recursos específicos para red ofrecidos por el operador de red inalámbrica particular. En el sistema simplificado ilustrado en la Figura 1, el dispositivo M2M 110 puede acceder a un servicio de registro 160, y a su base de datos 170 asociada a través de la PDN 150 y de la red de Operador Visitado 130 ó la red de Operador Doméstico 140. El dispositivo M2M 110 puede asimismo acceder al servidor de suscripción 180 a través de la PDN 150 y de una red inalámbrica o la otra. Alternativamente, en algunas realizaciones, puede accederse al servidor de suscripción 180 directamente o a través de la red de Operador Doméstico 140.

55 Como se ha observado anteriormente, las técnicas descritas en esta memoria son aplicables de manera general a sistemas que utilizan espacio de problema de aplicación de USIM descargable (DLUSIM). Puesto que éste es un espacio de problema relativamente nuevo, no existen soluciones fijas o específicas para implementar toda la funcionalidad que realmente permite el uso del concepto de USIM descargable. Un problema particular que no ha sido abordado adecuadamente es cómo asociar un dispositivo M2M inalámbrico “genérico”, es decir, un dispositivo que no está pre-programado con credenciales de suscripción correspondientes a un operador particular, con un Operador Doméstico designado por el propietario del dispositivo. Un problema estrechamente relacionado que es asimismo abordado mediante las técnicas descritas en esta memoria es cómo conectar automáticamente un dispositivo M2M recientemente activado a un servidor apropiado para la descarga de las credenciales de suscripción para el Operador Doméstico. En la descripción que sigue, estos procesos se denominarán de manera general “servicios de registro”, o “registro de Operador Doméstico”.

5 Cuando se crea un dispositivo de DLUSIM su Identidad de Abonado Móvil Internacional Preliminar (PIMSI – Preliminary International Mobile Subscriber Identity, en inglés) y otra información relacionada es almacenada en un Servicio de Registro. Este Servicio de Registro puede ser implementado en un servidor de registro, tal como el servidor de registro 160 de la Figura 1. Cuando el usuario de este dispositivo eventualmente decide activar el dispositivo, necesitará suscribirse para el uso de la red de telefonía móvil de un operador de red inalámbrica, denominado en esta memoria el Operador Doméstico. No obstante, para que el Operador Doméstico conozca las credenciales del dispositivo, el usuario debe proporcionar alguna información de identificación al Operador Doméstico. Esto es realizado de la manera más conveniente a través de la Internet. Por ello, las técnicas de invención explicadas en esta memoria proporcionan un mecanismo para cómo pueden asegurar el Operador Doméstico y el Servicio de Registro que un usuario está registrando su propio dispositivo en lugar de teclear sólo algunas credenciales al azar, y que las credenciales de suscripción sean fácilmente accesibles para dispositivos autorizados.

15 Además de la PIMSI, muchas otras técnicas descritas en esta memoria se basan en un código de seguridad asociado con la PIMSI. Este código de seguridad, que se denomina en ocasiones en esta memoria Identificador de IMSI Preliminar (PID – Preliminary IMSI Identifier, en inglés), actúa como un testigo de identificación para el usuario del dispositivo DLUSIM. Aunque el PID no identifica al usuario per se, indica la autoridad del usuario para registrar el dispositivo DLUSIM que se suscribe con un cierto operador doméstico. Como resultará evidente para los expertos en la materia, el PID no tiene que ser único para cada dispositivo, pero debe ser difícil adivinar el PID que está asociado con cualquier PIMSI dada.

25 La solución general descrita en esta memoria puede ser ilustrada con el siguiente ejemplo, con referencia a la Figura 2. Un fabricante de dispositivos de medición ordena credenciales preliminares para cada dispositivo desde un Servicio de Registro 220. (Debe observarse que los nodos representados en la Figura 2 representan entidades funcionales; estos nodos pueden o no corresponder a nodos físicos discretos o a ubicaciones geográficas.) En algunas realizaciones, el Servicio de Registro 220 proporciona credenciales preliminares para cada dispositivo, acompañadas con toda la información relevante para el uso de una USIM descargable, incluyendo la PIMSI, las claves asociadas y el Identificador de IMSI Preliminar (PID), como se muestra en 212. En otros casos, el Servicio de Registro 220 proporciona sólo las credenciales preliminares, y el fabricante genera PIDs correspondientes, devolviendo los PIDs al Servicio de Registro 220 como se muestra en 222. En cualquier caso, el PID puede ser una clave numérica o alfanumérica u otro código. En algunos casos, el PID es preferiblemente legible por una persona, aunque éste no es necesariamente el caso. En cualquier caso, el fabricante 210 incluye las credenciales de PIMSI en el interior del dispositivo, por ejemplo, en la memoria no volátil del dispositivo, y proporciona el par PIMSI / PID al comprador del dispositivo. En algunas aplicaciones el fabricante 210 puede simplemente imprimir el número de PIMSI junto con el PID en una etiqueta, manual de instrucciones, folleto u otro similar. En aplicaciones de gran volumen, el fabricante 210 podría por el contrario proporcionar una base de datos electrónica de la PIMSI y los PIDs correspondientes a un abonado.

40 Cuando se despliega el dispositivo, el usuario final del dispositivo (representado en la Figura 2 en 230) desea crear una suscripción para el dispositivo para el servicio de red inalámbrica proporcionado por un operador de red particular, es decir, el Operador Doméstico. El usuario 230 del dispositivo accede de este modo a un servicio de suscripción 240 del operador de red proporcionado por el proveedor de servicios de su elección (es decir, el Operador Doméstico o un afiliado); el servicio de suscripción 240 puede ser proporcionado a través de un sitio web de la Internet. El usuario del dispositivo 230 entonces simplemente proporciona al servicio de suscripción 240 la PIMSI del dispositivo que se suscribe y el correspondiente PID, como se muestra en 232. (La Posesión del PID “prueba” que el usuario del dispositivo 230 realmente tiene el control del dispositivo correspondiente a la PIMSI.)

50 Una vez que esto se ha llevado a cabo, el Servicio de Suscripción 240 contacta con el Servicio de Registro 220 con la PIMSI, el PID correspondiente y los datos de identificación de la red del Operador Doméstico, como se muestra en 242. El Servicio de Suscripción 240 informa así al Servicio de Registro 220 de que el dispositivo identificado por la PIMSI es ahora servido por el Operador Doméstico. Para evitar registros fraudulentos, el Servicio de Registro 220 puede autenticar la solicitud de actualización de registro del Servicio de Suscripción 240 comparando el PID proporcionado con la solicitud con el PID previamente almacenado por el Servicio de Registro 220 en asociación con la correspondiente PIMSI. A menos que el PID coincida con el almacenado en el Servicio de Registro 220, la solicitud es denegada. Si la solicitud es autenticada, no obstante, entonces el Servicio de Registro 220 almacena los datos de identificación del Operador Doméstico en asociación con la PIMSI para el dispositivo. (En algunas realizaciones, el Servicio de Registro 220 puede devolver un mensaje de confirmación, como se muestra en 224.) Así, el Servicio de Registro 220 mantiene una base de datos que asocia las PIMSI del dispositivo con operadores de telefonía inalámbrica.

60 En algunas implementaciones, puede resultar deseable proporcionar seguridad adicional para el PID, para evitar una mala utilización por parte del operador del Servicio de Suscripción o por parte de alguien que obtenga acceso no autorizado a datos guardados por el Servicio de Suscripción. De acuerdo con esto, en algunas realizaciones de la invención, el propietario de un dispositivo puede contactar con el Servicio de Registro 220 antes de contactar con el Servicio de Suscripción 240, para solicitar un código de seguridad de una sola vez, que puede ser considerado como un PID secundario. Al propietario puede requerírsele que se autentique, utilizando la PIMSI y el PID del dispositivo,

antes de recibir el código de seguridad de una sola vez. Cuando a continuación contacta con el Servicio de Suscripción 240, el propietario entonces proporciona el código de seguridad de una sola vez al Servicio de Suscripción 240, en lugar del PID más permanente. El Servicio de Suscripción 240 a continuación proporciona el código de seguridad de una sola vez al Servicio de Registro 220 para su utilización en la autenticación de la solicitud de actualización de registro. El Servicio de Registro 220 puede entonces marcar el código de seguridad de una sola vez como no válido, de manera que no puede ser utilizado de nuevo.

Para una mayor seguridad, los códigos de seguridad de una sola vez emitidos pueden tener una limitación de vida útil "incorporada". En un planteamiento, el código de seguridad de una sola vez podría ser generado sobre la base de un código de fecha o un código de tiempo, por ejemplo, troceando la PIMSI, el PID y la hora actual. Cuando se está autenticando una solicitud de actualización de registro desde el Servicio de Suscripción 240, el Servicio de Registro 220 puede entonces repetir el mismo cálculo – si la fecha no coincide, entonces los resultados del cálculo diferirán y la solicitud será rechazada.

En cualquier caso, una vez que el Servicio de Registro 220 es notificado acerca del (nuevo) operador doméstico del dispositivo, el dispositivo puede utilizar sus credenciales preliminares para conectarse a la red y, a través del Servicio de Registro, averiguar cómo encontrar su red doméstica y descargar un USIM adecuado. Como se ha observado anteriormente, las credenciales preliminares identificadas mediante la PIMSI permiten al dispositivo M2M acceder temporalmente a la red. En algunas realizaciones, la PIMSI es indistinguible de una IMSI convencional. Así, a menos que la red a la cual se conecta el primer dispositivo sea por casualidad el operador que proporciona el servicio de registro (y por ello el operador que controla las credenciales preliminares), es probable que la red trate el dispositivo como lo haría cualquier otro dispositivo en itinerancia, y contacte con el operador de registro para la autenticación del dispositivo utilizando protocolos de itinerancia normales. Así, aunque el reconocimiento de la PIMSI como tal por parte de la red visitada es posible, no se requiere; el acceso a los servicios de red puede ser temporalmente proporcionado al dispositivo utilizando protocolos de telecomunicaciones convencionales. Además, resultará evidente para los expertos en la materia que el operador de registro puede limitar los servicios disponibles para el dispositivo hasta la descarga de un USIM real. En particular, el dispositivo M2M puede estar limitado a conexiones de datos al Servicio de Registro 220, y al Servicio de Suscripción 240 (o a otro servidor de aprovisionamiento). Así, cuando se activa, el dispositivo M2M 110 se conecta a una red disponible utilizando sus credenciales preliminares, y a continuación establece una conexión de datos al Servicio de Registro 220. Proporcionando su PIMSI al Servicio de Registro 220, como se muestra en 252, el Servicio de Registro 220 proporciona al dispositivo M2M 110 datos dirigiendo al dispositivo M2M 110 a un servidor de aprovisionamiento para el Operador Doméstico, como se muestra en 254. Por supuesto, el Servicio de Registro 220 puede requerir procedimientos de autenticación adicionales antes de proporcionar los datos de dirección del Operador Doméstico; estos procedimientos no se ilustran en la Figura 2. En cualquier caso, los datos del operador doméstico pueden comprender una dirección para el servidor de aprovisionamiento (por ejemplo, una dirección de IP, o URL), o pueden ser un parámetro que es utilizado por el dispositivo M2M 110 para obtener una dirección de una tabla de búsqueda, o para formar una dirección. En algunos casos, el servidor de aprovisionamiento puede ser parte del Servicio de Suscripción 240 del Operador Doméstico. En este caso, como se representa en la Figura 2, el dispositivo M2M 110 se conecta al Servicio de Suscripción 240, y proporciona su PIMSI, como se muestra en 256. En cambio, el Servicio de Suscripción 240 proporciona las credenciales de suscripción descargables, por ejemplo, un USIM descargable. De nuevo, el Servicio de Suscripción 240 probablemente requerirá procedimientos de autenticación adicionales antes de proporcionar las credenciales descargables; un amplio rango de procedimientos de autenticación aplicables son bien conocidos para los expertos en la materia.

Con la red de comunicación de ejemplo de la Figura 1 y el flujo de mensajes de ejemplo de la Figura 2 en mente, la Figura 3 ilustra un método general para el guardado de datos de registro electrónicos para una pluralidad de dispositivos inalámbricos. En algunas realizaciones, el método de la Figura 3, o una variante del mismo, puede ser implementado en un servidor de registro, tal como el servidor de registro 160 representado en la Figura 1, que proporciona servicios tales como los descritos en conexión con el Registro 220 de la Figura 2.

El método de la Figura 3 empieza con la recepción de una pluralidad de identificadores de dispositivo preliminares y códigos de seguridad procedentes del fabricante de un dispositivo, como se muestra en el bloque 310. En el método representado, a continuación, los identificadores de dispositivo preliminares (que pueden ser PIMSI) y los correspondientes códigos de seguridad (PIDs) son proporcionados a un servicio de registro por un fabricante. En otras realizaciones, los identificadores de dispositivo preliminares y los códigos de seguridad pueden ser proporcionados por uno o más operadores de red inalámbrica; uno de estos operadores de red inalámbrica puede asimismo operar el servicio de registro. En otras realizaciones, el operador del servicio de registro puede proporcionar a un fabricante los identificadores de dispositivo preliminares, y el fabricante puede proporcionar correspondientes códigos de seguridad.

En cualquier caso, los identificadores de servicio preliminares y los códigos de seguridad son almacenados, como se muestra en el bloque 320. Los identificadores de servicios preliminares y los códigos de seguridad son generalmente almacenados en una base de datos, que puede estar físicamente situada junto con el servicio de registro, tal como en el dispositivo de almacenamiento externo 170 representado en la Figura 1, o remotamente situado y accesible a través de una red de datos privada o pública.

En el bloque 330, el servicio de registro recibe una solicitud de actualización de registro desde un servicio de suscripción del operador. La solicitud de actualización de registro comprende un identificador de dispositivo, un código de seguridad candidato, y datos identificativos de la red del Operador Doméstico. Por ejemplo, una solicitud de actualización de registro puede ser parecida a “Registrar PIMSI: 224387123456789 al ‘Operador Doméstico’, PID: 746726”. En efecto, la solicitud de actualización de registro es una instrucción para ligar el identificador del dispositivo a los datos de la red del Operador Doméstico. Aunque se describe en esta memoria como una solicitud de “actualización” de registro, tal solicitud puede establecer tal enlace por primera vez. Así, puede utilizarse una orden de un único formato para establecer nuevos registros o para actualizar registros establecidos previamente. En otras realizaciones, puede utilizarse una orden o procedimiento separados para actualizar registros previamente establecidos.

En cualquier caso, el código de seguridad candidato se utiliza para autenticar la solicitud, como se muestra en el bloque 340, estableciendo con ello que el solicitante (por ejemplo, el servicio de suscripción del operador) está autorizado para actualizar la información de registro. De acuerdo con esto, el identificador del dispositivo proporcionado se utiliza para obtener información almacenada asociada con el identificador del dispositivo que coincide en la memoria, y el código de seguridad candidato es comparado con el código de seguridad ya almacenado en asociación con el identificador del dispositivo proporcionado. Si coincide, la solicitud de actualización de registro es autorizada, y los datos del operador doméstico son almacenados, como se muestra en el bloque 350, junto con el identificador del dispositivo que coincide y el código de seguridad.

En algún momento posterior, el dispositivo inalámbrico puede acceder al servicio de registro correspondiente al identificador de dispositivo preliminar procesado en los bloques 320 – 350. Así, como se muestra en el bloque 360, se recibe una solicitud de conexión desde el dispositivo inalámbrico. Esta solicitud de conexión puede tomar una variedad de formas, pero generalmente comprenderá al menos un mensaje que incluye la PIMSI que identifica al dispositivo. Pueden asimismo emplearse procedimientos de autenticación, para asegurar que la solicitud de conexión realmente se origina en el dispositivo inalámbrico identificado por la PIMSI. Por ejemplo, puede utilizarse tecnología de Infraestructura de Clave Pública (PKI – Public Key Infrastructure, en inglés) para validar un mensaje firmado por el dispositivo inalámbrico utilizando una clave secreta o un certificado almacenado en el dispositivo.

Cuando se recibe la solicitud de conexión (y cuando se completa con éxito alguno de los procedimientos de autenticación), los datos de la red doméstica son enviados al dispositivo inalámbrico, como se muestra en el bloque 370. Como se ha observado anteriormente, estos datos de la red doméstica pueden en algunos casos comprender una dirección de red, tal como una dirección de Protocolo de Internet (IP – Internet Protocol, en inglés), o un Localizador de Recurso Uniforme (URL – Uniform Resource Locator, en inglés), para su uso por parte del dispositivo inalámbrico en el acceso a y la descarga de credenciales de suscripción. En otros casos, los datos de la red doméstica pueden incluir un puntero hacia tal dirección de red. Por ejemplo, los datos de la red doméstica pueden incluir un parámetro utilizado por el dispositivo inalámbrico para indexar una tabla de búsqueda almacenada que contiene varias direcciones de red. Alternativamente, los datos de la red doméstica pueden incluir un parámetro que puede ser utilizado para calcular o formar una dirección de red completa. Por ejemplo, los datos de la red doméstica pueden incluir un código alfanumérico que puede ser combinado con una plantilla almacenada para formar una URL específica para un operador.

El método de la Figura 3 representa en general un método para el registro inicial y la activación de un dispositivo inalámbrico. Las etapas ilustradas en los bloques 310 y 320 pueden así ejecutarse incluso antes de que el dispositivo sea vendido. En tal caso, la entrada al Servicio de Registro para un identificador de dispositivo preliminar dado puede indicar que no existe ningún Operador Doméstico definido para el dispositivo en cuestión. Tras el bloque 350, la entrada incluye un campo que indica el Operador Doméstico. Por supuesto, resultará evidente para los expertos en la materia que el método ilustrado en la Figura 3 no es sino un planteamiento de ejemplo para proporcionar un procedimiento de activación.

En el caso de que un dispositivo sea revendido o nuevamente desplegado, la suscripción asociada con un dispositivo inalámbrico puede ser cambiada. En algunos casos, por supuesto, el propietario de un dispositivo puede simplemente cambiar de operador. En cualquier caso, los datos de la red doméstica asociados con un identificador de dispositivo preliminar pueden necesitar ser actualizados. Además, el usuario puede solicitar un cambio al código de seguridad asociado con un dispositivo; una solicitud de cambio de código de seguridad puede estar separada de o junto con un cambio en los datos de suscripción. Así, en algunas realizaciones, un servicio de registro, tal como un servicio de registro implementado en el servidor de registro 160 de la Figura 1, puede actualizar uno o más parámetros asociados con un registro de dispositivo de acuerdo con el método de la Figura 4.

El método de la Figura 4 empieza en el bloque 410, con la recepción de una solicitud de actualización del código de seguridad. La solicitud de actualización de código de seguridad incluye el identificador de servicio y el nuevo código de seguridad, y debería generalmente incluir un código de seguridad candidato correspondiente al código de seguridad ya almacenado por el servicio de registro. Opcionalmente, la solicitud de actualización de código de seguridad puede asimismo incluir datos de la red doméstica actualizados. Por ejemplo, una solicitud de actualización del código de seguridad puede ser parecida a: “Registrar PIMSI: 224387123456789 a ‘Nuevo Operador Doméstico’,

PID: 746726, NUEVOPID: hxus82H". (Aunque denominada "solicitud de actualización del código de seguridad" para el propósito de esta explicación, una o más realizaciones de la invención puede o pueden emplear un único formato de solicitud de actualización que permite actualizaciones a uno o a los dos del código de seguridad o la red doméstica. Como se ha observado anteriormente, este mismo formato de solicitud puede asimismo soportar un registro inicial de los datos de la red doméstica. Otras realizaciones pueden requerir órdenes separadas para la actualización del código de seguridad y de los datos de la red doméstica. Así, para el propósito de esta explicación, el término "solicitud" puede incluir uno o varios mensajes u órdenes.)

En el bloque 420, el código de seguridad candidato proporcionado en la solicitud de actualización es utilizado para la autenticación de la solicitud. Así, en algunas realizaciones, el identificador del dispositivo proporcionado es hecho coincidir con un identificador de dispositivo preliminar almacenado, y el código de seguridad candidato es comparado con el código de seguridad almacenado en asociación con el identificador de dispositivo preliminar coincidente. Si los códigos de seguridad coinciden, la solicitud es autorizada, y el código de seguridad actualizado es almacenado en asociación con el identificador de dispositivo preliminar almacenado, como se muestra en el bloque 430. En algunas realizaciones, el código de seguridad original es actualizado, o sobrescrito, por el nuevo código de seguridad; en otras realizaciones el código de seguridad original puede ser mantenido junto con el nuevo código de seguridad.

De manera similar, en el bloque 440, los datos de la red doméstica actualizados, si son proporcionados con la solicitud de actualización, son almacenados en asociación con el identificador de dispositivo preliminar coincidente. Los datos de la red doméstica actualizados son utilizados en el caso de que el correspondiente dispositivo solicite a continuación una conexión a su servidor de aprovisionamiento del operador doméstico.

La Figura 5 ilustra un método de ejemplo para la actualización de los datos de registro para un dispositivo inalámbrico. Todo o parte del método de la Figura 5, puede ser implementado, por ejemplo, en un servidor de suscripción, tal como el servidor de suscripción 180 de la Figura 1, operado por un operador de red inalámbrica. Así, la Figura 5 ilustra un procedimiento de ejemplo que podría seguirse cuando un propietario de dispositivo busca conectarse a un dispositivo inalámbrico a una nueva o existente suscripción con el operador de la red inalámbrico.

El método de la Figura 5 empieza, como se muestra en el bloque 510, con la recepción de una solicitud de suscripción para un dispositivo inalámbrico. Esta solicitud de suscripción puede ser recibida del propietario del dispositivo, en algunos casos a través de una interfaz de sitio de red de Internet. En algunos casos, la solicitud de suscripción puede ser para un único dispositivo. En otros, el propietario de un dispositivo puede proporcionar una solicitud de suscripción de gran volumen identificando varios dispositivos inalámbricos. En cualquier caso, la solicitud de suscripción incluye al menos un identificador de dispositivo preliminar y un código de seguridad correspondiente, y puede incluir otra información, tal como información identificativa para el propietario del dispositivo, información del número de cuenta, información de pago, u otros similares. (Como se ha observado anteriormente, "solicitud" en este contexto puede referirse a un único mensaje, o a una serie de mensajes y órdenes.)

Como se ha descrito anteriormente, al propietario del dispositivo puede haberse proporcionado el identificador de dispositivo preliminar y el código de seguridad en el momento de la compra. Proporcionando estos parámetros al servicio de suscripción, el propietario del dispositivo busca conectar el correspondiente dispositivo inalámbrico a una suscripción activa con el operador de red inalámbrico que proporciona el servicio de suscripción.

En el bloque 520, una solicitud de actualización de registro es enviada a un servicio de registro. La solicitud de actualización de registro incluye al menos el identificador del dispositivo y el código de seguridad proporcionado por el propietario del dispositivo. La solicitud de actualización de registro puede asimismo incluir datos identificativos de la red doméstica para el dispositivo inalámbrico. La solicitud de actualización puede ser procesada por el servidor de registro de acuerdo con los métodos descritos anteriormente en referencia a las Figuras 3 y 4.

En algunas realizaciones, el servicio de suscripción puede seleccionar un servicio de registro apropiado de entre varios servicios disponibles. Por ejemplo, existen varios servicios de registro en diferentes regiones geográficas. En tal escenario, los dispositivos M2M destinados para una particular región pueden ser fabricados con credenciales preliminares asociadas con el servicio de registro regional más cercano. La identificación del servicio de registro apropiado por parte del servicio de suscripción puede estar basada en el identificador del dispositivo preliminar o en otra información relacionada con el dispositivo. Por ejemplo, diferentes bloques de PIMSI pueden corresponder a diferentes servicios de registro, en cuyo caso el servicio de registro apropiado puede ser identificado simplemente examinando el identificador del dispositivo preliminar. En otros casos, el servicio de registro apropiado puede corresponder al fabricante del dispositivo, o al tipo de dispositivo.

Los datos de la red doméstica proporcionados al servicio de registro son utilizados por el servicio de registro para conectar el dispositivo inalámbrico al operador doméstico. El servicio de registro utiliza esta información posteriormente para dirigir al dispositivo inalámbrico a una dirección de red apropiada para la descarga de credenciales de suscripción, tal como un USIM descargable. El servicio de descarga de credenciales es una parte de los servicios de suscripción del operador inalámbrico; en algunos casos este servicio de descarga puede ser efectuado utilizando el mismo servidor utilizado para proporcionar la gestión de la solicitud de suscripción explicada



anteriormente, mientras que en otros puede ser proporcionada por un servidor de aprovisionamiento separado. Este servicio de descarga se ilustra así en la Figura 5 en los bloques 530 y 540. En el bloque 530, una solicitud de descarga de credencial es recibida de un dispositivo inalámbrico a través de la red inalámbrica. Esta solicitud puede tomar cualquiera de varias formas, como se ha explicado anteriormente, y puede incluir procedimientos de autenticación para asegurar que la solicitud se originó en un dispositivo autorizado. Como se ha observado anteriormente, tales procedimientos de autenticación pueden incluir, por ejemplo, el uso de certificados PKI para autenticar un mensaje firmado digitalmente desde el dispositivo inalámbrico. En cualquier caso, durante una correcta autenticación, si se produce, las credenciales de suscripción son enviadas al dispositivo inalámbrico, como se representa en el bloque 540. Estas credenciales de suscripción pueden ser utilizadas por el dispositivo inalámbrico para un subsiguiente acceso a su red doméstica, y para un acceso a los servicios a los cuales el propietario del dispositivo se ha suscrito.

Como se ha observado anteriormente, los servicios de registro y los servicios de suscripción descritos en esta memoria pueden ser proporcionados sobre una red de datos pública, una red de datos privada, o ambas. En algunos casos, uno o ambos servicios pueden ser proporcionados utilizando sitios web accesibles a través de la Internet. Las Figuras 6 y 7 proporcionan así diagramas de bloques simplificados de un servidor de registro 160 y un servidor de suscripción 180 de ejemplo, respectivamente. Los servidores 160 y 180 pueden comprender equipos de servidor de datos de red convencionales configurados para poner en práctica uno o más de los métodos descritos anteriormente.

En particular, el servidor de registro 160 comprende una unidad de procesamiento 610, que puede incluir uno o más microprocesadores de propósito general configurados con el software apropiado para poner en práctica uno o más de los métodos descritos anteriormente junto con las Figuras 3 y 4. El servidor de registro 160 comprende asimismo una interfaz de red 630, que proporciona acceso a una red de datos privada o pública, tal como la Internet, y una unidad de almacenamiento 620. La unidad de almacenamiento 620 puede comprender uno o más dispositivos de memoria situados conjuntamente con los otros componentes del servidor de registro 160. La unidad de almacenamiento 620 puede asimismo, o en lugar de, comprender uno o más dispositivos de memoria situados remotamente de los otros componentes del servidor de registro 160.

Así, en algunas realizaciones, la unidad de almacenamiento 620 está configurada para almacenar una pluralidad de identificadores de dispositivo preliminares y correspondientes códigos de seguridad, donde cada identificador de dispositivo preliminar está asociado con un dispositivo inalámbrico. En algunas realizaciones, los identificadores de dispositivo preliminares pueden comprender PIMSI. En algunas realizaciones, los códigos de seguridad pueden comprender códigos legibles por personas. En algunas realizaciones, la unidad de procesamiento 610 del servidor de registro 160 está configurada para la recepción de una solicitud de actualización de registro a través de la interfaz de red 630, comprendiendo la solicitud de actualización de registro un primer identificador de dispositivo, un primer código de seguridad candidato y datos de la red doméstica correspondientes a la red de un operador. La unidad de procesamiento 610 está asimismo configurada para la autenticación de la solicitud de actualización de registro comparando el primer identificador del dispositivo y el primer código de seguridad del dispositivo con los identificadores del dispositivo preliminares y los códigos de seguridad almacenados para la identificación de un identificador de dispositivo coincidente y un código de seguridad coincidente. Si el código de seguridad candidato coincide con el código de seguridad almacenado, entonces los datos de la red doméstica son almacenados en la unidad de almacenamiento 620 en asociación con el identificador de dispositivo coincidente y el código de seguridad coincidente.

En algunas realizaciones, la unidad de procesamiento 610 está asimismo configurada para recibir una solicitud de actualización del código de seguridad a través de la interfaz de red 630, comprendiendo la solicitud de actualización de código de seguridad un segundo identificador de dispositivo, un segundo código de seguridad candidato y un código de seguridad actualizado. En tales realizaciones, la unidad de procesamiento 610 puede estar asimismo configurada para la autenticación de la solicitud de actualización de código de seguridad comparando el segundo código de seguridad candidato con el código de seguridad almacenado en la unidad de almacenamiento 620 en asociación con el identificador del dispositivo. Si la solicitud es autenticada con éxito, entonces el código de seguridad actualizado es almacenado en la unidad de almacenamiento 620 en asociación con el identificador del dispositivo.

En algunas realizaciones, la unidad de procesamiento 610 está asimismo configurada para la recepción de una solicitud de conexión, a través de la interfaz de red 630, desde un dispositivo inalámbrico correspondiente a un identificador de dispositivo preliminar almacenado y para el envío de al menos una porción de los datos de la red doméstica correspondiente al dispositivo inalámbrico. Los datos de la red doméstica enviados al dispositivo inalámbrico pueden incluir una dirección de red para su uso por parte del dispositivo inalámbrico en la descarga de las credenciales de suscripción, o un puntero hacia tal dirección de red.

El servidor de suscripción 180 comprende asimismo una interfaz de red 720, que proporciona acceso a una red de datos privada o pública, y una unidad de procesamiento 710, que puede incluir uno o más microprocesadores de propósito general configurado o configurados con el software apropiado para poner en práctica uno o más de los métodos descritos anteriormente en conjunción con la Figura 5. Así, en algunas realizaciones la unidad de

- procesamiento 710 de la suscripción está configurada para la recepción de una solicitud de suscripción para un dispositivo inalámbrico suscrito a través de la interfaz de red 720, incluyendo la solicitud de suscripción un identificador de dispositivo preliminar y un código de seguridad correspondiente para el dispositivo inalámbrico que se está suscribiendo. La unidad de procesamiento 710 está asimismo configurada para enviar una solicitud de actualización de registro electrónico a un servidor de registro, a través de la interfaz de red 720, incluyendo la solicitud de actualización de registro el identificador de dispositivo preliminar, el código de seguridad, y datos de la red doméstica para el dispositivo inalámbrico que se suscribe. Los datos de la red doméstica identifican (directa o indirectamente) una dirección de red para la descarga de credenciales de suscripción.
- 5
- 10 En algunas realizaciones, el servidor de suscripción 180 está asimismo configurado para recibir posteriormente una solicitud de descarga de credencial del dispositivo inalámbrico que se suscribe, a través de la interfaz de red 720, dirigida a la dirección de red identificada por los datos de la red doméstica.
- 15 El servidor de suscripción 180 descarga a continuación las credenciales de suscripción, tales como un USIM descargable, al dispositivo inalámbrico que se suscribe para su subsiguiente uso en el acceso a los servicios de red. En algunas realizaciones, puede llamarse a procedimientos de autenticación antes de la descarga de las credenciales de suscripción, para asegurar que la solicitud de descarga de credencial se origina en un dispositivo autorizado.
- 20 Resultará evidente para los expertos en la materia que un operador de red puede proporcionar servicios de registro, como se ha descrito de manera general en esta memoria, así como los servicios de suscripción descritos anteriormente. En tal caso, los servicios de registro y los servicios de suscripción pueden ser proporcionados utilizando servidores separados, o utilizando uno o más de los mismos servidores. Además, resultará evidente para los expertos en la materia que las diferentes unidades de procesamiento descritas anteriormente pueden comprender cada una un único microprocesador y el software asociado, o puede comprender dos o más microprocesadores configurados para efectuar de manera conjunta las diferentes funciones descritas anteriormente.
- 25
- 30 Las presentes realizaciones deben ser así consideradas a todos los respectos como ilustrativas y no restrictivas, y todos los cambios que se encuentren dentro del significado y rango de equivalencia de las reivindicaciones adjuntas pretenden estar abarcados en las mismas.

**REIVINDICACIONES**

1. Un método para guardar datos de registro electrónicos para una pluralidad de dispositivos inalámbricos, **caracterizado por que** el método comprende:
- 5 almacenar (320) una pluralidad de identificadores de dispositivo preliminares y correspondientes códigos de seguridad, donde cada identificador de dispositivo preliminar está asociado con un dispositivo inalámbrico; recibir (330) una solicitud de actualización de registro para un primer dispositivo inalámbrico, comprendiendo la solicitud de actualización de registro un primer identificador de dispositivo y un primer código de seguridad candidato y datos de la red doméstica;
- 10 autenticar (340) la solicitud de actualización de registro comparando el primer código de seguridad candidato con un código de seguridad almacenado correspondiente al primer identificador de dispositivo; y almacenar (350) datos de la red doméstica para el primer dispositivo inalámbrico en asociación con el primer identificador de dispositivo y el correspondiente código de seguridad, si el primer código de seguridad candidato coincide con el código de seguridad almacenado correspondiente al primer identificador del dispositivo.
- 15
2. El método de la reivindicación 1, en el que almacenar (350) los datos de la red doméstica comprende actualizar datos de la red doméstica previos asociados con el primer identificador de dispositivo y el correspondiente código de seguridad.
- 20
3. El método de la reivindicación 1, en el que los datos de la red doméstica para el primer dispositivo inalámbrico comprenden una dirección de red para su uso por parte del primer dispositivo inalámbrico en la descarga de las credenciales de suscripción.
- 25
4. El método de la reivindicación 1, que comprende asimismo:
- recibir (410) una solicitud de actualización del código de seguridad, comprendiendo la solicitud de actualización de código de seguridad un segundo identificador de dispositivo, un segundo código de seguridad candidato y un código de seguridad actualizado;
- 30 autenticar (420) la solicitud de actualización de código de seguridad comparando el segundo código de seguridad candidato con un segundo código de seguridad almacenado correspondiente al segundo identificador de dispositivo; y almacenar (430) el código de seguridad actualizado en asociación con el segundo identificador de dispositivo.
- 35
5. El método de la reivindicación 4, en el que almacenar el código de seguridad actualizado en asociación con el segundo identificador de dispositivo comprende reemplazar el segundo código de seguridad almacenado con el código de seguridad actualizado.
- 40
6. El método de la reivindicación 1, que comprende asimismo:
- recibir una solicitud de conexión desde el primer dispositivo inalámbrico correspondiente al primer identificador de dispositivo; y
- 45 enviar al menos una porción de los datos de la red doméstica al primer dispositivo inalámbrico.
7. El método de la reivindicación 6, en el que cada porción de datos de la red doméstica comprende uno de una dirección de red y un puntero hacia una dirección de red, para su uso por parte del primer dispositivo inalámbrico en la descarga de las credenciales de suscripción.
- 50
8. El método de la reivindicación 1, en el que el código de seguridad almacenado correspondiente al primer identificador de dispositivo comprende un código de seguridad de una sola vez, y donde el método comprende asimismo rechazar una segunda solicitud de actualización de registro que comprende el primer identificador de dispositivo y el código de seguridad de una sola vez.
- 55
9. Un método para la actualización de datos de registro para dispositivos inalámbricos, **caracterizado por que** el método comprende:
- recibir (510) una solicitud de suscripción para un primer dispositivo inalámbrico, comprendiendo la solicitud de suscripción un identificador de dispositivo preliminar y un correspondiente código de seguridad;
- 60 enviar (520) una solicitud de actualización de registro a un servidor de registro, comprendiendo la solicitud de actualización de registro el identificador de dispositivo preliminar, el correspondiente código de seguridad y los datos de la red doméstica para el primer dispositivo inalámbrico, donde los datos de la red doméstica identifican una dirección de red para la descarga de las credenciales de suscripción;
- 65 recibir (530) una solicitud de descarga de credencial desde el primer dispositivo inalámbrico a través de la dirección de red identificada por los datos de la red doméstica; y

enviar (540) credenciales de suscripción al primer dispositivo inalámbrico para su uso en el acceso a servicios de red.

5 10. El método de la reivindicación 9, que comprende asimismo la selección del servidor de registro de entre una pluralidad de servidores de registro disponibles sobre la base del identificador de dispositivo preliminar.

10 11. Un servidor de registro (160) para el guardado de datos de registro electrónicos para una pluralidad de dispositivos inalámbricos, comprendiendo el servidor de registro una interfaz de red (630), una unidad de procesamiento (610) y una unidad de almacenamiento (620) configurada para almacenar una pluralidad de identificadores de dispositivo preliminares, donde cada identificador de dispositivo preliminar está asociado con un dispositivo inalámbrico, **caracterizado por que:**

15 la unidad de almacenamiento (620) está configurada para almacenar códigos de seguridad correspondientes a los identificadores de dispositivo preliminares; y  
la unidad de procesamiento (610) está configurada para recibir una solicitud de actualización de registro a través de la interfaz de red, comprendiendo la solicitud de actualización de registro un primer identificador de dispositivo, un primer código de seguridad candidato y datos de la red doméstica para un primer dispositivo inalámbrico;  
20 autenticar la solicitud de actualización de registro comparando el primer código de seguridad candidato con un código de seguridad candidato correspondiente al primer identificador de dispositivo; y  
almacenar los datos de la red doméstica en la unidad de almacenamiento (620) en asociación con el primer identificador de dispositivo y el correspondiente código de seguridad, si el primer código de seguridad candidato coincide con el código de seguridad almacenado correspondiente al primer identificador de dispositivo.

25 12. El servidor de registro (160) de la reivindicación 11, en el que la unidad de procesamiento (610) está configurada para almacenar los datos de la red doméstica actualizando los datos de la red doméstica previos asociados con el primer identificador de dispositivo y almacenando los datos de la red doméstica actualizados en la unidad de almacenamiento (620) en asociación con el primer identificador de dispositivo.

30 13. El servidor de registro (160) de la reivindicación 11, en el que la unidad de procesamiento (610) está asimismo configurada para:

35 recibir una solicitud de actualización de código de seguridad a través de la interfaz de red (630), comprendiendo la solicitud de actualización de código de seguridad un segundo identificador de dispositivo, un segundo código de seguridad candidato y un código de seguridad actualizado;  
autenticar la solicitud de actualización de código de seguridad comparando el segundo código de seguridad candidato con un segundo código de seguridad almacenado correspondiente al segundo código de seguridad; y  
40 almacenar el código de seguridad actualizado en la unidad de almacenamiento (620) en asociación con el segundo identificador de dispositivo.

45 14. El servidor de registro (160) de la reivindicación 13, en el que la unidad de procesamiento (610) está configurada para almacenar el código de seguridad actualizado en asociación con el segundo identificador de dispositivo reemplazando el segundo código de seguridad almacenado con el código de seguridad actualizado.

15. El servidor de registro (160) de la reivindicación 11, en el que la unidad de procesamiento (610) está asimismo configurada para:

50 recibir una solicitud de conexión a través de la interfaz de red (630) desde el primer dispositivo inalámbrico correspondiente al primer identificador de dispositivo; y  
enviar al menos una porción de los datos de la red doméstica al primer dispositivo inalámbrico a través de la interfaz de red (630).

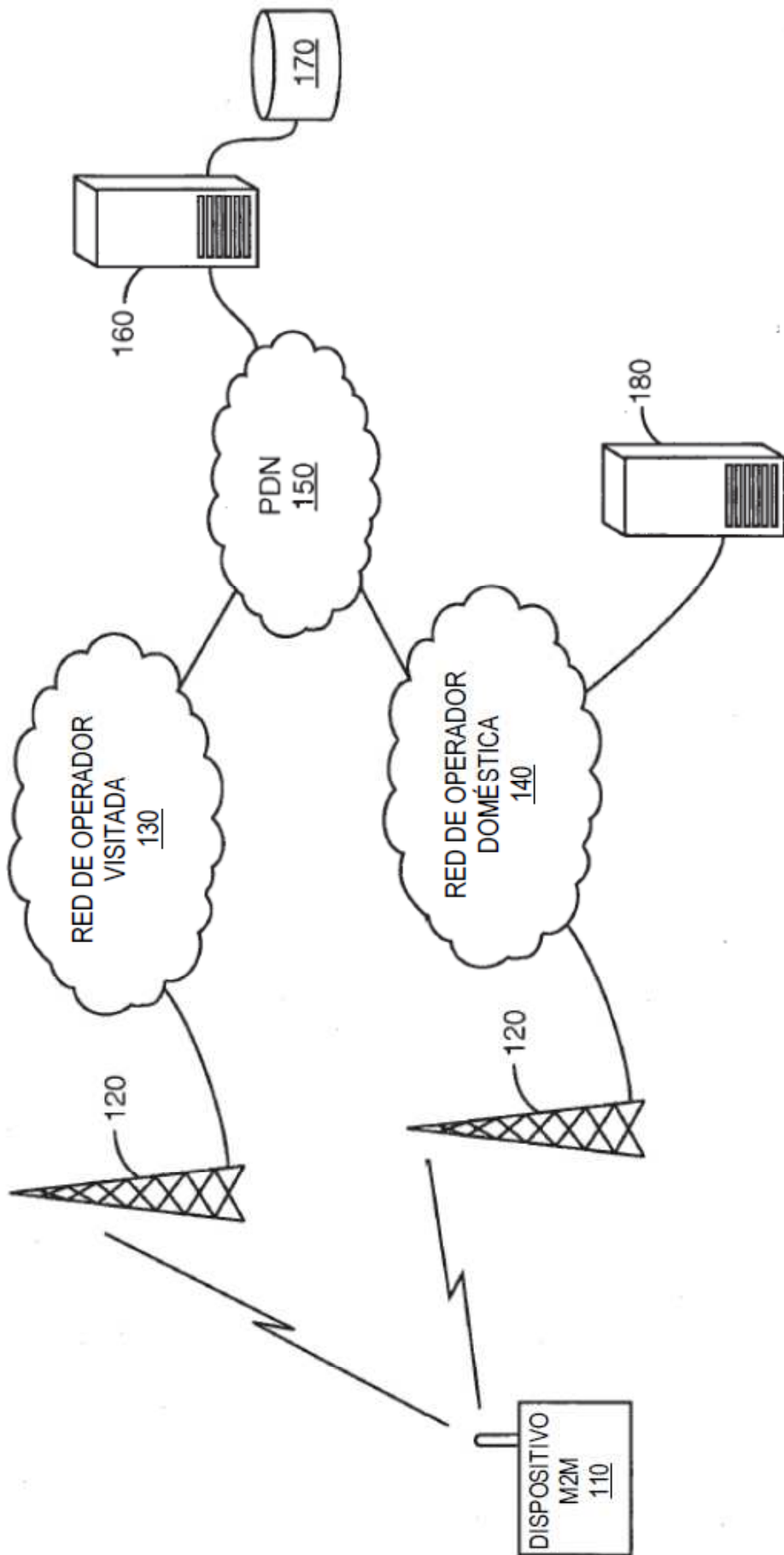


FIG. 1

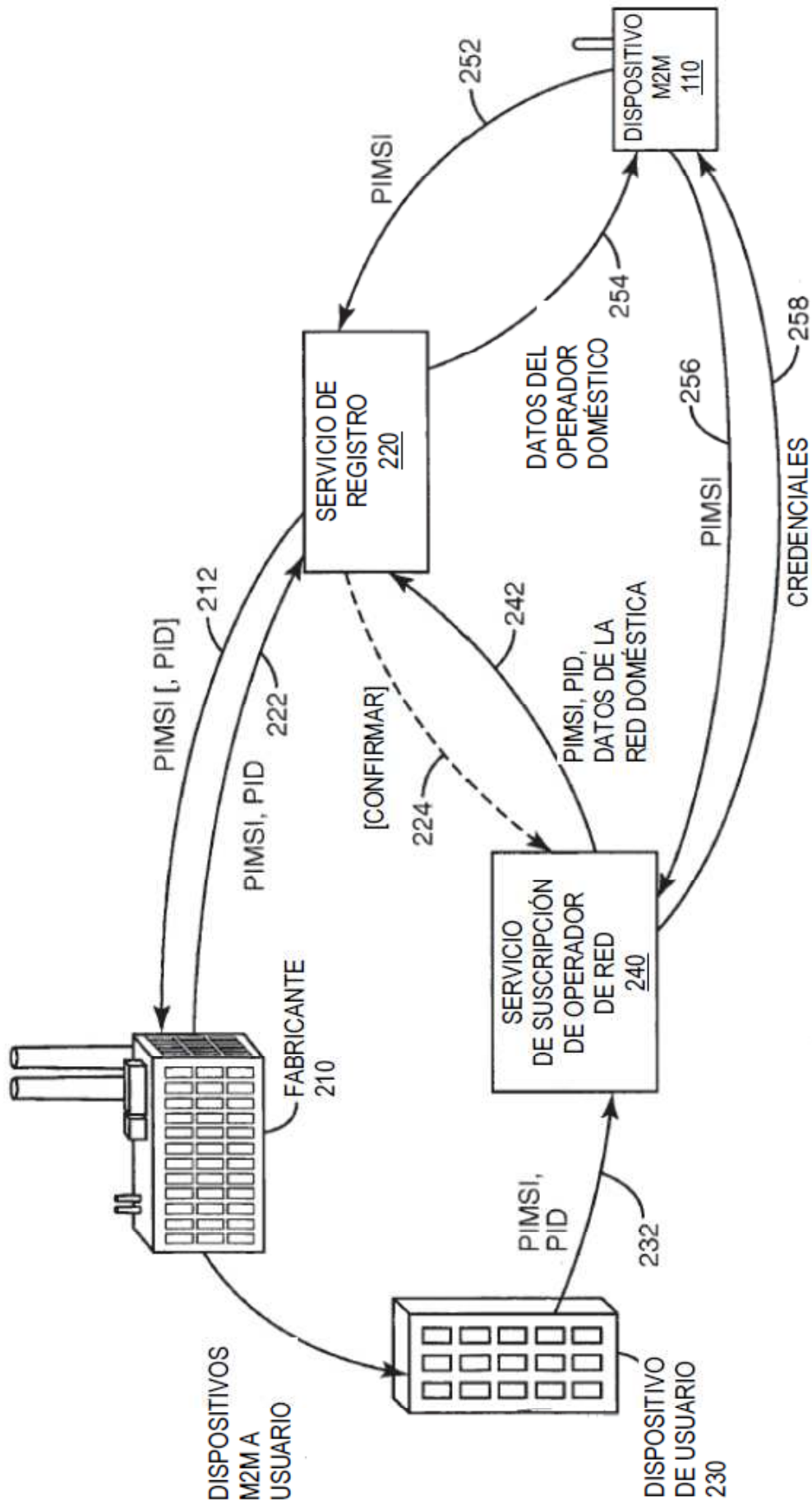
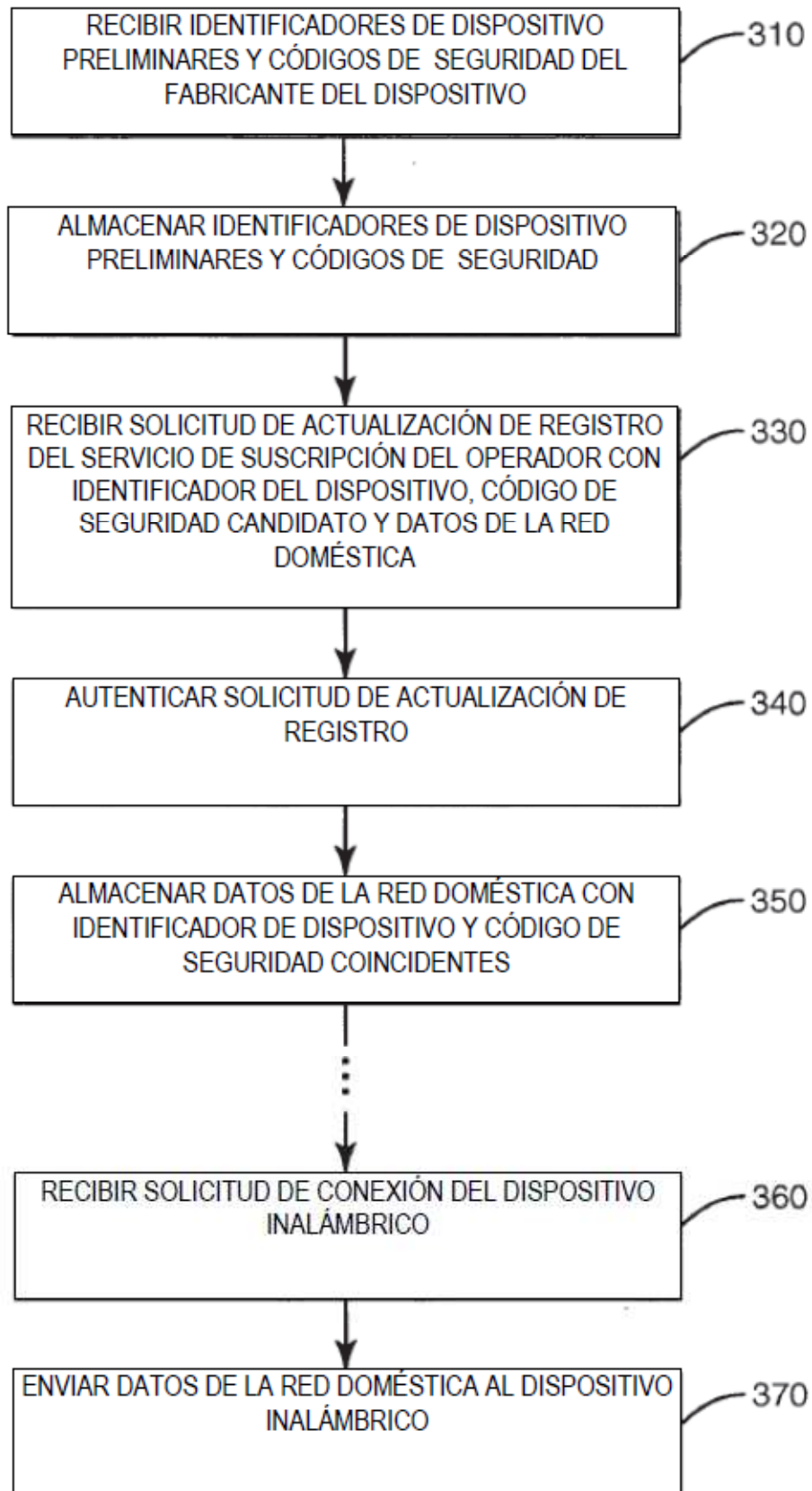
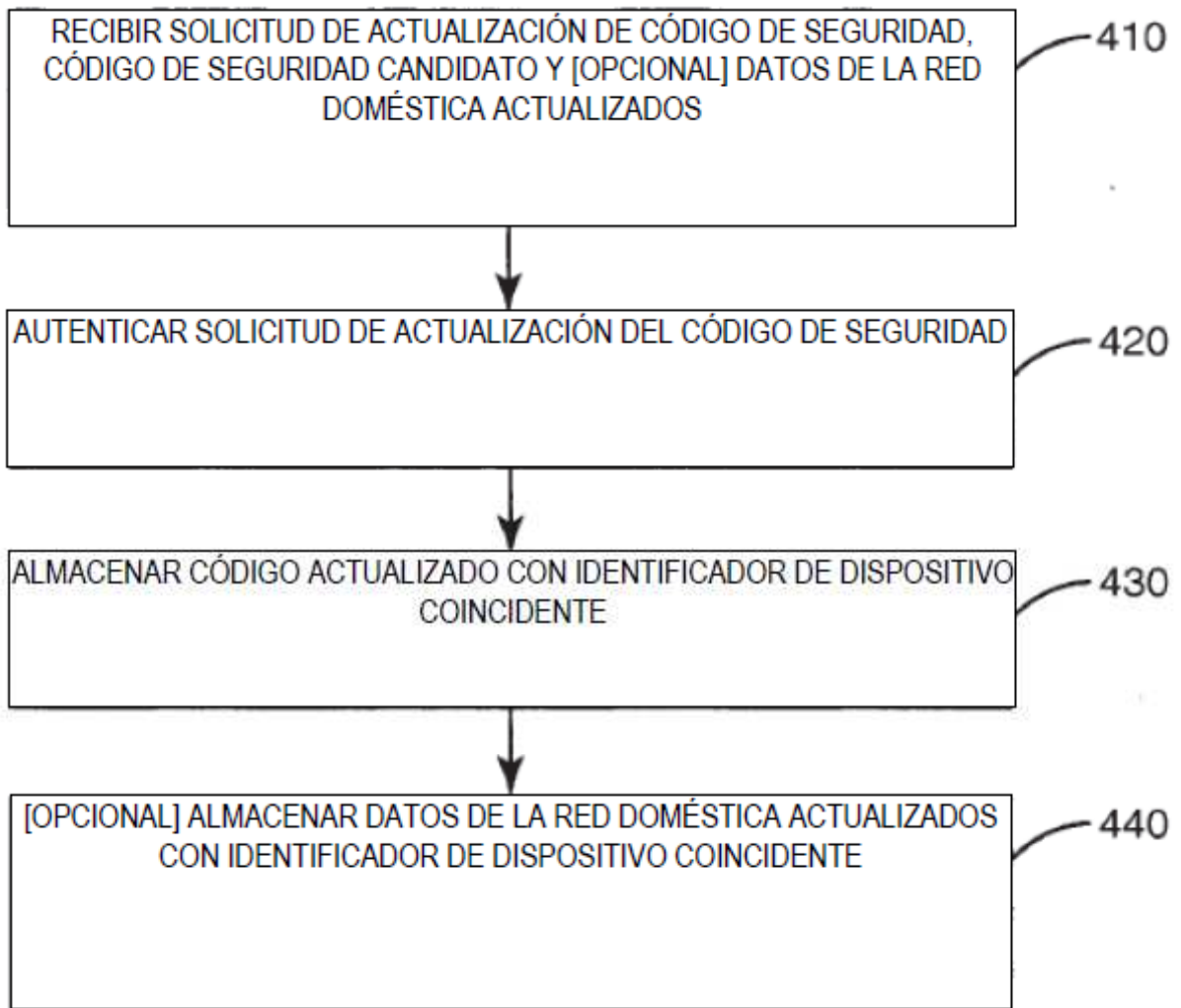


FIG. 2

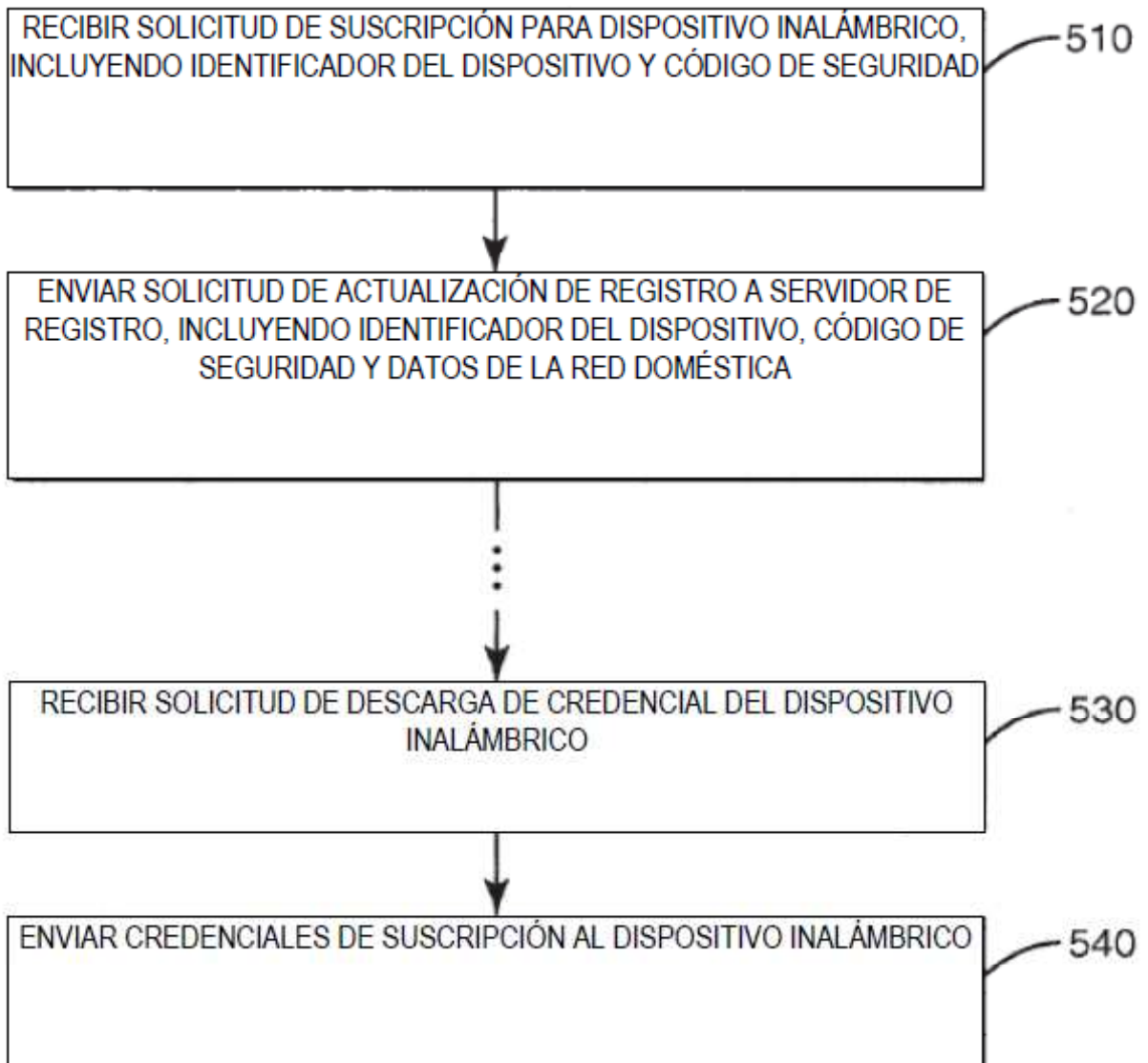


**FIG. 3**



**FIG. 4**





**FIG. 5**

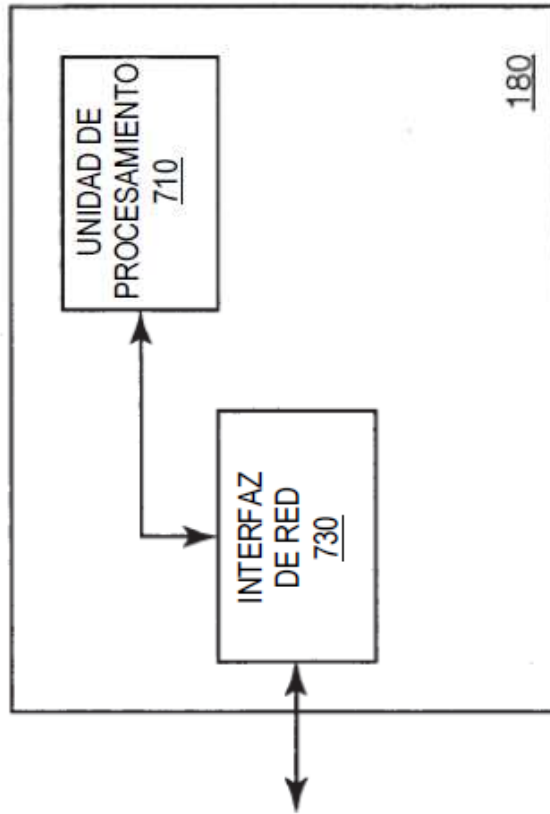


FIG. 7

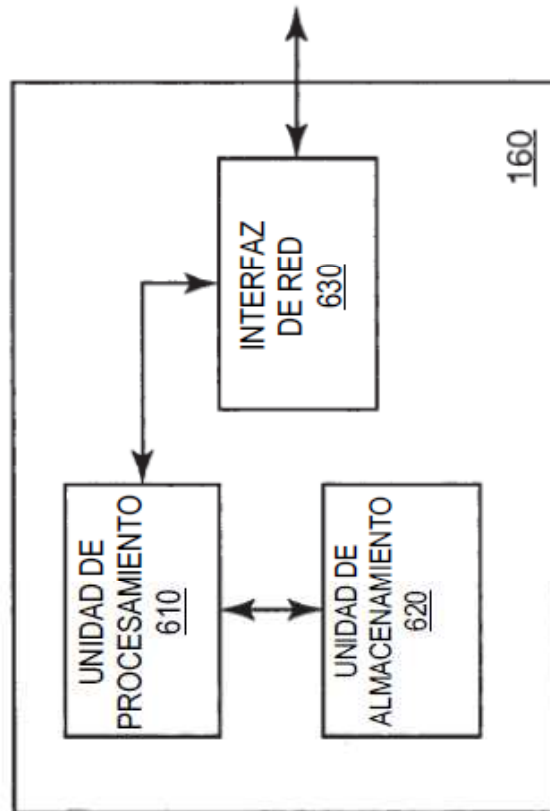


FIG. 6