(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 755 953**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04W 8/20 (2009.01)
H04W 4/00 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.05.2013 PCT/US2013/040811**

(87) Fecha y número de publicación internacional: **21.11.2013 WO13173246**

(96) Fecha de presentación y número de la solicitud europea: **13.05.2013 E 13727688 (7)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2019 EP 2850806**

(54) Título: **Sistemas y procedimientos para la gestión remota de credenciales**

(30) Prioridad:

14.05.2012 US 201261646792 P
25.01.2013 US 201313750816

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2020

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
International IP Administration 5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

PALANIGOUNDER, ANAND

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Sistemas y procedimientos para la gestión remota de credenciales

ANTECEDENTES

Campo

[0001] La presente solicitud se refiere, en general, a los sistemas de comunicación inalámbrica y, más específicamente, a los sistemas, procedimientos y dispositivos para la gestión remota de credenciales dentro de los sistemas de comunicación inalámbrica.

Antecedentes

[0002] En muchos sistemas de telecomunicación, las redes de comunicaciones se pueden usar para intercambiar mensajes entre varios dispositivos separados espacialmente que interactúan. Las redes pueden clasificarse de acuerdo con el alcance geográfico, que podría ser, por ejemplo, un área metropolitana, un área local o un área personal. Dichas redes se designarían respectivamente como una red de área amplia (WAN), una red de área metropolitana (MAN), una red de área local (LAN) o una red de área personal (PAN). Las redes difieren también de acuerdo con la técnica de conmutación/encaminamiento usada para interconectar los diversos nodos y dispositivos de red (por ejemplo, conmutación de circuitos frente a conmutación de paquetes), el tipo de medios físicos empleados para la transmisión (por ejemplo, cableados frente a inalámbricos) y el conjunto de protocolos de comunicación usados (por ejemplo, la familia de protocolos de Internet, SONET (red óptica síncrona), Ethernet, etc.).

[0003] A menudo se prefieren las redes inalámbricas cuando los elementos de red son móviles y por tanto tienen necesidades de conectividad dinámica, o si la arquitectura de red está formada en una topología ad hoc, en lugar de una fija. Las redes inalámbricas emplean medios físicos intangibles en una modalidad de propagación no guiada, usando ondas electromagnéticas en las bandas de frecuencia de radio, microondas, infrarrojos, óptica, etc. Las redes inalámbricas facilitan de forma ventajosa la movilidad del usuario y el rápido despliegue sobre el terreno en comparación con las redes alámbricas fijas.

[0004] Antes de que un dispositivo pueda comenzar a usar una red, el dispositivo puede necesitar proporcionar información a la red que lo identifica y, en algunos casos, información de abono asociada. La información de abono puede incluir el nivel de servicio, los servicios de red disponibles y otras características que puede usar el dispositivo. En algunas implementaciones, el identificador del dispositivo puede ser suficiente para identificar la información de abono asociada.

[0005] Por ejemplo, para obtener el servicio celular de un operador a elección del usuario, la electrónica de consumo celular (por ejemplo, tabletas electrónicas, teléfonos inteligentes, teléfonos mejorados, cámaras) o dispositivos de máquina a máquina (M2M) (por ejemplo, medidores de servicios inteligentes, sensores, dispositivos de asistencia para vehículos) típicamente requieren que el usuario compre una tarjeta SIM del operador y la instale en el dispositivo. De forma alternativa, los dispositivos pueden venir preinstalados con credenciales de abono (por ejemplo, en una tarjeta inteligente o en la memoria del dispositivo) del operador que el usuario desea obtener el servicio. Lo primero puede ser caro para el operador (por ejemplo, debido a las complejidades del canal de distribución). Lo primero también puede ser poco práctico para el usuario. Por ejemplo, si el dispositivo es un medidor de energía inteligente, la tarjeta SIM debería estar asegurada para evitar robos. Lo segundo puede vincular el dispositivo a un operador particular. Esto puede ser caro para el proveedor del dispositivo puesto que se fabricarían diferentes modelos para cada operador (por ejemplo, múltiples SKU por operador, por país, etc.). Además, este último puede limitar las opciones del usuario, ya que se pueden proporcionar ciertos dispositivos para un número limitado de operadores.

[0006] Una forma de resolver el problema es configurar el dispositivo de forma remota utilizando un abono existente en el dispositivo (por ejemplo, en la tarjeta inteligente o en el propio dispositivo) para descargar las credenciales. De forma alternativa, un abono existente asociado con otra forma de conectividad fuera de banda (por ejemplo, WLAN) se puede usar para descargar las credenciales. Sin embargo, si el dispositivo no admite otra forma de conectividad fuera de banda (por ejemplo, carece de capacidad WLAN o la WLAN no está disponible para el dispositivo) y/o no hay credenciales de abono disponibles para el dispositivo, aún es deseable proporcionar un procedimiento para que estos dispositivos vírgenes sean abastecidos utilizando una red celular.

[0007] Se hace referencia al documento WO 2009/103621 A1 que describe procedimientos y aparatos para ubicar y acceder a un servidor de datos en una red inalámbrica. Las técnicas se pueden usar para permitir que un dispositivo inalámbrico provisto de credenciales temporales acceda a una red inalámbrica y obtenga una dirección de red para un servidor de datos para descargar las credenciales de abono. Un dispositivo inalámbrico a modo de ejemplo comprende una unidad de procesamiento configurada para enviar una petición de autentificación de acceso a una red inalámbrica y recibir un valor de desafío de autentificación desde la red inalámbrica en respuesta. La

unidad de procesamiento está configurada además para generar una respuesta criptográfica a partir del valor de desafío de autentificación y enviar la respuesta criptográfica a la red inalámbrica, y también obtener una dirección del servidor de datos a partir del valor de desafío de autentificación. Por lo tanto, el valor de desafío de autentificación tiene dos propósitos: como una clave de desafío para su uso en un procedimiento de autentificación de acceso a la red y como una portadora de información de dirección del servidor de datos.

[0008] También se hace referencia al documento WO 2011/115407 A2, que proporciona un procedimiento y un sistema para el abastecimiento remoto y seguro de una tarjeta de circuito integrado universal de un equipo de usuario. Un sistema incluye un equipo de usuario para iniciar una petición de abastecimiento remoto de una tarjeta de circuito integrado universal (UICC) en el equipo de usuario, donde la petición de abastecimiento remoto incluye un identificador de máquina (MID) asociado con el equipo de usuario y un identificador (ID) de red móvil pública terrestre (PLMN) asociado con un operador de red. El sistema también incluye al menos un servidor de gestión de claves compartidas para generar dinámicamente claves de seguridad y una clave compartida del operador que utiliza las claves de seguridad, el MID. Además, el sistema incluye una red de operador para generar una clave de abono utilizando la clave compartida del operador y una identidad internacional de abonado móvil (IMSI), y abasteciendo el IMSI de forma segura a la UICC del equipo de usuario utilizando las claves de seguridad.

[0009] También se hace referencia al documento WO2011159952 A1 que describe un procedimiento de autentificación entre un dispositivo (por ejemplo, un dispositivo cliente o terminal de acceso) y una entidad de red. Se puede acoplar un dispositivo de almacenamiento extraíble al dispositivo y almacenar una clave específica del abonado que se puede usar para la autentificación del abonado. Se puede acoplar un dispositivo de almacenamiento seguro al dispositivo y almacenar una clave específica del dispositivo utilizada para la autentificación del dispositivo. La autentificación del abonado se puede realizar entre el dispositivo y una entidad de red. La autentificación del dispositivo también se puede realizar del dispositivo con la entidad de red. A continuación, se puede generar una clave de seguridad que vincula la autentificación del abonado y la autentificación del dispositivo. La clave de seguridad se puede usar para asegurar las comunicaciones entre el dispositivo y una red de servicio.

SUMARIO

[0010] De acuerdo con la presente invención, se proporcionan procedimientos y aparatos como se expone en las reivindicaciones independientes, respectivamente. Los modos de realización preferentes de la invención se describen en las reivindicaciones dependientes.

[0011] Los sistemas, procedimientos y dispositivos de la invención tienen cada uno varios aspectos, ninguno de los cuales es el único responsable de sus atributos deseables. Sin limitar el alcance de la presente invención expresado por las reivindicaciones siguientes, a continuación se analizarán brevemente algunas características. Después de considerar esta exposición y, en particular, después de leer la sección titulada "Descripción detallada", se comprenderá cómo las características de la presente invención proporcionan ventajas que incluyen sistemas de comunicación inalámbrica de configuración inicial rápida de enlace de red, para puntos de acceso y dispositivos.

[0012] En un aspecto innovador, se proporciona un procedimiento de obtención de información de abastecimiento a través de una red del proveedor de servicios para un dispositivo. El procedimiento incluye transmitir, a través de la red del proveedor de servicios, una petición de conexión para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo. El procedimiento también incluye recibir información de abastecimiento de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo.

[0013] En otro aspecto innovador, se proporciona un aparato para obtener información de abastecimiento a través de una red del proveedor de servicios. El aparato incluye un gestor de conexiones configurado para transmitir, a través de la red del proveedor de servicios, una petición de conexión para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el aparato. El aparato incluye un gestor de credenciales configurado para recibir información de abastecimiento de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo.

[0014] En un aspecto innovador, se proporciona otro aparato para obtener información de abastecimiento a través de una red del proveedor de servicios. El aparato incluye medios para transmitir, a través de la red del proveedor de servicios, una petición de conexión para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el aparato. El aparato incluye medios para recibir información de abastecimiento de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo.

[0015] En un aspecto innovador adicional se proporciona un medio de almacenamiento legible por ordenador que comprende instrucciones ejecutables por un procesador de un aparato. Las instrucciones hacen que el aparato transmita, a través de la red del proveedor de servicios, una petición de conexión para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el

aparato. Las instrucciones también hacen que el aparato reciba información de abastecimiento de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo.

[0016] En otro aspecto innovador, se proporciona un procedimiento de suministro de información de abastecimiento a través de una red del proveedor de servicios a un dispositivo. El procedimiento incluye recibir una petición de conexión del dispositivo a través de la red del proveedor de servicios para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo. El procedimiento incluye la autentificación del dispositivo basándose, al menos en parte, en la información del proveedor del dispositivo. El procedimiento incluye transmitir información de abastecimiento asociada con un abono tras determinar que el dispositivo se ha autentificado.

[0017] En otro aspecto innovador, se proporciona un aparato para proporcionar información de abastecimiento a través de una red del proveedor de servicios a un dispositivo. El aparato incluye un gestor de conexiones configurado para recibir una petición de conexión del dispositivo a través de la red del proveedor de servicios para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo. El aparato incluye un autentificador configurado para autentificar el dispositivo basándose, al menos en parte, en la información del proveedor del dispositivo. El aparato incluye un gestor de credenciales configurado para provocar la transmisión de información de abastecimiento asociada con un abono tras determinar que el dispositivo se ha autentificado.

[0018] Se describe un aparato innovador adicional para proporcionar información de abastecimiento a través de una red del proveedor de servicios para un dispositivo. El aparato incluye medios para recibir una petición de conexión del dispositivo a través de la red del proveedor de servicios para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo. El aparato incluye medios para autentificar el dispositivo basándose, al menos en parte, en la información del proveedor del dispositivo. El aparato también incluye medios para transmitir información de abastecimiento asociada con un abono tras determinar que el dispositivo se ha autentificado.

[0019] En otro aspecto innovador, se proporciona un medio de almacenamiento legible por ordenador que comprende instrucciones ejecutables por un procesador de un aparato. Las instrucciones hacen que el aparato reciba una petición de conexión desde un dispositivo a través de la red del proveedor de servicios para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo. Las instrucciones hacen que el aparato autentifique el dispositivo basándose, al menos en parte, en la información del proveedor del dispositivo. Las instrucciones hacen que el aparato transmita información de abastecimiento asociada con un abono tras determinar que el dispositivo se ha autentificado.

[0020] En uno o más de los aspectos anteriores, la petición de conexión puede incluir un tipo de abastecimiento. Por ejemplo, el tipo de abastecimiento puede incluirse en la petición de conexión en un elemento de información.

[0021] En algunas implementaciones, los procedimientos, aparatos o instrucciones pueden incluir o configurarse para comunicar (por ejemplo, transmitir y/o recibir) una petición de desafío para autentificar la información del proveedor del dispositivo y comunicar (por ejemplo, transmitir y/o recibir) una respuesta de desafío basándose, al menos en parte, en la información del proveedor del dispositivo. En algunas implementaciones, se puede tomar una determinación con respecto a si la respuesta de desafío está asociada con un abono. La determinación puede basarse en la información del proveedor del dispositivo.

[0022] De forma alternativa o adicional, los procedimientos, aparatos o instrucciones pueden incluir o configurarse para comunicar (por ejemplo, transmitir y/o recibir) una petición de autentificación de abono y comunicar (por ejemplo, transmitir y/o recibir) una respuesta de desafío basándose, al menos en parte, en una credencial predeterminada compartida por múltiples dispositivos.

[0023] En algunas implementaciones, se puede obtener una clave de sesión. La clave de sesión puede basarse, al menos en parte, en la información del proveedor del dispositivo. Las comunicaciones entre el dispositivo y la red del proveedor de servicios pueden ser seguras basándose, al menos en parte, en la clave de sesión. Tras recibir la información de abastecimiento, el dispositivo se puede configurar para desconectarse de la red del proveedor de servicios y obtener un servicio basándose, al menos en parte, en la información de abastecimiento recibida. En algunas implementaciones, la red del proveedor de servicios se puede configurar para iniciar la desconexión tras la transmisión de la información de abastecimiento.

[0024] En uno o más de los aspectos anteriores, la información del proveedor del dispositivo puede incluir un certificado de cifrado asociado con un proveedor de un dispositivo. El identificador único para el dispositivo puede incluir un identificador internacional de equipo móvil y/o un identificador de equipo móvil. La red del proveedor de servicios analizada anteriormente puede incluir una red celular.

[0025] En algunas implementaciones, tras determinar que el dispositivo no se ha autentificado, los procedimientos, aparatos o instrucciones descritos pueden incluir o configurarse para obtener una oferta de abono de un proveedor

de credenciales, transmitir la oferta de abono al dispositivo, recibir un mensaje que indique la aceptación de la oferta de abono, y transmitir información de abastecimiento basándose en la oferta de abono aceptada.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0026]

La FIG. 1 muestra un ejemplo de un sistema de comunicación inalámbrica en el que se pueden emplear aspectos de la presente divulgación.

La FIG. 2 ilustra un ejemplo de un sistema de comunicación inalámbrica en el que se pueden emplear aspectos de la presente divulgación.

La FIG. 3 muestra un diagrama de bloques funcional de un ejemplo de un dispositivo inalámbrico que se puede emplear dentro del sistema de comunicación inalámbrica de la FIG. 1.

La FIG. 4 muestra un diagrama de flujo de proceso de un ejemplo de un proceso para la gestión remota de credenciales.

La FIG. 5 muestra un diagrama de flujo de proceso de un ejemplo de un proceso para el procesamiento de no abonados durante la gestión remota de credenciales.

La FIG. 6 muestra un diagrama de flujo de llamadas que se puede incluir en un ejemplo de un sistema de gestión remota de credenciales.

La FIG. 7 muestra un diagrama de flujo de proceso para un procedimiento de ejemplo de obtención de información de abastecimiento a través de una red del proveedor de servicios.

La FIG. 8 muestra un diagrama de bloques funcional para un ejemplo de un aparato de comunicación de red inalámbrica.

La FIG. 9 muestra un diagrama de flujo de proceso para un procedimiento de ejemplo de suministro de información de abastecimiento a través de una red del proveedor de servicios.

La FIG. 10 muestra un diagrama de bloques funcional para un ejemplo de otro aparato de comunicación de red inalámbrica.

DESCRIPCIÓN DETALLADA

[0027] Se describen los sistemas y procedimientos para suministrar dispositivos celulares con credenciales celulares (gestión remota de credenciales) a través de la red celular (por ejemplo, UMTS, LTE, 1x, DO). Dichos sistemas y procedimientos permiten que un dispositivo celular que carece de credenciales y conectividad fuera de banda acceda a una red celular para suministrar credenciales que pueden usarse para acceder a una red celular. En algunos sistemas, los sistemas y procedimientos descritos de suministro de información de abastecimiento para un servicio pueden denominarse gestión remota de credenciales.

[0028] A continuación, en el presente documento se describen de forma más detallada diversos aspectos de los sistemas, aparatos y procedimientos novedosos, en referencia a los dibujos adjuntos. Sin embargo, la divulgación de estas enseñanzas puede realizarse de muchas formas diferentes y no debería considerarse limitada a ninguna estructura o función específica presentada a lo largo de esta divulgación. En cambio, estos aspectos se proporcionan de modo que esta divulgación sea exhaustiva y completa, y transmita por completo el alcance de la divulgación a los expertos en la técnica. Basándose en las enseñanzas del presente documento, un experto en la técnica debería apreciar que el alcance de la divulgación está concebido para abarcar cualquier aspecto de los sistemas, aparatos y procedimientos novedosos divulgados en el presente documento, ya sean implementados de forma independiente de, o en combinación con, cualquier otro aspecto de la invención. Por ejemplo, un aparato se puede implementar o un procedimiento se puede llevar a la práctica usando cualquier número de los aspectos expuestos en el presente documento. Además, el alcance de la invención está concebido para abarcar dicho aparato o procedimiento, que se lleva a la práctica usando otra estructura, funcionalidad, o estructura y funcionalidad, de forma adicional o alternativa a los diversos aspectos de la invención expuestos en el presente documento. Debería entenderse que cualquier aspecto divulgado en el presente documento puede materializarse mediante uno o más elementos de una reivindicación.

[0029] Aunque en el presente documento se describen aspectos particulares, muchas variantes y permutaciones de estos aspectos quedan dentro del alcance de la divulgación. Aunque se mencionan algunos beneficios y ventajas de los aspectos preferentes, el alcance de la divulgación no está concebido para limitarse a beneficios, usos u objetivos particulares. En cambio, los aspectos de la divulgación están concebidos para ser ampliamente aplicables

a diferentes tecnologías inalámbricas, configuraciones de sistema, redes y protocolos de transmisión, algunos de los cuales se ilustran a modo de ejemplo en las figuras y en la siguiente descripción de los aspectos preferentes. La descripción detallada y los dibujos son meramente ilustrativos de la divulgación, en lugar de limitantes, el alcance de la divulgación que está definido por las reivindicaciones adjuntas y los equivalentes de las mismas.

[0030] Los sistemas y procedimientos descritos en el presente documento se pueden aplicar para la gestión remota de credenciales en redes basadas en LTE, UMTS, HRPD, HRPD evolucionado (eHRPD) o CDMA (por ejemplo, CDMA 1x).

[0031] En algunos aspectos, se pueden transmitir señales inalámbricas en una banda de subgigahercios. En algunos aspectos, las señales inalámbricas se pueden transmitir utilizando multiplexación por división ortogonal de frecuencia ortogonal (OFDM), comunicaciones de espectro ensanchado de secuencia directa (DSSS), una combinación de comunicaciones de OFDM y DSSS, u otros esquemas. Los protocolos de subgigahercios se pueden usar para sensores, medición y redes interconectadas inteligentes. Aspectos de ciertos dispositivos que implementan dichos protocolos pueden consumir menos energía que los dispositivos que implementan otros protocolos inalámbricos. Estos dispositivos se pueden usar para transmitir señales inalámbricas a través de un alcance relativamente largo, por ejemplo, alrededor de un kilómetro o más.

[0032] En algunas implementaciones, una red inalámbrica puede incluir diversos dispositivos que son los componentes que acceden a la red inalámbrica. Por ejemplo, pueden existir dos tipos de dispositivos: puntos de acceso (AP) y clientes (también denominados estaciones o STA). En general, un AP sirve como un concentrador o estación base para la red inalámbrica y una STA sirve como un usuario de la red inalámbrica. Por ejemplo, una STA puede ser un ordenador portátil, un asistente personal digital (PDA), un teléfono móvil, etc. En un ejemplo, una STA se conecta a un AP a través de un enlace inalámbrico celular para obtener conectividad global a Internet o a otras redes de área amplia. En algunas implementaciones, se puede usar también una STA como un AP.

[0033] Un punto de acceso (AP) puede comprender también, implementarse como, o conocerse como nodo B, controlador de red de radio (RNC), eNodoB, controlador de estación base (BSC), estación transceptora base (BTS), estación base (BS), función transceptora (TF), encaminador de radio, transceptor de radio o con alguna otra terminología.

[0034] Una estación "STA" también puede comprender, implementarse como o conocerse como un terminal de acceso (AT), una estación de abonado, una unidad de abonado, una estación móvil, una estación remota, un terminal remoto, un terminal de usuario, un agente de usuario, un dispositivo de usuario, un equipo de usuario, o con alguna otra terminología. En algunas implementaciones, un terminal de acceso puede comprender un teléfono celular, un teléfono sin cables, un teléfono de protocolo de inicio de sesión (SIP), una estación de bucle local inalámbrico (WLL), un asistente personal digital (PDA), un dispositivo manual con capacidad de conexión inalámbrica o algún otro dispositivo de procesamiento adecuado conectado a un módem inalámbrico. Por consiguiente, uno o más aspectos divulgados en el presente documento se pueden incorporar a un teléfono (por ejemplo, un teléfono celular o un teléfono inteligente), un ordenador (por ejemplo, un ordenador portátil), un dispositivo de comunicación portátil, un auricular, un dispositivo informático portátil (por ejemplo, un asistente de datos personal), un dispositivo de entretenimiento (por ejemplo, un dispositivo de música o de vídeo o una radio por satélite), un dispositivo o sistema de juegos, un dispositivo de sistema de posicionamiento global o cualquier otro dispositivo adecuado que esté configurado para comunicarse a través de un medio inalámbrico.

[0035] Dichos dispositivos, ya sea que se usen como una STA o un AP o como otro dispositivo, se pueden usar en dispositivos de medición inteligentes o en una red interconectada inteligente. Dichos dispositivos pueden proporcionar aplicaciones de sensor o usarse en domótica. Los dispositivos se pueden usar, en lugar de o además de, en un contexto de asistencia sanitaria, por ejemplo, para asistencia sanitaria particular. Pueden usarse también para vigilancia, para habilitar la conectividad a Internet de alcance ampliado (por ejemplo, para su uso con puntos de acceso wifi) o para implementar comunicaciones de máquina a máquina.

[0036] La FIG. 1 muestra un sistema de comunicación inalámbrica a modo de ejemplo. El sistema de comunicación inalámbrica 100 puede incluir un AP 104, que se comunica con las STA tales como un teléfono móvil 106a, un televisor 106b, un ordenador 106c u otro punto de acceso 106d (individualmente o colectivamente de aquí en adelante identificado por 106).

[0037] Se puede usar una variedad de procesos y procedimientos para transmisiones en el sistema de comunicación inalámbrica 100 entre el AP 104 y las STA 106. Por ejemplo, se pueden enviar y recibir señales entre el AP 104 y las STA 106, de acuerdo con técnicas de OFDM/OFDMA. Si este es el caso, el sistema de comunicación inalámbrica 100 se puede denominar sistema de OFDM/OFDMA. De forma alternativa, se pueden enviar y recibir señales entre el AP 104 y las STA 106 de acuerdo con técnicas de CDMA. Si este es el caso, el sistema de comunicación inalámbrica 100 se puede denominar sistema de CDMA.

[0038] Un enlace de comunicación que facilita la transmisión desde el AP 104 a una o más de las STA 106 se puede denominar enlace descendente (DL) 108 y un enlace de comunicación que facilita la transmisión desde una o

más de las STA 106 al AP 104 se puede denominar enlace ascendente (UL) 110. De forma alternativa, un enlace descendente 108 se puede denominar enlace directo o canal directo, y un enlace ascendente 110 se puede denominar enlace inverso o canal inverso.

[0039] El AP 104 puede proporcionar cobertura de comunicación inalámbrica en un área de servicios básicos (BSA) 102. El AP 104 junto con las STA 106 asociadas al AP 104 y que están configuradas para usar el AP 104 para la comunicación puede denominarse como un conjunto de servicios básicos (BSS). Cabe destacar que el sistema de comunicación inalámbrica 100 puede no tener un AP central 104, sino que, en cambio, puede funcionar como una red de igual a igual entre las STA 106. Por consiguiente, las funciones del AP 104 descritas en el presente documento pueden realizarse, de forma alternativa, mediante una o más de las STA 106.

[0040] La FIG. 2 ilustra un ejemplo de un sistema de comunicación inalámbrica en el que se pueden emplear aspectos de la presente divulgación. El sistema de comunicación inalámbrica que se muestra en la FIG. 2 incluye un dispositivo 202 con capacidad de gestión remota de credenciales. Un dispositivo 202 con capacidad de gestión remota de credenciales puede incluir un teléfono inteligente, un teléfono mejorado, un dispositivo celular incluido en un automóvil, un sensor tal como un indicador de temperatura o un sismógrafo, una cámara, una tableta electrónica, un lector de libro electrónico (e-book), un lector de tarjetas de crédito u otro dispositivo configurado para la comunicación inalámbrica. El dispositivo 202 con capacidad de gestión remota de credenciales puede ser una STA 106. Sin embargo, no todas las STA pueden ser dispositivos 202 con capacidad de gestión remota de credenciales.

[0041] Como se ha descrito anteriormente, el dispositivo 202 con capacidad de gestión remota de credenciales puede comunicarse con un punto de acceso 104. El punto de acceso 104 se puede configurar para proporcionar acceso a una red celular 206. La red celular 206 puede incluir una o más pasarelas que están configuradas para proporcionar acceso a redes de datos.

[0042] Directamente o a través de la red de datos, la red celular 206 se puede configurar para comunicarse con un servidor de gestión remota de credenciales 210. El servidor de gestión remota de credenciales 210 puede estar ubicado en la red de un operador. Por ejemplo, el servidor de gestión remota de credenciales 210 puede incluirse en un sistema de gestión de dispositivos y abastecimiento. En algunas implementaciones, el servidor de gestión remota de credenciales 210 puede estar alojado por un proveedor de servicios máquina a máquina en nombre del operador de red. En algunas implementaciones, el servidor de gestión remota de credenciales 210 puede ser alojado por un proveedor de dispositivos en nombre del operador de red.

[0043] El servidor de gestión remota de credenciales 210 se puede configurar para gestionar dispositivos con capacidad de gestión remota de credenciales. El servidor de gestión remota de credenciales 210 se puede configurar para gestionar el abono a las asignaciones de dispositivos. Esta asignación se puede usar para el abastecimiento de credenciales de abono y/o propósitos de facturación. El servidor de gestión remota de credenciales 210 puede admitir una interfaz con proveedores de servicios externos para registrar dispositivos y asociar planes de facturación.

[0044] Los proveedores de servicios (por ejemplo, empresa de servicios públicos o vendedor de libros electrónicos) también pueden ser proveedores de credenciales 212. En algunas implementaciones, los proveedores de credenciales 212 pueden no proporcionar servicios de red más allá de proporcionar credenciales. Por ejemplo, un proveedor de credenciales 212 puede comprar servicios de red en grandes cantidades de un operador y revender estos servicios. Para mencionar otro ejemplo, un proveedor de credenciales 212 puede ofrecer credenciales si los usuarios proporcionan información (por ejemplo, realizar una encuesta, ver contenido, etc.). Los proveedores de credenciales 212 pueden estar ubicados dentro de la red del proveedor de servicios o conectados a la red del proveedor de servicios.

[0045] Un ejemplo de un proveedor de credenciales es un operador de red 212a. Otro ejemplo de un proveedor de credenciales es un fabricante de dispositivos 212b. Otro ejemplo de un proveedor de credenciales 212 es un proveedor de servicios de máquina a máquina 212c. Los proveedores de credenciales pueden gestionar dispositivos 202 con capacidad de gestión remota de credenciales proporcionando identificadores de dispositivo, identificadores para clases de dispositivos y/o certificados para autentificar dispositivos con capacidad de gestión remota de credenciales.

[0046] El sistema también puede incluir un centro de operaciones de red 208. El centro de operaciones de red 208 se puede configurar para gestionar características de procesos internos relacionadas con las credenciales de abono. Por ejemplo, si un proveedor de credenciales 212 está subvencionando el acceso para un dispositivo 202 con capacidad de gestión remota de credenciales, el centro de operaciones de red 208 puede supervisar el tráfico desde el dispositivo y determinar si el servicio solicitado por el dispositivo 202 con capacidad de gestión remota de credenciales está dentro del nivel de servicio negociado asociado con el proveedor de credenciales. El centro de operaciones de red 208 se puede configurar para aplicar también políticas y funciones de carga, así como calidad de servicio para el dispositivo 202 con capacidad de gestión remota de credenciales.

[0047] La FIG. 3 muestra un diagrama de bloques funcional de un dispositivo de gestión de credenciales a modo de ejemplo que puede emplearse dentro del sistema de comunicación inalámbrica de la FIG. 1. El dispositivo de gestión de credenciales 302 es un ejemplo de un dispositivo que se puede configurar para implementar los diversos procedimientos descritos en el presente documento. Por ejemplo, el dispositivo de gestión de credenciales 302 puede comprender el dispositivo 202 con capacidad de gestión remota de credenciales o el servidor de gestión remota de credenciales 210.

[0048] El dispositivo de gestión de credenciales 302 puede incluir una unidad o unidades de procesador 304 que controlan el funcionamiento del dispositivo de gestión de credenciales 302. Una o más de la unidad o unidades de procesador 304 puede denominarse colectivamente como una unidad central de procesamiento (CPU). La memoria 306, que puede incluir tanto memoria de solo lectura (ROM) como memoria de acceso aleatorio (RAM), proporciona instrucciones y datos a las unidades de procesador 304. Una porción de la memoria 306 también puede incluir memoria de acceso aleatorio no volátil (NVRAM). La unidad o unidades de procesador 304 se pueden configurar para realizar operaciones lógicas y aritméticas basadas en instrucciones de programa almacenadas en la memoria 306. Las instrucciones en la memoria 306 pueden ser ejecutables para implementar los procedimientos descritos en el presente documento.

[0049] La unidad o unidades de procesador 304 se pueden implementar con cualquier combinación de microprocesadores de propósito general, microcontroladores, procesadores de señales digitales (DSP), matrices de puertas programables in situ (FPGA), dispositivos lógicos programables (PLD), controladores, máquinas de estado, lógica de puertas, componentes de hardware discretos, máquinas de estado finitas de hardware dedicado o cualquier otra entidad adecuada que pueda realizar cálculos u otras manipulaciones de información. En una implementación en la que la unidad o unidades de procesador 304 comprenden un DSP, el DSP se puede configurar para generar un paquete (por ejemplo, un paquete de datos) para su transmisión. En algunos aspectos, el paquete puede comprender una unidad de datos de capa física (PPDU).

[0050] El dispositivo de gestión de credenciales 302 también puede incluir medios legibles por máquina para almacenar software. La unidad o unidades de procesamiento 304 pueden comprender uno o más medios legibles por máquina para almacenar software. Se interpretará en sentido amplio que software significa cualquier tipo de instrucciones, independientemente de si se denominan software, firmware, middleware, microcódigo, lenguaje de descripción de hardware o de otro modo. Las instrucciones pueden incluir código (por ejemplo, en formato de código fuente, formato de código binario, formato de código ejecutable o cualquier otro formato de código adecuado). Las instrucciones, cuando se ejecutan por la unidad o unidades de procesador 304, hacen que el dispositivo de gestión de credenciales 302 realice las diversas funciones descritas en el presente documento.

[0051] El dispositivo de gestión de credenciales 302 puede incluir un transmisor 310 y/o un receptor 312 para permitir la transmisión y la recepción, respectivamente, de datos entre el dispositivo de gestión de credenciales 302 y una ubicación remota. El transmisor 310 y el receptor 312 se pueden combinar en un transceptor 314. Una antena 316 se puede conectar a la carcasa 308 y acoplarse de forma eléctrica al transceptor 314. El dispositivo de gestión de credenciales 302 también puede incluir (no se muestra) múltiples transmisores, múltiples receptores, múltiples transceptores y/o múltiples antenas.

[0052] El transmisor 310 se puede configurar para transmitir de forma inalámbrica paquetes y/o señales. Por ejemplo, el transmisor 310 se puede configurar para transmitir diferentes tipos de paquetes generados por la unidad o unidades de procesador 304, analizada anteriormente. Los paquetes se ponen a disposición del transmisor 301. Por ejemplo, la unidad o unidades de procesador 304 pueden almacenar un paquete en la memoria 306 y el transmisor 301 se puede configurar para recuperar el paquete. Una vez que el transmisor recupera el paquete, el transmisor 301 transmite el paquete a través de la antena 316.

[0053] La antena 316 en el dispositivo de gestión de credenciales 302 puede detectar paquetes/señales transmitidos de forma inalámbrica. El receptor 312 se puede configurar para procesar los paquetes/señales detectados y ponerlos a disposición de la unidad o unidades de procesador 304. Por ejemplo, el receptor 312 puede almacenar el paquete en la memoria 306 y la unidad o unidades de procesador 304 se pueden configurar para recuperar el paquete.

[0054] El dispositivo de gestión de credenciales 302 puede incluir también un detector de señales 318 que se puede usar con la intención de detectar y cuantificar el nivel de las señales recibidas por el transceptor 314. El detector de señales 318 puede detectar dichas señales como energía total, energía por subportadora por símbolo, densidad espectral de potencia y otras señales. El dispositivo de gestión de credenciales 302 también puede incluir un procesador de señales digitales (DSP) 320 para su uso en el procesamiento de señales. El DSP 320 se puede configurar para generar un paquete para su transmisión. En algunos aspectos, el paquete puede comprender una unidad de datos de capa física (PPDU).

[0055] El dispositivo de gestión de credenciales 302 puede comprender además una interfaz de usuario 322 en algunos aspectos. La interfaz de usuario 322 puede comprender un teclado, un micrófono, un altavoz y/o una pantalla. La interfaz de usuario 322 puede incluir cualquier elemento o componente que transmite información a un

usuario del dispositivo de gestión de credenciales 302 y/o recibe una entrada desde el usuario. El dispositivo de gestión de credenciales 302 también puede incluir una carcasa 308 que rodea uno o más de los componentes incluidos en el dispositivo de gestión de credenciales 302.

[0056] El dispositivo de gestión de credenciales 302 también puede incluir un gestor remoto de credenciales 324. Cuando el dispositivo de gestión de credenciales 302 se implementa como un dispositivo 202 con capacidad de gestión remota de credenciales (por ejemplo, una STA), el gestor remoto de credenciales 324 puede incluir uno o más circuitos configurados para generar una petición de conexión de abastecimiento que incluye la información de arranque para obtener credenciales de abono, recibir y responder a peticiones de desafío, y gestionar las credenciales de abono proporcionadas tal como se describe con más detalle a continuación. Cuando el dispositivo de gestión de credenciales 302 se implementa como un servidor de gestión remota de credenciales 210, el gestor remoto de credenciales 324 puede incluir uno o más circuitos configurados para procesar las peticiones de conexión de abastecimiento, incluida la información de arranque, realizar mensajes de desafío de autentificación del dispositivo, e identificar y proporcionar credenciales de abono, tal como se describe con más detalle a continuación.

[0057] Los diversos componentes del dispositivo de gestión de credenciales 302 pueden acoplarse entre sí mediante un sistema de bus 326. El sistema de bus 326 puede incluir un bus de datos, por ejemplo, así como un bus de alimentación, un bus de señal de control y un bus de señal de estado, además del bus de datos. Los expertos en la técnica apreciarán que los componentes del dispositivo de gestión de credenciales 302 pueden acoplarse juntos o aceptar o proporcionar entradas entre sí usando algún otro mecanismo.

[0058] Aunque se ilustran un número de componentes separados en la FIG. 3, los expertos en la técnica reconocerán que uno o más de los componentes se pueden combinar o implementar en común. Por ejemplo, la unidad o unidades de procesador 304 pueden usarse para implementar no solo la funcionalidad que se ha descrito anteriormente con respecto a la unidad o unidades de procesador 304, sino también para implementar la funcionalidad que se ha descrito anteriormente con respecto al detector de señales 318. Además, cada uno de los componentes ilustrados en la FIG. 3 se puede implementar usando una pluralidad de elementos separados.

[0059] La FIG. 4 muestra un diagrama de flujo de proceso de un ejemplo de un proceso para la gestión remota de credenciales. El proceso que se muestra en la FIG. 4 puede implementarse mediante uno o más elementos incluidos en una red inalámbrica tal como la que se muestra en las FIG. 1 o 2. En el bloque 402, se puede proporcionar información de arranque. La información de arranque en general puede referirse a la información proporcionada por un proveedor de módulo/dispositivo. La información puede instalarse en el módulo/dispositivo para acceder a una red inalámbrica. La información de arranque puede basarse en los requisitos del operador de red. Por ejemplo, un operador de red puede arrancar basándose en el identificador internacional de equipo móvil (IMEI) y un certificado o un par de claves privadas/públicas asociadas con el IMEI, mientras que otro operador de red puede arrancar basándose en el IMEI, un certificado o un par o pares de claves privadas/públicas asociadas con el IMEI, y un identificador de proveedor de servicios. En algunas implementaciones, se puede usar un identificador de equipo móvil (MEID) para identificar un dispositivo. Por consiguiente, un módulo/dispositivo puede incluir varias piezas de información de arranque que pueden usarse o no para proporcionar credenciales basadas en el operador de red.

[0060] La información de arranque, en algunas implementaciones, puede incluir un identificador internacional de equipo móvil, un identificador de equipo móvil y/o un certificado de identificador internacional de equipo móvil. Los elementos de información de arranque se pueden configurar de forma segura en la fase de fabricación. Por ejemplo, los elementos pueden almacenarse en una ubicación de memoria estática y/o segura en el dispositivo. En algunas implementaciones, puede ser deseable que el certificado de identificador internacional de equipo móvil sea emitido por una autoridad de certificación de confianza del operador. La información de arranque puede almacenarse en una memoria del dispositivo. La información de arranque puede almacenarse en una memoria extraíble, como una tarjeta inteligente que puede acoplarse con el dispositivo.

[0061] En el bloque 404, el dispositivo puede estar encendido. En el bloque de decisión 406, se puede tomar una determinación de si hay un abono válido disponible para el dispositivo. Por ejemplo, las credenciales de abono celular se pueden incluir en una tarjeta inteligente o en la memoria del dispositivo.

[0062] Si el dispositivo incluye credenciales de abono válidos, estas credenciales se pueden usar para conectarse a la red en el bloque 418 usando los procedimientos de conexión prescritos por el operador de red o un estándar que rige la red inalámbrica. Sin embargo, si la determinación en el bloque de decisión 406 no identifica un abono válido para el dispositivo, en el bloque 408 el dispositivo se puede configurar para conectarse a la red utilizando una petición de conexión de abastecimiento. En algunas implementaciones, una petición de conexión puede incluir un campo de tipo de conexión. En dichas implementaciones, el tipo de conexión puede identificarse como abastecimiento o servicio de abastecimiento. La red se puede configurar para permitir que este dispositivo se conecte con el propósito limitado de obtener las credenciales de abono. Una forma en que la red puede determinar esta conexión es para este propósito limitado mediante el uso de un campo de conexión.

[0063] En el bloque 410, basándose en la petición de servicio de abastecimiento, la red puede identificar información de abono para el dispositivo. Como parte de la identificación de la información de abono, la red puede realizar una autentificación basándose en la información de arranque incluida en la petición de servicio de abastecimiento. En algunas implementaciones, la autentificación puede incluir mensajes adicionales (por ejemplo, petición/respuesta de desafío) para obtener información para la autentificación.

[0064] En algunas implementaciones, la red puede omitir la autentificación y la gestión de claves (AKA) para abastecer peticiones de conexión. En dichas implementaciones, el contexto de seguridad de estrato sin acceso, tal como $K_{ASME,}$ se puede obtener a partir de la autentificación IMEI. En algunas implementaciones, la autentificación AKA se puede realizar utilizando un conjunto de credenciales bien conocido. Las credenciales AKA bien conocidas, junto con las credenciales a partir de la autentificación IMEI, se pueden usar como credenciales de "invitado" para permitir comunicaciones de AKA seguras con el dispositivo durante el proceso de abastecimiento. Las credenciales AKA bien conocidas pueden estar predeterminadas y compartidas por múltiples dispositivos. Las credenciales bien conocidas pueden ser un IMSI temporal, una identidad de abonado móvil temporal (TMSI), un identificador único global temporal (GUTI) o un identificador similar. Este identificador se puede usar con el propósito de abastecer dispositivos que pueden no tener un abono válido.

[0065] Si la autentificación basada en la información de arranque es satisfactoria, la red puede considerar que el dispositivo es proporcionado por un operador autorizado y/o proveedor certificado. En algunas implementaciones, este dispositivo puede denominarse un dispositivo "de confianza" para fines de abastecimiento. Al identificar así el dispositivo, se puede identificar un abono correspondiente en el bloque 410. Como parte de la identificación, el servidor de gestión remota de credenciales 210 puede obtener de forma segura la información de abono para el dispositivo.

[0066] En el bloque de decisión 412, se toma una determinación sobre si se identifica información de abono para el dispositivo. La determinación puede basarse en el resultado de la autentificación. La determinación puede basarse en un dispositivo autentificado que no tiene un abono activo. Por ejemplo, un dispositivo puede tener un abono mensual con un proveedor de servicios. Al final del mes, el abono puede finalizar. Como tal, el dispositivo puede necesitar renovar su abono para obtener acceso al servicio.

[0067] Si se identifica un abono para el dispositivo, en el bloque 414, las credenciales de abono identificadas se pueden proporcionar al dispositivo. Las credenciales también se pueden proporcionar a uno o más elementos de la red, tal como entidades de red configuradas para realizar la autentificación 3GPP. Las entidades de red pueden incluir un servidor de abonado local (HSS) o un servidor de autentificación, autorización y acceso (AAA) junto con la red del proveedor de servicios.

[0068] En el bloque 416, el dispositivo puede desconectarse de la red. Puesto que el dispositivo se conectó previamente en un modo de solo abastecimiento, los recursos de red disponibles para el dispositivo pueden haberse limitado a solo servicios de credenciales de abastecimiento. La red puede incluir filtros IP para limitar el tráfico de datos, por ejemplo. En el bloque 418, el dispositivo puede conectarse a la red utilizando las credenciales proporcionadas.

[0069] Volviendo al bloque de decisión 412, si no se identifica un abono válido para el dispositivo, se puede realizar un procesamiento adicional de no abonados en el bloque 500. El procesamiento adicional de no abonados se describirá con más detalle en referencia a la FIG. 5 a continuación.

[0070] La FIG. 5 muestra un diagrama de flujo de proceso de un ejemplo de un proceso para el procesamiento de no abonados durante la gestión remota de credenciales. El proceso para el procesamiento de no abonados puede realizarse para dispositivos autentificados. En dichos casos, el dispositivo puede identificarse y asociarse con uno o más proveedores de credenciales 212. Sin embargo, el dispositivo puede no tener una credencial válida activa para ningún proveedor. El proceso puede comenzar en el bloque 502 donde se identifican posibles proveedores de credenciales. Se puede consultar un servidor de gestión remota de credenciales utilizando uno o más elementos de la información de arranque para identificar posibles proveedores de credenciales 212.

[0071] En el bloque de decisión 504, se toma una determinación de si hay algún proveedor de credenciales 212 disponible para el dispositivo identificado. Si no se encuentran proveedores de credenciales 212 para el dispositivo, el proceso continúa en el bloque 518. En el bloque 518, se puede proporcionar un mensaje de error al dispositivo que indica que no hay proveedores de credenciales 212 disponibles para abastecer información de abono. El flujo puede terminar en el bloque 520 con el dispositivo desconectado de la red. La desconexión puede ser realizada por la red y/o el dispositivo.

[0072] Volviendo al bloque de decisión 504, si se identifican uno o más proveedores de credenciales 212 para el dispositivo, el proceso continúa en el bloque 506 donde se obtiene la oferta de abono del proveedor. Una oferta de abono del proveedor puede en general referirse a condiciones y/o términos para obtener una credencial de abono del proveedor. Por ejemplo, la oferta puede incluir proporcionar información de pago para una credencial de abono.

La oferta puede incluir solicitar un valor clave para una credencial de abono. El valor clave puede proporcionarse fuera de banda, tal como en un recibo de compra.

[0073] En el bloque 508, la oferta de abono se puede transmitir al dispositivo. La transmisión puede hacer que una interfaz visualice la información de oferta, por ejemplo, a través de un navegador web. En el bloque 510, se puede recibir una respuesta a la oferta de abono. En el bloque de decisión 512 se toma una determinación de si la oferta se ha aceptado. La determinación de aceptación puede incluir proporcionar la respuesta a la oferta de abono para ser un proveedor de credenciales para verificación, validación y/o procesamiento adicional. Si se acepta la oferta, las credenciales se pueden proporcionar al dispositivo. El proceso puede continuar como, por ejemplo, en la FIG. 4 en el bloque 416.

[0074] Si no se acepta la oferta, en el bloque de decisión 516, se toma una determinación de si se han identificado proveedores de credenciales 212 adicionales para el dispositivo. Si no se han identificado proveedores de credenciales 212 adicionales, el proceso continúa en el bloque 518 como se describe anteriormente. Si se han identificado proveedores de credenciales 212 adicionales, el proceso continúa en el bloque 506 como se describe anteriormente.

[0075] La FIG. 6 muestra un diagrama de flujo de llamadas que se puede incluir en un ejemplo de un sistema de gestión remota de credenciales. El diagrama de flujo de llamadas que se muestra en la FIG. 6 incluye algunas de las entidades que pueden incluirse en un sistema de comunicación inalámbrica que dispone de gestión remota de credenciales. Las entidades que se muestran en la figura 6 incluyen el dispositivo 202 con capacidad RCM, la red de acceso 104 (por ejemplo, UTRAN o E-UTRAN), y el autentificador 604, y la pasarela de acceso IP 608, y HSS/HAA 610, una función de reglas y políticas de cobros 612 y un servidor RCM 210.

[0076] El flujo de llamadas puede comenzar con un mensaje 650 transmitido desde el servidor RCM 210 o un proveedor de dispositivos al HSS/HAA 610. El mensaje 650 puede identificar los perfiles de dispositivo autorizados asociados con el proveedor de credenciales. Los perfiles de dispositivos autorizados pueden incluir información de arranque (tal como una clave pública de confianza o un certificado de CA) que pueden estar asociados con un dispositivo con capacidad RCM o una clase de dispositivos con capacidad RCM. Por ejemplo, el mensaje 650 puede identificar una clase de dispositivos asociados con un proveedor de credenciales. Como algunos ejemplos específicos, el mensaje 650 puede identificar medidores inteligentes que pertenecen a una empresa de servicios públicos, teléfonos inteligentes asociados con un proveedor de servicios o un lector de libros electrónicos proporcionado por un distribuidor de libros electrónicos. La identificación puede ser de acuerdo con los identificadores del dispositivo, porción de los identificadores del dispositivo (por ejemplo, intervalos de identificadores), identificadores de clase de dispositivo y similares. La información del identificador también puede almacenarse en el dispositivo 202 con capacidad RCM durante la fabricación o antes de la entrega a un cliente. La información puede almacenarse en el dispositivo 202 con capacidad RCM usando un elemento de memoria seguro.

[0077] En un momento posterior, el dispositivo 202 con capacidad RCM puede transmitir un mensaje 652 a la red de acceso 104. El mensaje 652 puede ser una petición de conexión para el servicio de abastecimiento. La petición de conexión puede estar asociada a un tipo. El mensaje 652 puede incluir una petición de conexión del tipo asociado con el servicio de abastecimiento. A modo de ejemplo, la petición de conexión puede incluir un elemento de información que incluye un valor que indica que la petición de conexión es de un tipo asociado con el servicio de abastecimiento. El mensaje 652 puede incluir información del proveedor del dispositivo, tal como un identificador de dispositivo único, un identificador de clase de dispositivo o similares. Un ejemplo de un identificador de dispositivo único es el identificador internacional de equipo móvil (IMEI). Otro ejemplo de un identificador de dispositivo único es un identificador de equipo móvil (MEID). La información incluida en el mensaje 652 puede incluirse en la información proporcionada por el mensaje 650.

[0078] La red de acceso 104 puede permitir el dispositivo 202 con capacidad RCM en la red. Por ejemplo, la red de acceso 104 puede determinar que el mensaje 652 es una petición de conexión de tipo de abastecimiento. Esto puede hacer que la red de acceso 104 se anticipe a los procedimientos de autentificación de abono y permita el acceso a la red del dispositivo 202 con capacidad RCM. El proveedor de servicios puede limitar el acceso del dispositivo 202 con capacidad RCM a ciertos servicios y/o ubicaciones de red. Por ejemplo, el proveedor de servicios solo puede permitir que el dispositivo acceda al servidor de gestión remota de credenciales 210. En algunas implementaciones, el proveedor de servicios puede asignar una cierta calidad de servicio para las peticiones de conexión de abastecimiento en comparación con una calidad de servicio para las peticiones de conexión de no abastecimiento. Por ejemplo, el proveedor de servicios puede asignar una calidad de servicio inferior (por ejemplo, prioridad) para abastecer peticiones de conexión en comparación con peticiones de conexión de no abastecimiento (por ejemplo, de dispositivos que tienen credenciales abastecidas previamente).

[0079] Una vez permitido en la red, la autentificación del dispositivo se puede realizar a través del mensaje de autentificación 654. Cabe destacar que el mensaje de autentificación 654 es para autentificar el dispositivo, no un abono, ya que el dispositivo aún no ha sido abastecido con información de servicio. El mensaje de autentificación 654 puede incluir la transmisión del IMEI así como la información del certificado IMEI asociada con el dispositivo 202 con capacidad RCM a un autentificador 604. En algunas implementaciones, el autentificador 604 puede ser un nodo

de soporte de servicio general de radio por paquetes en servicio (SGSN) o una entidad de gestión de la movilidad (MME). En algunas implementaciones de red cdma2000, el autentificador puede ser un nodo de servicio de datos en paquetes (PDSN) o una pasarela de servicio HRPD (HSGW). Si aún no está disponible, la información de autentificación del dispositivo específico del proveedor autorizado, tal como la asociada con la autoridad certificadora del dispositivo 202 con capacidad RCM

[0080] El autentificador 604 puede obtener el certificado y el perfil (CA) mediante mensajes con el HSS/AAA 610 o de otra entidad de la red del proveedor de servicios.

[0081] Si la autentificación falla, el flujo de llamadas finaliza. Como se muestra en la FIG. 6 sin embargo, la autentificación es satisfactoria. El mensaje 658 entre el autentificador 604 y la pasarela de acceso IP 606 puede transmitirse. Los ejemplos de la pasarela de acceso IP 606 incluyen un nodo de soporte general de pasarela, un nodo de servicio del servicio general de radio por paquetes de pasarela o una pasarela de red de datos en paquetes.

[0082] El mensaje 658 puede generar una sesión IP para que el dispositivo 202 con capacidad RCM acceda al servidor RCM 210 para obtener credenciales de abono. En algunas implementaciones, la sesión IP puede autorizarse mediante mensajes (no se muestran) entre la pasarela de acceso IP y la función de reglas y políticas de cobro 412. La autorización puede basarse, al menos en parte, en la autorización IMEI/MEID para el dispositivo. En algunas implementaciones, la pasarela de acceso IP 606 puede incluir filtros de IP restringidos específicos del dispositivo para limitar el acceso a la red del dispositivo 202 con capacidad RCM. Los filtros IP pueden establecerse por dispositivo, por clase de dispositivo, por conexión de abastecimiento o configurarse de la misma manera en la pasarela IP para todos los dispositivos que soliciten el servicio de abastecimiento.

[0083] El dispositivo 202 con capacidad RCM ahora puede comunicarse con el servidor RCM 210. El mensaje 660 puede transmitirse entre el dispositivo 202 con capacidad RCM y el servidor RCM 210 para abastecer las credenciales de abono para el dispositivo 202 con capacidad RCM. En algunas implementaciones, el dispositivo 202 con capacidad RCM puede estar asociado con una credencial válida. Si el servidor RCM 210 puede identificar esta credencial, el abastecimiento se puede lograr sin mensajes adicionales con el dispositivo 202 con capacidad RCM. Sin embargo, como se describe anteriormente, en una situación de no abonado, se pueden presentar ofertas de abono al dispositivo 202 con capacidad RCM. El mensaje 660 puede incluir información de oferta, información de respuesta de oferta y similares. Debe observarse que la comunicación entre el dispositivo 202 con capacidad RCM en el servidor RCM 210 se autentifica mutuamente, está basada en IP y está asegurada.

[0084] El mensaje 660 puede resultar en el abastecimiento satisfactorio de credenciales para el dispositivo 202 con capacidad RCM. En dichas circunstancias, los datos de gestión remota de credenciales también pueden actualizarse con el HSS/AAA 610 que indica la credencial de abono válido para el dispositivo 202 con capacidad RCM. La actualización puede producirse a través de un mensaje 662.

[0085] El mensaje 664 puede transmitirse para conseguir la gestión o activación adicional del dispositivo. Por ejemplo, el abono puede proporcionarse al dispositivo 202 con capacidad RCM, pero puede ser necesaria información adicional para que el dispositivo acceda a una red particular. Esta información puede transmitirse al dispositivo 202 con capacidad RCM a través de la mensajería 664.

[0086] El dispositivo 202 con capacidad RCM ahora puede tener una credencial de abono válido y cualquier información adicional de gestión o activación necesaria para acceder a la red. El mensaje 666 puede transmitirse entre el dispositivo 202 con capacidad RCM y la red de acceso 104 para desconectar el dispositivo 202 con capacidad RCM. Aunque no se muestra, la desconexión también puede hacer que se cierre la sesión IP creada por el mensaje 658. El mensaje 668 puede transmitirse para conectar el dispositivo 202 con capacidad RCM a la red utilizando las credenciales de abono abastecidas.

[0087] Por consiguiente, como se muestra, el dispositivo 202 con capacidad RCM que inicialmente no tiene credenciales de abono válidas puede abastecer credenciales de abono utilizando conectividad celular al proporcionar información de autentificación del proveedor del dispositivo almacenada en el dispositivo 202 con capacidad RCM.

[0088] La FIG. 7 muestra un diagrama de flujo de un proceso para un procedimiento de ejemplo de obtención de información de abastecimiento a través de una red del proveedor de servicios. El procedimiento puede implementarse por completo o parcialmente mediante los dispositivos descritos en el presente documento, tales como los mostrados en la FIG. 3 anterior o la FIG. 8 a continuación. En algunas implementaciones, el proceso puede implementarse en una STA, tal como un dispositivo con capacidad de gestión remota de credenciales.

[0089] El proceso comienza en el bloque 702 donde se puede transmitir una petición de conexión a través de la red del proveedor de servicios para el servicio de abastecimiento. La petición de conexión puede incluir información del proveedor del dispositivo, tal como la información de arranque analizada anteriormente. En algunas implementaciones, se puede recibir una petición de desafío para autentificar un dispositivo. En dichas

implementaciones, se puede transmitir una respuesta de desafío basada, al menos en parte, en información del proveedor del dispositivo (por ejemplo, credenciales). En el bloque 704, se puede recibir información de abastecimiento de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo. Las señales transmitidas y/o recibidas pueden ser similares a las mostradas en los flujos de llamadas de la FIG. 6.

[0090] La FIG. 8 muestra un diagrama de bloques funcional para un aparato de comunicación de red inalámbrica. Los expertos en la técnica apreciarán que un aparato de comunicación de red inalámbrica puede tener más componentes que el aparato de comunicación de red inalámbrica 800 mostrado en la FIG. 8. El aparato de comunicación de red inalámbrica 800 mostrado incluye solamente esos componentes útiles para la descripción de algunas características destacables de implementaciones dentro del alcance de las reivindicaciones. El aparato de comunicación de red inalámbrica 800 puede incluir un gestor de conexiones 802 y un gestor de credenciales 804.

[0091] En algunas implementaciones, el gestor de conexiones 802 se puede configurar para transmitir una petición de conexión a través de la red del proveedor de servicios para el servicio de abastecimiento. La petición de conexión puede incluir información del proveedor del dispositivo que tiene un identificador único para el aparato de comunicación de red inalámbrica 800. El gestor de conexiones 802 puede incluir uno o más entre un chip programable, un procesador, una memoria, una antena y un transmisor. En algunas implementaciones, los medios para transmitir una petición de conexión para el servicio de abastecimiento pueden incluir el gestor de conexiones 802.

[0092] En algunas implementaciones, el gestor de abono 804 se puede configurar para recibir información de abono de la red del proveedor de servicios. El circuito de abono 804 puede incluir uno o más entre un receptor, una antena, un procesador de señales y una memoria. En algunas implementaciones, los medios para recibir información de abastecimiento pueden incluir el gestor de abono 804.

[0093] La FIG. 9 muestra un diagrama de flujo de proceso para un procedimiento de ejemplo de suministro de información de aprovisionamiento a través de una red del proveedor de servicios a un dispositivo. El procedimiento puede implementarse por completo o parcialmente mediante los dispositivos descritos en el presente documento, tales como los mostrados en la FIG. 3 anterior o la FIG. 10 a continuación. En algunas implementaciones, el proceso se puede implementarse en un servidor de gestión remota de credenciales.

[0094] El proceso comienza en el bloque 902, donde se recibe desde el dispositivo a través de la red del proveedor de servicios una petición de conexión para el servicio de abastecimiento. La petición de conexión puede incluir información del proveedor del dispositivo como se ha analizado anteriormente. En el bloque 904, el dispositivo se ha autentificado basándose, al menos en parte, en la información del proveedor del dispositivo. En el bloque 906, la información de abastecimiento asociada con un abono se transmite tras determinar que el dispositivo se ha autentificado.

[0095] La FIG. 10 muestra un diagrama de bloques funcional para un ejemplo de otro aparato de comunicación de red inalámbrica. Los expertos en la técnica apreciarán que un aparato de comunicación de red inalámbrica puede tener más componentes que el aparato de comunicación de red inalámbrica 1000 mostrado en la FIG. 10. El aparato de comunicación de red inalámbrica 1000 mostrado incluye solamente esos componentes útiles para la descripción de algunas características destacables de implementaciones dentro del alcance de las reivindicaciones. El aparato de comunicación de red inalámbrica 1000 puede incluir un gestor de conexiones 1002, un autentificador 1004 y un gestor de credenciales 1006.

[0096] En algunas implementaciones, el gestor de conexiones 1002 se puede configurar para recibir una petición de conexión a través de la red del proveedor de servicios desde el dispositivo para el servicio de abastecimiento, la petición de conexión que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo. El gestor de conexiones 1002 puede incluir uno o más entre un receptor, una antena, un chip programable, un procesador, una memoria y una interfaz de red. En algunas implementaciones, los medios para recibir una petición de conexión pueden incluir el gestor de conexiones 1002.

[0097] En algunas implementaciones, el autentificador 1004 se puede configurar para autentificar el dispositivo basándose, al menos en parte, en la información del proveedor del dispositivo. El autentificador 1004 puede incluir uno o más entre una interfaz de red de datos, un comparador, un procesador de certificados, un procesador y una memoria. En algunas implementaciones, los medios para autentificar el dispositivo pueden incluir el autentificador 1004.

[0098] En algunas implementaciones, el gestor de credenciales 1006 se puede configurar para provocar la transmisión de información de abastecimiento asociada con un abono tras la autentificación del dispositivo. El gestor de credenciales 1006 puede incluir uno o más entre un transmisor, una antena, una memoria, un procesador, un generador de señales y un almacén de credenciales. En algunas implementaciones, los medios para transmitir información de abastecimiento pueden incluir el gestor de credenciales 1006.

[0099] Como se usa en el presente documento, el término “determinar” abarca una amplia variedad de acciones. Por ejemplo, "determinar" puede incluir calcular, computar, procesar, derivar, investigar, consultar (por ejemplo, consultar una tabla, una base de datos u otra estructura de datos), averiguar y similares. También, "determinar" puede incluir recibir (por ejemplo, recibir información), acceder (por ejemplo, acceder a datos en una memoria) y similares. También, "determinar" puede incluir resolver, seleccionar, elegir, establecer y similares. Además, un “ancho de canal”, como se usa en el presente documento, puede abarcar, o se puede denominar también como, un ancho de banda en determinados aspectos.

[0100] Como se usa en el presente documento, una frase que se refiere a “al menos uno de entre” una lista de elementos se refiere a cualquier combinación de esos elementos, incluidos elementos individuales. Como ejemplo, "al menos uno de entre: *a, b* o *c*" pretende abarcar: *a, b, c, a-b, a-c, b-c* y *a-b-c.*

[0101] Las diversas operaciones de los procedimientos descritos anteriormente pueden ser realizadas por cualquier medio adecuado, capaz de realizar las operaciones, tal como diversos componentes, circuitos y/o módulo(s) de hardware y/o software. En general, cualquier operación ilustrada en las figuras puede ser realizada por correspondientes medios funcionales capaces de realizar las operaciones.

[0102] Los diversos bloques, módulos y circuitos lógicos ilustrativos descritos en relación con la presente divulgación se pueden implementar o realizar con un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una señal de matriz de puertas programables in situ (FPGA) u otro dispositivo de lógica programable (PLD), lógica de puertas discretas o de transistores, componentes de hardware discretos o cualquier combinación de estos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados disponible en el mercado. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

[0103] En uno o más aspectos, las funciones descritas pueden implementarse en hardware, software, firmware o cualquier combinación de los mismos. Si se implementan en software, las funciones se pueden almacenar en, o transmitir por, un medio legible por ordenador, como una o más instrucciones o código. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informático como medios de comunicación que incluyen cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que se pueda acceder mediante un ordenador. A modo de ejemplo y no de limitación, dichos medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otros dispositivos de almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda utilizarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Además, cualquier conexión recibe adecuadamente la denominación de medio legible por ordenador. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota, usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas, tales como infrarrojos, radio y microondas, se incluyen en la definición de medio. Los discos, como se usan en el presente documento, incluyen el disco compacto (CD), el disco láser, el disco óptico, el disco versátil digital (DVD), el disco flexible y el disco Blu-ray, donde algunos discos reproducen habitualmente los datos magnéticamente, mientras que otros discos reproducen los datos ópticamente con láseres. Por tanto, en algunos aspectos, el medio legible por ordenador puede comprender un medio no transitorio legible por ordenador (por ejemplo, medios tangibles). Además, en algunos aspectos, el medio legible por ordenador puede comprender un medio transitorio legible por ordenador (por ejemplo, una señal). Las combinaciones de lo anterior se deberían incluir también dentro del alcance de los medios legibles por ordenador.

[0104] Los procedimientos divulgados en el presente documento comprenden una o más etapas o acciones para lograr el procedimiento descrito. Las etapas y/o acciones de procedimiento se pueden intercambiar entre sí sin apartarse del alcance de las reivindicaciones. En otras palabras, a menos que se especifique un orden específico de etapas o acciones, el orden y/o el uso de etapas y/o acciones específicas se pueden modificar sin apartarse del alcance de las reivindicaciones.

[0105] Las funciones descritas pueden implementarse en hardware, software, firmware o en cualquier combinación de estos. Si se implementan en software, las funciones pueden almacenarse como una o más instrucciones en un medio legible por ordenador. Un medio de almacenamiento puede ser cualquier medio disponible al que se pueda acceder mediante un ordenador. A modo de ejemplo y no de limitación, dichos medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otros dispositivos de almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda utilizarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. El término

disco, como se usa en el presente documento, incluye disco compacto (CD), disco láser, disco óptico, disco versátil digital (DVD), disco flexible y disco Blu-ray®, donde algunos discos reproducen normalmente los datos magnéticamente, mientras que otros discos reproducen los datos ópticamente con láseres.

[0106] Por tanto, determinados aspectos pueden comprender un producto de programa informático para realizar las operaciones presentadas en el presente documento. Por ejemplo, dicho producto de programa informático puede comprender un medio legible por ordenador que tiene instrucciones almacenadas (y/o codificadas) en el mismo, siendo las instrucciones ejecutables por uno o más procesadores para realizar las operaciones descritas en el presente documento. Para determinados aspectos, el producto de programa informático puede incluir material de embalaje.

[0107] El software o las instrucciones pueden transmitirse también por un medio de transmisión. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otro origen remoto mediante un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o unas tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas tales como infrarrojos, radio y microondas están incluidos en la definición de medio de transmisión.

[0108] Además, se debería apreciar que los módulos y/u otros medios adecuados para realizar los procedimientos y las técnicas descritos en el presente documento se pueden descargar y/u obtener de otra forma mediante un terminal de usuario y/o una estación base, según corresponda. Por ejemplo, un dispositivo de este tipo puede estar acoplado a un servidor para facilitar la transferencia de medios para realizar los procedimientos descritos en el presente documento. De forma alternativa, diversos procedimientos descritos en el presente documento se pueden proporcionar mediante medios de almacenamiento (por ejemplo, RAM, ROM, un medio de almacenamiento físico tal como un disco compacto (CD) o un disco flexible, etc.), de manera que un terminal de usuario y/o una estación base puedan obtener los diversos procedimientos tras acoplarse o proporcionar los medios de almacenamiento al dispositivo. Además, se puede utilizar cualquier otra técnica adecuada para proporcionar a un dispositivo los procedimientos y técnicas descritos en el presente documento.

[0109] Se ha de entender que las reivindicaciones no están limitadas a la configuración y a los componentes exactos ilustrados anteriormente. Se pueden realizar diversas modificaciones, cambios y variantes en la disposición, el funcionamiento y los detalles de los procedimientos y del aparato descritos anteriormente sin apartarse del alcance de las reivindicaciones.

[0110] Aunque lo anterior está orientado a aspectos de la presente divulgación, pueden concebirse aspectos diferentes y adicionales de la divulgación sin apartarse del alcance básico de la misma, y el alcance de la misma está determinado por las reivindicaciones siguientes.

REIVINDICACIONES

1. Un procedimiento de obtención de información de abastecimiento a través de una red del proveedor de servicios para un dispositivo (106), el procedimiento que es realizado por el dispositivo (106) y que comprende:

transmitir, a través de la red del proveedor de servicios, una petición de conexión (702) para el servicio de abastecimiento, la petición de conexión que incluye información de arranque, la información de arranque que incluye información del proveedor del dispositivo que tiene un

identificador único para el dispositivo y un certificado asociado con el identificador único para el dispositivo, en el que la petición de conexión incluye un campo de tipo de conexión identificado como abastecimiento o servicio de abastecimiento;

recibir una petición para la autentificación de la red del proveedor de servicios;

transmitir una respuesta de desafío basada, al menos en parte, en una credencial predeterminada compartida por múltiples dispositivos configurados para obtener información de abastecimiento para cada uno de los múltiples dispositivos que usan la credencial predeterminada compartida a través de la red del proveedor de servicios, los múltiples dispositivos que incluyen el dispositivo; y

recibir información de abastecimiento (704) de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo y la respuesta al desafío y la identificación de un abono para el dispositivo; y

tras determinar que el dispositivo se ha autentificado sin identificación de un abono para el dispositivo:

obtener una oferta de abono de un proveedor de credenciales a través de la red del proveedor de servicios;

transmitir un mensaje que indique la aceptación de la oferta de abono; y

recibir información de abastecimiento basada en la oferta de abono aceptada.

2. El procedimiento de la reivindicación 1, que además comprende:

recibir una petición de desafío para autentificar la información del proveedor del dispositivo; y

transmitir una respuesta de desafío basada, al menos en parte, en la información del proveedor del dispositivo.

3. El procedimiento de la reivindicación 1, que además comprende:

obtener una clave de sesión, la clave de sesión basada, al menos en parte, en la información del proveedor del dispositivo; y

asegurar las comunicaciones entre el dispositivo y la red del proveedor de servicios basándose, al menos en parte, en la clave de sesión.

4. El procedimiento de la reivindicación 1, que además comprende:

desconectarse de la red del proveedor de servicios tras recibir la información de abastecimiento; y

obtener servicio basándose, al menos en parte, en la información de abastecimiento recibida.

5. Un dispositivo (202) para obtener información de abastecimiento a través de una red del proveedor de servicios, el dispositivo que comprende:

medios para transmitir, a través de la red del proveedor de servicios, una petición de conexión para el servicio de abastecimiento,

la petición de conexión que incluye información de arranque, la información de arranque que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo y un certificado asociado con el identificador único para el dispositivo, en el que la petición de conexión incluye un campo de tipo de conexión identificado como abastecimiento o servicio de abastecimiento;

medios para recibir una petición de desafío para la autentificación;

medios para transmitir una respuesta de desafío basada, al menos en parte, en una credencial predeterminada compartida por múltiples dispositivos configurados para obtener información de abastecimiento para cada uno de los múltiples dispositivos que usan la credencial predeterminada compartida a través de la red del proveedor de servicios, los múltiples dispositivos que incluyen el dispositivo; y

medios para recibir información de abastecimiento de la red del proveedor de servicios tras la autentificación de la información del proveedor del dispositivo y la respuesta al desafío y la identificación de un abono para el dispositivo; y

tras determinar que el dispositivo se ha autentificado sin identificación de un abono para el dispositivo:

medios para recibir una oferta de abono de un proveedor de credenciales a través de la red del proveedor de servicios;

medios para transmitir un mensaje que indique la aceptación de la oferta de abono; y

medios para recibir información de abastecimiento basada en la oferta de abono aceptada.

6. Un procedimiento de suministro de información de aprovisionamiento a través de una red del proveedor de servicios a un dispositivo, el procedimiento que es realizado por un aparato y que comprende:

recibir una petición de conexión del dispositivo a través de la red del proveedor de servicios para el servicio de abastecimiento, la petición de conexión que incluye información de arranque, la información de arranque que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo y un certificado asociado con el identificador único para el dispositivo, en el que la petición de conexión incluye un campo de tipo de conexión identificado como abastecimiento o servicio de abastecimiento;

transmitir una petición de desafío al dispositivo para la autentificación;

recibir una respuesta de desafío del dispositivo;

determinar si la respuesta de desafío está asociada con una credencial predeterminada compartida por múltiples dispositivos configurados para obtener información de abastecimiento para cada uno de los múltiples dispositivos que utilizan la credencial predeterminada compartida a través de la red del proveedor de servicios, los múltiples dispositivos que incluyen el dispositivo;

autentificar el dispositivo basándose, al menos en parte, en la información del proveedor del dispositivo; y

transmitir información de abastecimiento asociada con el abono tras determinar que el dispositivo se ha autentificado y asociado con un abono; y

tras determinar que el dispositivo se ha autentificado sin identificación de un abono para el dispositivo:

obtener una oferta de abono de un proveedor de credenciales;

transmitir la oferta de abono al dispositivo;

recibir un mensaje que indica la aceptación de la oferta de abono del dispositivo; y

transmitir información de abastecimiento basada en la oferta de abono aceptada al dispositivo.

7. El procedimiento de la reivindicación 1 y/o 6, en el que la petición de conexión comprende un tipo de abastecimiento y, preferentemente, en el que el tipo de abastecimiento para la petición de conexión se incluye en un elemento de información de la petición de conexión.

8. El procedimiento de la reivindicación 6, que además comprende:

transmitir una petición de desafío para autentificar el dispositivo;

recibir una respuesta de desafío; y

determinar si la respuesta de desafío está asociada con un abono basada, al menos en parte, en la información del proveedor del dispositivo.

9. El procedimiento de la reivindicación 6, que además comprende:

generar una clave de sesión, la clave de sesión basada, al menos en parte, en información del proveedor del dispositivo; y

asegurar las comunicaciones entre el dispositivo y la red del proveedor de servicios basándose, al menos en parte, en la clave de sesión.

10. El procedimiento de la reivindicación 1 o 6, en el que la información del proveedor del dispositivo además comprende un certificado de cifrado asociado con un proveedor del dispositivo.

11. El procedimiento de la reivindicación 1 o 6, en el que el identificador único para el dispositivo comprende al menos uno de entre un identificador internacional de equipo móvil para el dispositivo y un identificador de equipo móvil para el dispositivo.

12. El procedimiento de la reivindicación 1 o 6, en el que la red del proveedor de servicios es una red celular.

13. El procedimiento de la reivindicación 6, que además comprende desconectar el dispositivo de la red del proveedor de servicios tras la transmisión de la información de abastecimiento.

14. Aparato para proporcionar información de abastecimiento a través de una red del proveedor de servicios a un dispositivo, el aparato que comprende:

medios para recibir una petición de conexión del dispositivo a través de la red del proveedor de servicios para el servicio de abastecimiento, la petición de conexión que incluye información de arranque, la información de arranque que incluye información del proveedor del dispositivo que tiene un identificador único para el dispositivo y un certificado asociado con el identificador único para el dispositivo, en el que la petición de conexión incluye un campo de tipo de conexión identificado como abastecimiento o servicio de abastecimiento;

medios para transmitir una petición de desafío al dispositivo para la autentificación;

medios para recibir una respuesta de desafío del dispositivo;

medios para determinar si la respuesta de desafío está asociada con una credencial predeterminada compartida por múltiples dispositivos configurados para obtener información de abastecimiento para cada uno de los múltiples dispositivos que utilizan la credencial predeterminada compartida a través de la red del proveedor de servicios, los múltiples dispositivos que incluyen el dispositivo;

medios para autentificar el dispositivo basándose, al menos en parte, en información del proveedor del dispositivo; y

medios para transmitir información de abastecimiento asociada con el abono tras determinar que el dispositivo se ha autentificado y asociado con un abono; y

tras determinar que el dispositivo se ha autentificado sin identificación de un abono para el dispositivo:

medios para obtener una oferta de abono de un proveedor de credenciales;

medios para transmitir la oferta de abono al dispositivo;

medios para recibir un mensaje que indica aceptación de la oferta de abono del dispositivo; y

medios para transmitir información de abastecimiento basada en la oferta de abono aceptada al dispositivo.

15. Un medio de almacenamiento legible por ordenador, que comprende instrucciones ejecutables por un procesador de un aparato, las instrucciones que hacen que el aparato lleve a cabo el procedimiento de una cualquiera de las reivindicaciones 1-4 o 6-13.

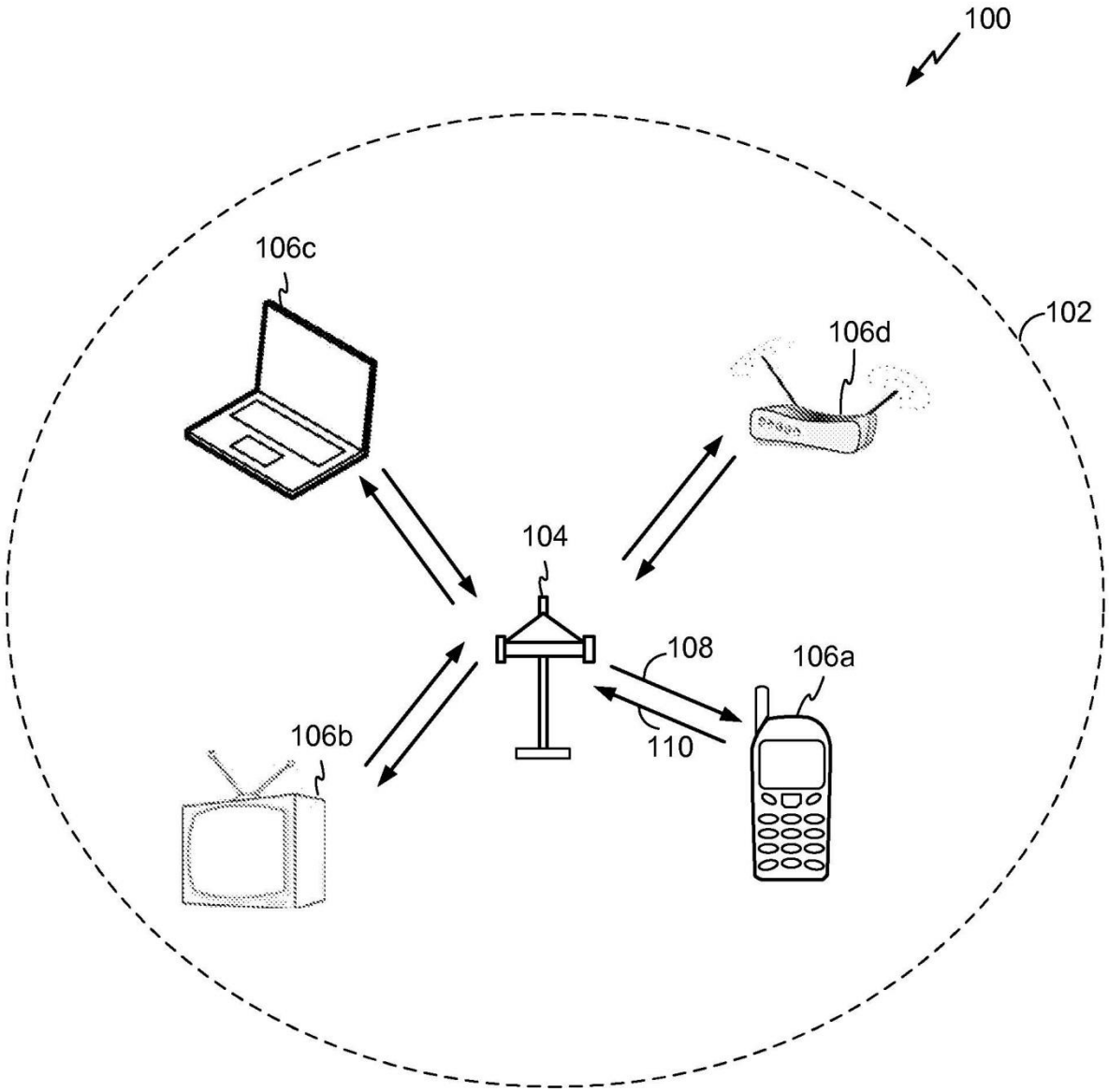

FIG. 1

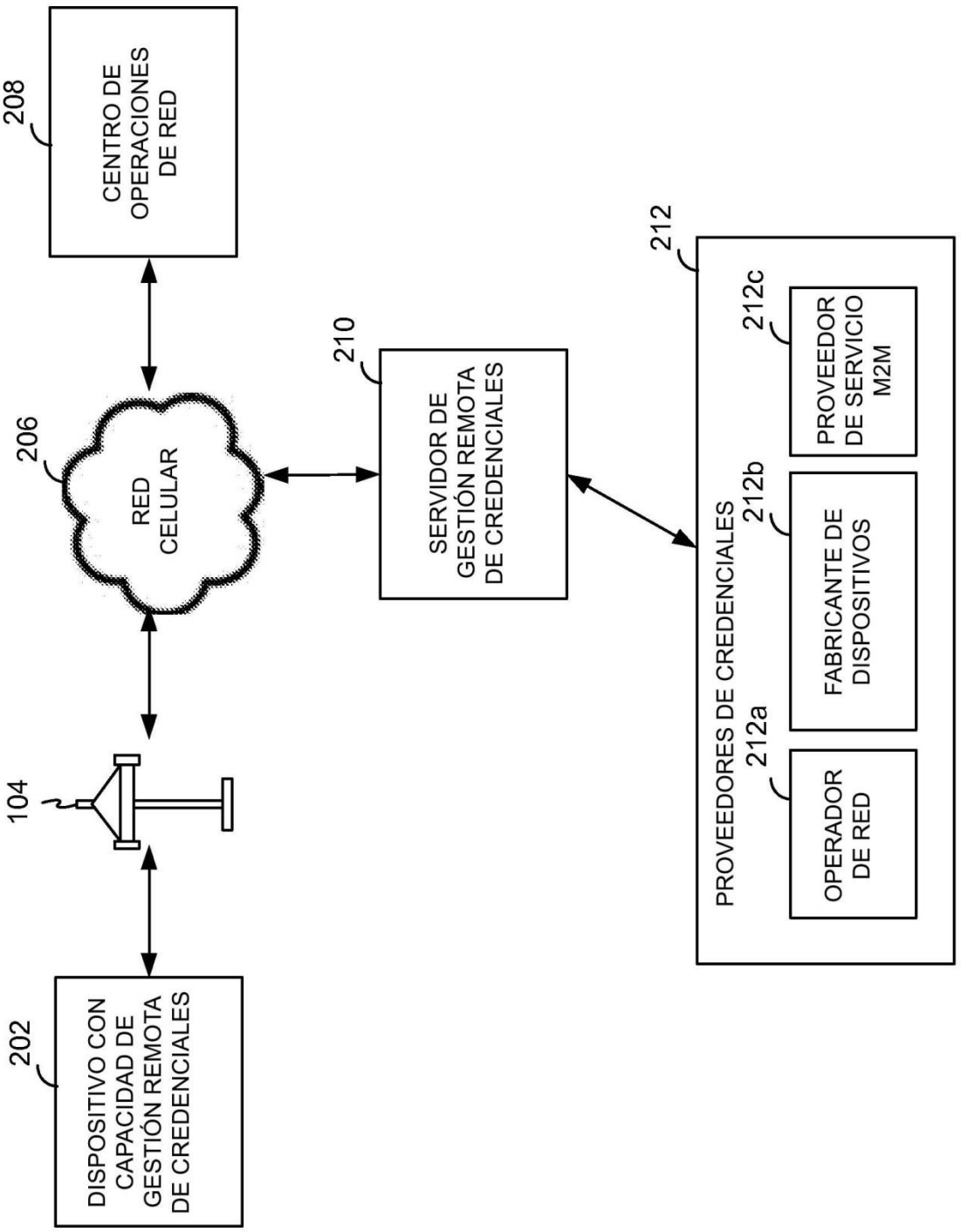
208
CENTRO DE OPERACIONES DE RED
206
RED CELULAR
210
SERVIDOR DE GESTIÓN REMOTA DE CREDENCIALES
212
PROVEEDORES DE CREDENCIALES
212a
OPERADOR DE RED
212b
FABRICANTE DE DISPOSITIVOS
212c
PROVEEDOR DE SERVICIO M2M
104
202
DISPOSITIVO CON CAPACIDAD DE GESTIÓN REMOTA DE CREDENCIALES

FIG. 2

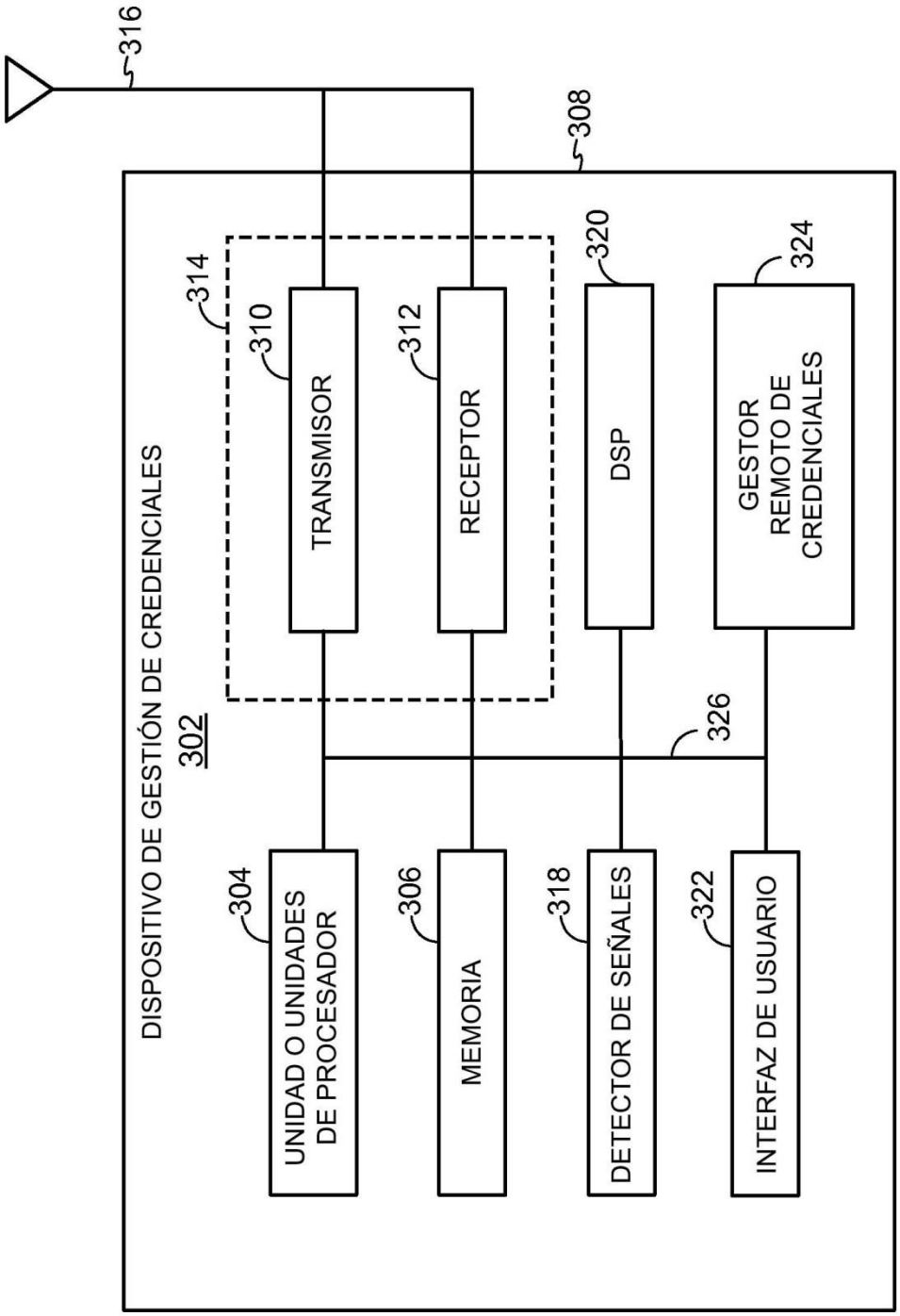
316
308
DISPOSITIVO DE GESTIÓN DE CREDENCIALES
302
314
310
TRANSMISOR
312
RECEPTOR
320
DSP
324
GESTOR REMOTO DE CREDENCIALES
326
304
UNIDAD O UNIDADES DE PROCESADOR
306
MEMORIA
318
DETECTOR DE SEÑALES
322
INTERFAZ DE USUARIO

FIG. 3

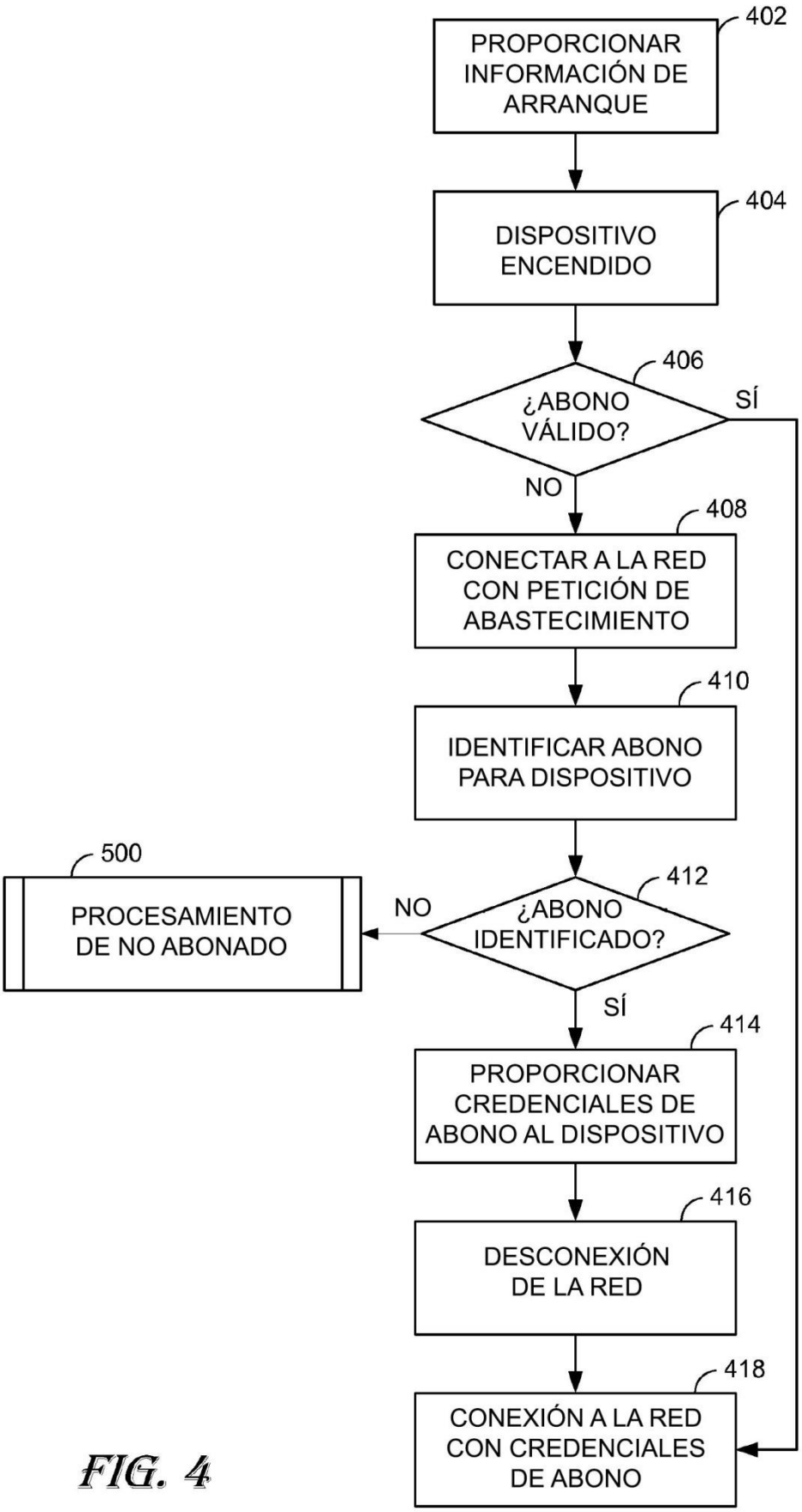
402
PROPORCIONAR INFORMACIÓN DE ARRANQUE
404
DISPOSITIVO ENCENDIDO
406
¿ABONO VÁLIDO?
SÍ
NO
408
CONECTAR A LA RED CON PETICIÓN DE ABASTECIMIENTO
410
IDENTIFICAR ABONO PARA DISPOSITIVO
500
PROCESAMIENTO DE NO ABONADO
NO
412
¿ABONO IDENTIFICADO?
SÍ
414
PROPORCIONAR CREDENCIALES DE ABONO AL DISPOSITIVO
416
DESCONEXIÓN DE LA RED
418
CONEXIÓN A LA RED CON CREDENCIALES DE ABONO

FIG. 4

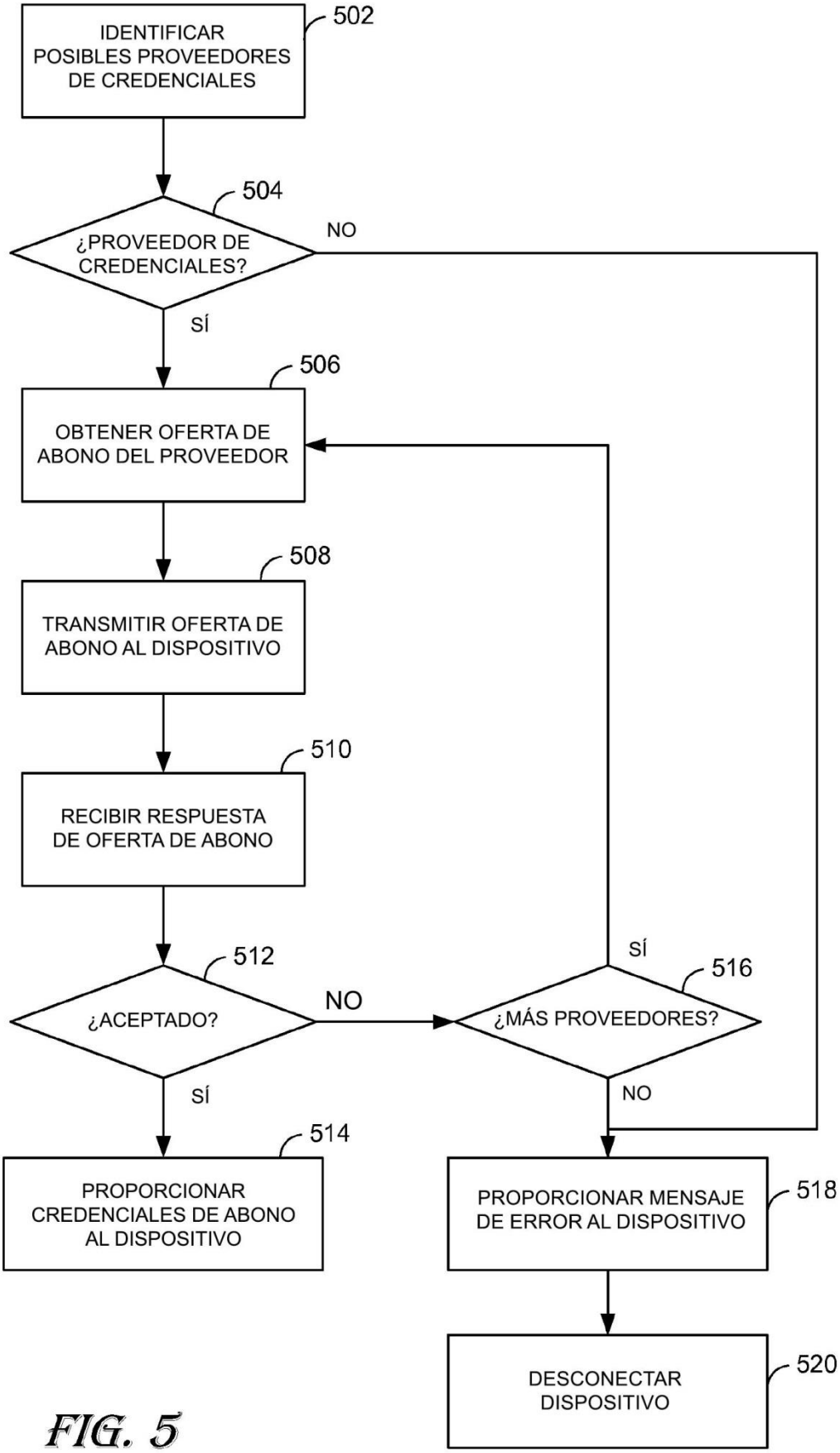
IDENTIFICAR POSIBLES PROVEEDORES DE CREDENCIALES
502
¿PROVEEDOR DE CREDENCIALES?
504
NO
SÍ
OBTENER OFERTA DE ABONO DEL PROVEEDOR
506
TRANSMITIR OFERTA DE ABONO AL DISPOSITIVO
508
RECIBIR RESPUESTA DE OFERTA DE ABONO
510
¿ACEPTADO?
512
NO
SÍ
¿MÁS PROVEEDORES?
516
SÍ
NO
PROPORCIONAR CREDENCIALES DE ABONO AL DISPOSITIVO
514
PROPORCIONAR MENSAJE DE ERROR AL DISPOSITIVO
518
DESCONECTAR DISPOSITIVO
520

FIG. 5

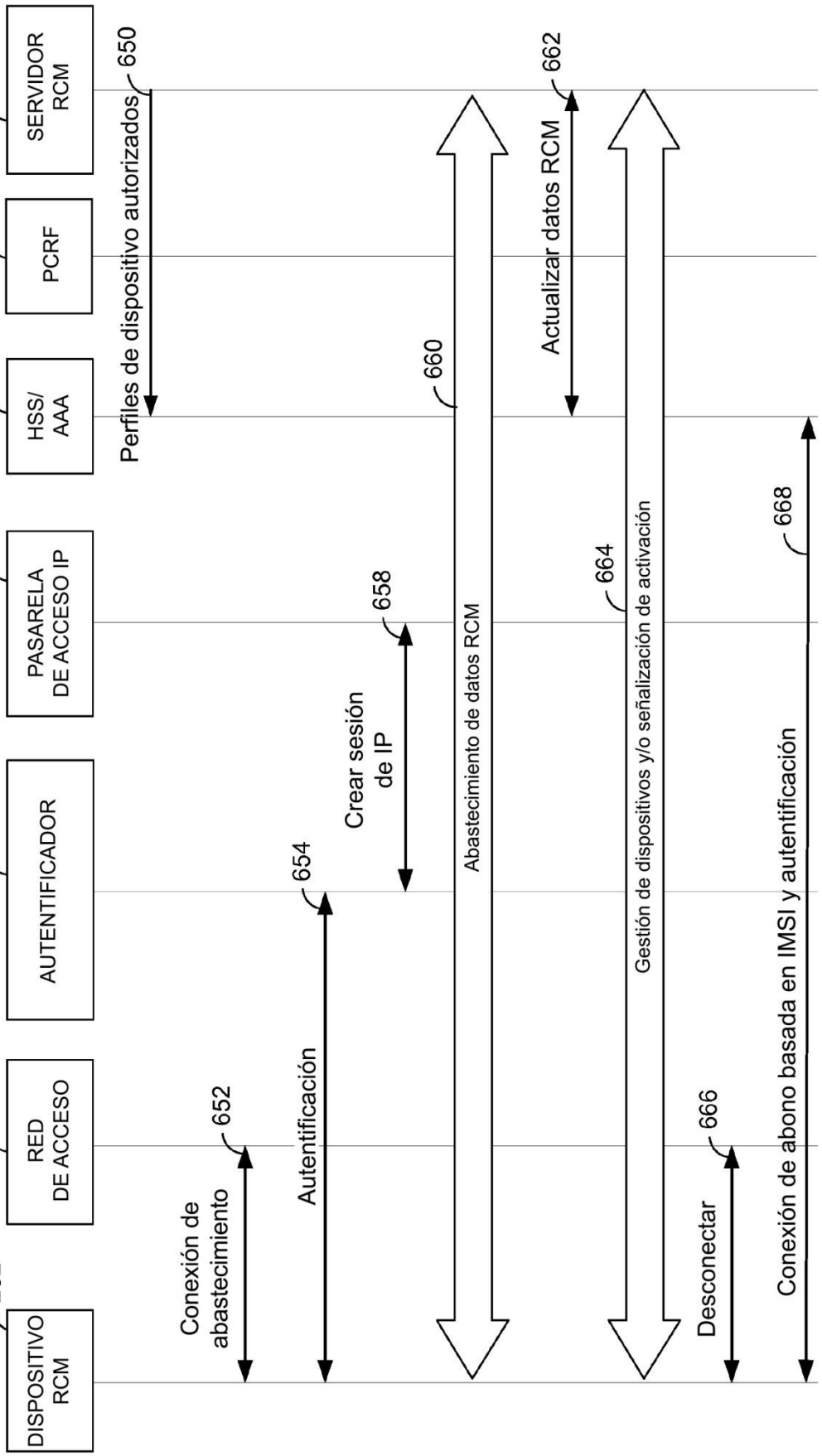
202
DISPOSITIVO RCM
104
RED DE ACCESO
604
AUTENTIFICADOR
608
PASARELA DE ACCESO IP
610
HSS/ AAA
612
PCRF
210
SERVIDOR RCM
650
Perfiles de dispositivo autorizados
652
Conexión de abastecimiento
654
Autentificación
658
Crear sesión de IP
660
Abastecimiento de datos RCM
662
Actualizar datos RCM
664
Gestión de dispositivos y/o señalización de activación
666
Desconectar
668
Conexión de abono basada en IMSI y autentificación

FIG. 6

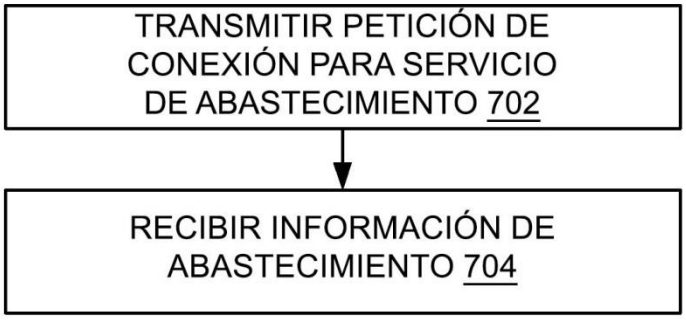
TRANSMITIR PETICIÓN DE CONEXIÓN PARA SERVICIO DE ABASTECIMIENTO 702
RECIBIR INFORMACIÓN DE ABASTECIMIENTO 704

FIG. 7

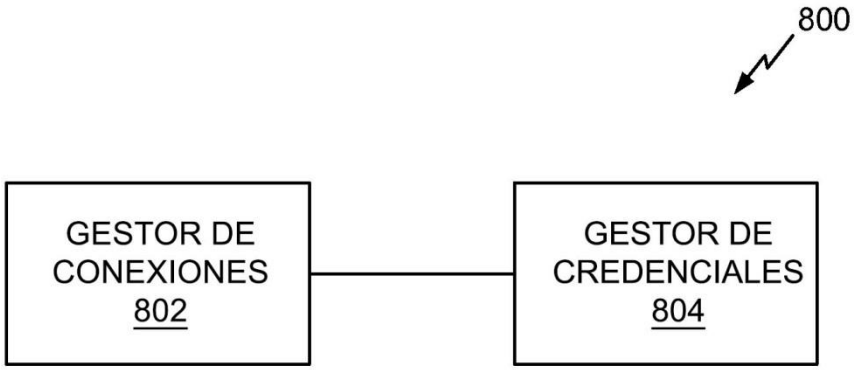
800
GESTOR DE CONEXIONES 802
GESTOR DE CREDENCIALES 804

FIG. 8

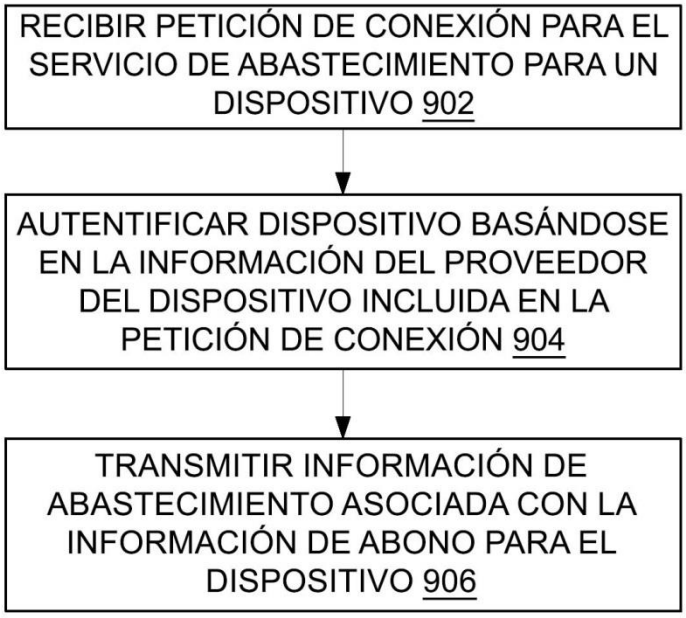
RECIBIR PETICIÓN DE CONEXIÓN PARA EL SERVICIO DE ABASTECIMIENTO PARA UN DISPOSITIVO 902
AUTENTIFICAR DISPOSITIVO BASÁNDOSE EN LA INFORMACIÓN DEL PROVEEDOR DEL DISPOSITIVO INCLUIDA EN LA PETICIÓN DE CONEXIÓN 904
TRANSMITIR INFORMACIÓN DE ABASTECIMIENTO ASOCIADA CON LA INFORMACIÓN DE ABONO PARA EL DISPOSITIVO 906

FIG. 9

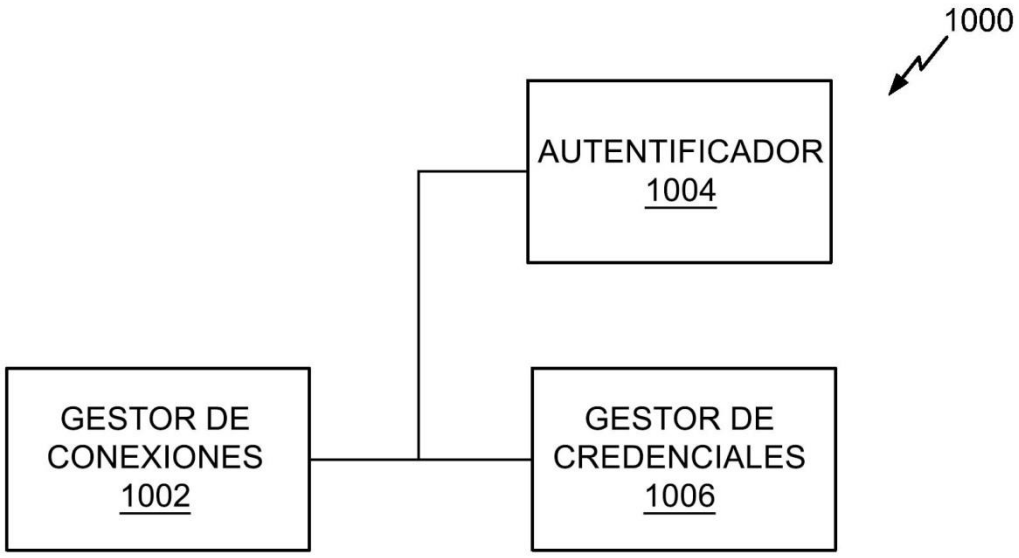
1000
AUTENTIFICADOR 1004
GESTOR DE CONEXIONES 1002
GESTOR DE CREDENCIALES 1006

FIG. 10