(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 724 099**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/06 (2006.01)
H04L 9/08 (2006.01)
H04W 12/06 (2009.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.02.2016 PCT/US2016/018855**

(87) Fecha y número de publicación internacional: **15.09.2016 WO16144516**

(96) Fecha de presentación y número de la solicitud europea: **22.02.2016 E 16707362 (6)**

(97) Fecha y número de publicación de la concesión europea: **30.01.2019 EP 3266180**

(54) Título: **Conectividad patrocinada a redes celulares utilizando credenciales existentes**

(30) Prioridad:

06.03.2015 US 201562129462 P
03.08.2015 US 201514817123

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.09.2019

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
ATTN: International IP Administration 5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

LEE, SOO BUM;
PALANIGOUNDER, ANAND y
HORN, GAVIN BERNARD

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Conectividad patrocinada a redes celulares utilizando credenciales existentes

CAMPO TÉCNICO

[0001] Esta solicitud se refiere en general a sistemas de comunicación inalámbrica, y más particularmente a un proveedor de servicios de aplicaciones que patrocina acceso a través de una red de servicio a uno o más servicios. Ciertos modos de realización habilitan y proporcionan dispositivos, procedimientos y sistemas capaces de y/o configurados para acceder a servicios de aplicaciones de red en situaciones en las que los usuarios pueden carecer de suscripciones de red de manera escalable, segura y rastreable (por ejemplo, con fines de facturación/medición).

INTRODUCCIÓN

[0002] Para recibir servicios desde una red, un equipo de usuario (UE) desconocido tiene que registrarse en la red o ser conocido de otra manera para la red. Esto se logra mediante un procedimiento de conexión de red. En general, un UE que no tiene una suscripción para el servicio no puede conectarse a una red de servicio para recibir servicios de voz o datos (aparte del servicio de emergencia, como el 911 en los Estados Unidos, por ejemplo). Se han hecho intentos para permitir que un UE siga recibiendo el servicio patrocinando la conectividad del UE a la red de servicio. La conectividad patrocinada típicamente implica un permiso limitado de acceso a la red a una aplicación o servicio específico que está patrocinado por la aplicación o servicio específico.

[0003] Los enfoques convencionales actuales no incluyen ciertos tipos de dispositivos (por ejemplo, los UE sin tarjetas SIM y/o suscripciones) para ser capaces de aprovecharse de la conectividad patrocinada y son ineficientes o exponer la red de servicio a tráfico no deseado (o malicioso) en su red central. Como se analiza a continuación, los aspectos y los modos de realización de esta divulgación tienen como objetivo mejorar la conectividad patrocinada.

[0004] El documento US 2013/316674 A1 divulga un procedimiento y un dispositivo para controlar el cobro en un sistema de comunicación móvil. El documento US 2014/308918 A1 divulga un procedimiento y un aparato para un proveedor de servicios de Internet que proporciona un servicio patrocinado, en el que un proveedor de servicios paga una tarifa de uso de comunicación móvil en lugar de un equipo de usuario.

BREVE SUMARIO DE EJEMPLOS SELECCIONADOS

[0005] A continuación se resumen algunos aspectos de la presente divulgación para proporcionar un entendimiento básico de la tecnología analizada. Este sumario no es una visión global extensiva de todas las características contempladas de la divulgación y no está previsto tampoco ni para identificar elementos clave o críticos de todos los aspectos de la divulgación ni para delimitar el alcance de algunos o todos los aspectos de la divulgación. Su única finalidad es presentar algunos conceptos de uno o más aspectos de la divulgación de manera resumida como un preludio de la descripción más detallada que se presentará posteriormente.

[0006] En un aspecto de la divulgación, un procedimiento para acceder a un servicio incluye identificar, mediante un equipo de usuario (UE), una red de servicio a través de la cual un servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio; enviar, desde el UE, una petición de conexión a la red de servicio con un token o testigo de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones, con el token de cliente que no es reconocible como una credencial de acceso celular a la red de servicio; y autentificar, mediante el UE, a la red de servicio a través del servidor de proveedor de servicios de aplicaciones para el acceso patrocinado al servicio basado en la credencial preexistente.

[0007] En un aspecto adicional de la divulgación, un procedimiento para permitir el acceso a un servicio patrocinado por un servidor de proveedor de servicios de aplicaciones incluye recibir, a partir de una red de servicio de intervención a través del cual el servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio, una petición de información de autentificación basada en una petición de conexión de un equipo de usuario (UE), la petición de información de autentificación que comprende un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones y que no es reconocible como una credencial de acceso celular a la red de servicio; determinar, mediante el servidor de proveedor de servicios de aplicaciones, la información de autentificación basada en la credencial preexistente a la que puede acceder el servidor de proveedor de servicios de aplicaciones en respuesta a la petición de información de autentificación; y transmitir, desde el servidor de proveedor de servicios de aplicaciones, la información de autentificación en una respuesta a la red de servicio, en el que la información de autentificación facilita la autentificación entre el UE y la red de servicio para el acceso patrocinado al servicio basado en la credencial preexistente.

[0008] En un aspecto adicional de la divulgación, un equipo de usuario (UE) para acceder a un servicio incluye un transceptor configurado para: ayudar en la identificación de una red de servicio a través del cual un servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio; y enviar una petición de conexión a la red de servicio con un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de

servicios de aplicaciones, siendo el token de cliente irreconocible como una credencial de acceso celular a la red de servicio; y un procesador configurado para autentificarse en la red de servicio a través del servidor de proveedor de servicios de aplicaciones para el acceso patrocinado al servicio basado en la credencial preexistente.

[0009] En un aspecto adicional de la divulgación, un servidor de proveedor de servicios de aplicaciones que patrocina el acceso a un servicio incluye un transceptor configurado para recibir, desde una red de servicio de intervención a través del cual el servidor de proveedor de servicios de aplicaciones de acceso al servicio, una petición de información de autentificación basada en una petición de conexión de un equipo de usuario (UE), con la petición de información de autentificación que comprende un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones y que no es reconocible como una credencial de acceso celular a la red de servicio; y un procesador configurado para determinar la información de autentificación basada en la credencial preexistente accesible por el servidor de proveedor de servicios de aplicaciones en respuesta a la petición de información de autentificación, en el que el transceptor está configurado además para transmitir la información de autentificación en una respuesta a la red de servicio, y en el que la información de autentificación ayuda en la autentificación entre el UE y la red de servicio para el acceso patrocinado al servicio basado en la credencial preexistente.

[0010] En un aspecto adicional de la divulgación, un medio legible por ordenador que tiene código de programa grabado en el mismo incluye código de programa que comprende código para hacer que un equipo de usuario (UE) identifique una red de servicio a través de la cual un servidor de proveedor de servicios de aplicaciones patrocina el acceso a un servicio; código para hacer que el UE envíe una petición de conexión a la red de servicio con un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones, con el token de cliente que no es reconocible como una credencial de acceso celular a la red de servicio; y el código para hacer que el UE se autentifique en la red de servicio a través del servidor de proveedor de servicios de aplicaciones para el acceso patrocinado al servicio basado en la credencial preexistente.

[0011] En un aspecto adicional de la divulgación, un medio legible por ordenador que tiene código de programa grabado en el mismo incluye código de programa que comprende código para hacer que un servidor de proveedor de servicios de aplicaciones reciba, desde una red de servicio de intervención a través del cual el servidor de proveedor de servicios de aplicaciones patrocina el acceso a un servicio, una petición de información de autentificación basada en una petición de conexión de un equipo de usuario (UE), con la petición de información de autentificación comprende un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones y no es reconocible como una credencial de acceso celular a la red de servicio; código para hacer que el servidor de proveedor de servicios de aplicaciones determine la información de autentificación basada en la credencial preexistente a la que puede acceder el servidor de proveedor de servicios de aplicaciones en respuesta a la petición de información de autentificación; y el código para hacer que el servidor de proveedor de servicios de aplicaciones transmita la información de autentificación en una respuesta a la red de servicio, en el que la información de autentificación ayuda en la autentificación entre el UE y la red de servicio para el acceso patrocinado al servicio basado en la credencial preexistente.

[0012] Otros aspectos, características y modos de realización de la presente divulgación resultarán evidentes para los expertos en la técnica, tras revisar la siguiente descripción de modos de realización a modo de ejemplo y específicos de la presente divulgación junto con las figuras adjuntas. Aunque las características de la presente divulgación pueden analizarse con respecto a ciertos modos de realización y figuras a continuación, todos los modos de realización de la presente divulgación pueden incluir una o más de las características analizadas en el presente documento. En otras palabras, aunque pueden analizarse uno o más modos de realización como que tienen ciertas características ventajosas, también se pueden usar una o más de dichas características de acuerdo con los diversos modos de realización de la divulgación analizados en el presente documento. De forma similar, aunque los modos de realización a modo de ejemplo pueden analizarse a continuación como modos de realización de dispositivo, sistema o procedimiento, debería entenderse que dichos modos de realización a modo de ejemplo pueden implementarse en diversos dispositivos, sistemas y procedimientos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0013]

La FIG. 1 ilustra una red de comunicaciones inalámbricas de acuerdo con ciertos aspectos de la presente divulgación.

La FIG. 2 es un diagrama de bloques de un UE a modo de ejemplo de acuerdo con modos de realización de la presente divulgación.

La FIG. 3 es un diagrama de bloques de un servidor a modo de ejemplo de acuerdo con modos de realización de la presente divulgación.

La FIG. 4 es un diagrama de bloques que ilustra un sistema transmisor a modo de ejemplo de acuerdo con varios aspectos de la presente divulgación.

La FIG. 5 es un diagrama de protocolo que ilustra aspectos de señalización a modo de ejemplo entre un UE, una red de servicio y un proveedor de servicios de aplicaciones para proporcionar conectividad patrocinada de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 6 es un diagrama de protocolo que ilustra aspectos de señalización a modo de ejemplo entre un UE, una red de servicio y un proveedor de servicios de aplicaciones para proporcionar conectividad patrocinada de acuerdo con diversos aspectos de la presente divulgación.

La FIG. 7A es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para acceder a una red para un servicio patrocinado por un servidor de acuerdo con varios aspectos de la presente divulgación.

La FIG. 7B es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para otorgar acceso a la red para un servicio patrocinado por un servidor de acuerdo con varios aspectos de la presente divulgación.

La FIG. 7C es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para facilitar el acceso a la red para un servicio patrocinado por un servidor de acuerdo con varios aspectos de la presente divulgación.

La FIG. 8A es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para acceder a una red para un servicio patrocinado por un servidor de acuerdo con varios aspectos de la presente divulgación.

La FIG. 8B es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para otorgar acceso a la red para un servicio patrocinado por un servidor de acuerdo con varios aspectos de la presente divulgación.

La FIG. 8C es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para facilitar el acceso a la red para un servicio patrocinado por un servidor de acuerdo con varios aspectos de la presente divulgación.

DESCRIPCIÓN DETALLADA

[0014] La descripción detallada expuesta a continuación en relación con los dibujos adjuntos está concebida como una descripción de diversas configuraciones y no está concebida para representar las únicas configuraciones en las cuales pueden llevarse a la práctica los conceptos descritos en el presente documento. La descripción detallada incluye detalles específicos con el fin de proporcionar un entendimiento exhaustivo de los diversos conceptos. Sin embargo, resultará evidente para los expertos en la materia que estos conceptos pueden llevarse a la práctica sin estos detalles específicos. En algunos ejemplos, se muestran estructuras y componentes bien conocidos en forma de diagrama de bloques para evitar oscurecer dichos conceptos.

[0015] Las técnicas descritas en el presente documento pueden usarse para diversas redes de comunicación inalámbrica, tales como las de CDMA, TDMA, FDMA, OFDMA, SC-FDMA y otras redes. Los términos "red" y "sistema" se usan a menudo de forma intercambiable. Una red CDMA puede implementar una tecnología de radio, tal como el Acceso Radioeléctrico Terrestre Universal (UTRA), cdma2000, etc. UTRA incluye CDMA de Banda Ancha (WCDMA) y otras variantes de CDMA. cdma2000 cubre las normas IS-2000, IS-95 e IS-856. Una red de TDMA puede implementar una tecnología de radio tal como el Sistema Global de Comunicaciones Móviles (GSM). Una red de OFDMA puede implementar una tecnología de radio tal como UTRA Evolucionado (E-UTRA), Banda Ultra Ancha Móvil (UMB), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDMA, etc. UTRA y E-UTRA son parte del Sistema Universal de Telecomunicaciones Móviles (UMTS). La Evolución a Largo Plazo (LTE) y la LTE Avanzada (LTE-A) del 3GPP son versiones nuevas del UMTS que usan el E-UTRA. UTRA, E-UTRA, UMTS, LTE, LTE-A y GSM se describen en documentos de una organización llamada "3rd Generation Partnership Project [Proyecto de Colaboración de Tercera Generación]" (3GPP). El CDMA2000 y la UMB se describen en documentos de una organización llamada "3rd Generation Partnership Project 2 [Segundo Proyecto de Colaboración de Tercera Generación]" (3GPP2). Las técnicas descritas en el presente documento pueden usarse para las redes inalámbricas y las tecnologías de radio mencionadas anteriormente, así como para otras redes inalámbricas y tecnologías de radio, como una red de próxima generación (por ejemplo, 5.ª generación (5G)). Los modos de realización de esta divulgación están dirigidos a cualquier tipo de esquema de modulación que se puede usar en una o más de las redes mencionadas anteriormente y/o aquellas que aún no se han desarrollado.

[0016] Los modos de realización de la presente divulgación introducen sistemas y técnicas para facilitar la conectividad patrocinada de un equipo de usuario (UE) en una red de servicio (por ejemplo, una red central tal como una red de núcleo de paquete evolucionado (EPC)).

[0017] Un ejemplo de conectividad patrocinada es el reenvío basado en nombre de punto de acceso (APN). En el reenvío basado en APN, un UE tiene una tarjeta SIM que ha sido configurada con un APN por un proveedor de servicios de aplicaciones de patrocinio (por ejemplo, un mercado en línea, etc.). El UE envía el tráfico de datos a una red de servicio, y la red de servicio aplica una regla en una pasarela de red de datos pública (PDN) en una red externa

basada en la información de perfil de suscripción provista de la información configurada en la tarjeta SIM del UE. Por lo tanto, el reenvío basado en APN está limitado en que no se puede usar para los UE que no tienen tarjetas SIM y/o que no tienen una suscripción celular. La arquitectura genérica de bootstrapping (GBA) está igualmente limitada porque también presupone una suscripción y capacidad de SIM actual.

[0018] Otro ejemplo de conectividad patrocinada es el reenvío basado en la aplicación. Aquí es donde la red de servicio filtra el tráfico de datos de un UE basándose en las direcciones de destino de un protocolo de Internet (IP) de los paquetes de datos individuales del UE. Esto puede funcionar en escenarios donde los UE no tienen capacidad SIM o una suscripción, pero están sujetos a varios otros inconvenientes. El reenvío basado en la aplicación permite que el tráfico de datos no autentificados y/o no autorizados fluya a través de la red central de la red de servicio. Esto puede ser explotado por un atacante para sobrecargar la red de acceso al servicio (como una pasarela) con peticiones/tráfico en exceso que no pueden ser manejados por la pasarela, que aún pueden cargarse en la aplicación/servicio patrocinador. El reenvío basado en la aplicación suele ser ineficiente, ya que la red de servicio debe escanear el tráfico de datos y determinar si está destinado a un destinatario patrocinador. Este escenario también puede hacer que el reenvío basado en la aplicación sea difícil de escalar a muchos patrocinadores y/o usuarios diferentes.

[0019] La facilitación de la conectividad patrocinada de acuerdo con aspectos de la presente divulgación pueden permitir en ciertos escenarios un UE que pueden acceder a uno o más servicios por el servidor de proveedor de servicios de aplicaciones que patrocina la conectividad (por ejemplo, en una red externa a la red EPC). La entidad que patrocina el servicio a través del servidor puede aprovisionar la red de servicio antes de un intento de conexión por parte del UE. Este aprovisionamiento puede tomar la forma de un acuerdo de nivel de servicio entre el operador de la red de servicio y el operador del servidor. Después del aprovisionamiento, la red de servicio puede anunciar la conectividad patrocinada a los usuarios potencialmente interesados.

[0020] En un modo de realización, un UE puede intentar conectarse a una red que sirve después de descubrir una conectividad patrocinada a través de la red de servicio. Como parte de la petición de conexión, el UE proporciona un token de cliente (o alguna otra información basada en el cliente) que se basa en una credencial preexistente establecida entre el UE y el proveedor de servicios de aplicaciones en lugar de un identificador de abonado. Por ejemplo, el UE no puede ser aprovisionado con ninguna credencial de operador/proveedor de servicios (por ejemplo, porque el UE no tiene una tarjeta SIM y/o no tiene una suscripción a una red doméstica o celular). La credencial preexistente puede no ser una credencial específica de la red celular. De hecho, puede estar asociado con un proveedor de servicios de aplicaciones que no opera una red celular (por ejemplo, un proveedor de contenido). La red de servicio puede reenviar la petición de conexión al servidor de la entidad patrocinadora. La petición de conexión puede incluir un identificador de la red de servicio. En un modo de realización, el servidor de la entidad patrocinadora está en una red externa a la red central de la red de servicio (por ejemplo, como se accede a través de una pasarela PDN como se describe más adelante). El servidor puede generar una nueva clave secreta compartida entre el UE y el servidor a través de un handshake o establecimiento de comunicación de múltiples vías, o de forma alternativa puede usar una forma de hash de la contraseña del usuario. Como ejemplo, una credencial preexistente puede ser una versión con hash de una contraseña preexistente establecida entre el UE y el servidor. El uso de una nueva clave secreta compartida permite la generación de uno o más elementos de un vector de autentificación.

[0021] Un servidor puede a continuación enviar el vector de autentificación a la red de servicio para continuar facilitando el acceso a la red. Uno o más elementos de red pueden extraer y almacenar aspectos del vector de autentificación (por ejemplo, una respuesta esperada del UE y K_{ASME}) y luego enviarlos al resto (por ejemplo, incluyendo un número aleatorio y un token de autentificación) al UE como parte de una petición de autentificación. El UE utiliza la clave secreta compartida o, de forma alternativa, la misma credencial preexistente, como una forma de hash de la contraseña del usuario, para generar una respuesta a la petición de autentificación. Estos datos se pueden enviar de nuevo a la red de servicio para su verificación. Si la respuesta del UE coincide con una respuesta esperada designada por el servidor, el procedimiento de conexión continúa. Cuando continúa, el UE puede utilizar la red de servicio para acceder al servicio en virtud de la conexión patrocinada, incluso cuando el UE no tiene una identidad de abonado y/o suscripción con un proveedor de servicios.

[0022] En un modo de realización alternativo, un UE puede usar otro procedimiento de autentificación para aprovecharse de la conectividad patrocinada. El UE puede intentar conectarse a una red de servicio, pero no incluir un token de cliente que se basa en una credencial preexistente con la petición de conexión. Por ejemplo, después de que la red de servicio envía una petición de autentificación al servidor, el servidor se comunica con el UE a través de la red de servicio para autentificar al UE y recibir la autorización para que el servidor otorgue uno o más elementos de la red de servicio para acceder a un perfil de usuario asociado con el usuario del UE para completar la autentificación y la conexión. Si el UE se autentifica con éxito con el servidor (por ejemplo, mediante una credencial preexistente o alguna de sus derivadas), el servidor interactuará con una entidad de red en la red de servicio para proporcionar un código de autorización al elemento de red (en lugar de al UE y luego al elemento de red). El código de autorización permite al elemento de red obtener un token de acceso que luego puede ser utilizado por el elemento de red para acceder al perfil de usuario asociado con el UE para completar la autentificación y conectar el UE a la red de servicio según los términos del patrocinio.

[0023] Volviendo ahora a las figuras, la FIG. 1 ilustra una red de comunicación inalámbrica 100 de acuerdo con diversos aspectos de la presente divulgación. La red de comunicación inalámbrica 100 puede incluir varios UE 102, así como varias redes de acceso por radio (RAN) 104 (donde cada una puede incluir cualquier número de estaciones base). Un único UE 102 y un solo RAN 104 se han ilustrado en la FIG. 1 por simplicidad de ilustración y explicación. Una estación base dada en una RAN 104 puede incluir un Nodo B evolucionado (eNodoB). Una estación base también puede denominarse una estación transceptora base o un punto de acceso. Aunque los modos de realización se analizan en el presente documento en general, a veces con referencia a las redes LTE/4G, esto se hace con fines a modo de ejemplo. Los modos de realización de la presente divulgación también son aplicables y operables con una serie de otras redes.

[0024] La RAN 104 se comunica con el UE 102 como se muestra. Un UE 102 puede comunicarse con la RAN 104 a través de un enlace ascendente y un enlace descendente. El enlace descendente (o enlace directo) se refiere al enlace de comunicación desde una estación base en la RAN 104 al UE 102. El enlace ascendente (o enlace inverso) se refiere al enlace de comunicación desde el UE 102 a la estación base en la RAN 104.

[0025] Los UE 102 pueden dispersarse por toda la red inalámbrica 100, y cada UE 102 puede ser fijo o móvil. El UE 102 también se puede denominar terminal, estación móvil, unidad de abonado, etc. El UE 102 puede ser un teléfono celular, un teléfono inteligente, un asistente digital personal, un módem inalámbrico, un ordenador portátil, una tablet, un dispositivo de entretenimiento, un dispositivo de comunicación portátil, un componente vehicular, un dispositivo informático móvil, un dispositivo de supervisión de salud, un dispositivo médico, dispositivos de Internet de las cosas/todo, dispositivos M2M/D2D, etc. La red de comunicación inalámbrica 100 es un ejemplo de una red para la cual se aplican varios aspectos de la divulgación.

[0026] También se ilustra en la FIG. 1 una entidad de gestión de la movilidad (MME) 106. La MME 106 puede estar a cargo de las funciones del plano de control relacionadas con los abonados (por ejemplo, el UE 102) y la administración de la sesión. Por ejemplo, la MME 106 puede proporcionar administración de sesiones de movilidad, así como soporte para transferencias a otras redes, itinerancia y autentificación de abonados. La MME 106 puede facilitar la selección de una pasarela de servicio (S-GW) 108 durante una conexión inicial del UE 102, señalización de no acceso al estrato (NAS), seguridad de señalización de NAS, selección de la pasarela de la red de datos de paquete (P-GW) 110, funciones de gestión de portadores, incluido el establecimiento de portadores dedicados, interceptación legal del tráfico de señalización y otras funciones por nombrar solo algunos ejemplos. La RAN 104, MME 106, S-GW 108 y P-GW 110 pueden estar en la misma red de servicio 112 (por ejemplo, parte de un núcleo de paquete evolucionado (EPC)). Como se reconocerá, la red de servicio 112 incluye otros elementos de red que no se muestran en la FIG. 1 para simplificar el análisis de aspectos de la presente divulgación.

[0027] La MME 106 se comunica con la S-GW 108 en la red de servicio 112. La S-GW 108 puede ser la pasarela que termina la interfaz hacia la RAN 104, facilita el traspaso de estaciones entre bases, proporciona un anclaje de movilidad para movilidad entre diferentes estándares (por ejemplo, 2G, 3G, 4G, LTE, 5G y futuras redes, etc.), intercepción legal, enrutamiento y reenvío basado en paquetes, y contabilización de cobro entre operadores, por nombrar solo algunos ejemplos. La S-GW 108 enruta y reenvía paquetes de datos desde el UE 102, por ejemplo, al P-GW 110. La FIG. 1 ilustra un solo P-GW 110 por simplicidad, aunque se reconocerá que existen múltiples redes externas (a la red de servicio 112) a las que se pueden dirigir los datos, donde la red 114 es solo un ejemplo. El P-GW 110 proporciona conectividad entre la red de servicio 112 y las redes externas de paquetes de datos como el punto de salida y entrada para el tráfico de datos desde/hacia el UE 102. El P-GW 110 puede estar involucrado en el filtrado de paquetes por usuario, la interceptación legal, el control de nivel de servicio, la aplicación de la tasa de nivel de servicio y la selección de paquetes por mencionar solo algunos ejemplos.

[0028] Como se ilustra en la FIG. 1, el P-GW 110 proporciona un punto de entrada/salida para paquetes de datos que se desplazan a través de la red 114 entre el UE 102 y el servidor 116. El servidor 116 puede ser operado por una entidad que proporciona patrocinio. En un modo de realización, el patrocinio puede incluir a un usuario que paga a un proveedor de servicios de aplicaciones por uno o más servicios (por ejemplo, transmisión de contenido, navegación en línea, compras en línea, etc.). En respuesta, el proveedor de servicios de aplicaciones habilita la conectividad patrocinada a través de una red al UE del usuario, como una red celular (de servicio), basada en un contrato con el usuario. En otro modo de realización, una conexión patrocinada puede estar disponible de forma gratuita para el UE de un usuario basándose en un intento por parte del proveedor de servicios de aplicaciones para aumentar su base de usuarios (por ejemplo, el proveedor de servicios de aplicaciones paga a la red celular por el servicio). De forma alternativa, la tarifa por la conectividad patrocinada se puede cobrar a partir de una tarifa cobrada por otras fuentes, como los ingresos por publicidad, en lugar del usuario.

[0029] El servidor 116 puede denominarse en el presente documento un proveedor de servicios de aplicaciones o servidor de proveedor de servicios de aplicaciones. En un modo de realización, el servidor 116 puede alojar uno o más servicios. Aunque se ilustra como un servidor, se reconocerá que el servidor 116 puede ser un sistema independiente o múltiples sistemas que operan en cooperación (por ejemplo, para proporcionar uno o más servicios). Los servicios pueden ser cualquier servicio en particular entre muchos, por ejemplo, un mercado en línea, una red de medios sociales, un proveedor de búsqueda, acceso general a Internet/red, un proveedor de contenido, comunicaciones de acceso a Internet, etc. (ya sea alojado en otro lugar o por el servidor 116 del proveedor de servicios de aplicaciones).

[0030] Los servicios patrocinados puede ser determinado por el proveedor de servicios de aplicaciones alojado en el servidor 116. Por ejemplo, esto puede ocurrir en el momento de la provisión de un acuerdo entre la red de servicio 112 y el proveedor de servicios de aplicaciones. En otro escenario, el servicio que se patrocina puede ser determinado por el servidor 116 en el momento de conexión la petición de una lista de servicios (aprovisionados) previamente acordados entre la red de servicio 112 y el proveedor de servicios de aplicaciones. Esto puede basarse en un servicio solicitado específicamente desde el UE 102 o la red de servicio 112, o en un servicio identificado por el servidor 116.

[0031] Un usuario del UE 102 puede haber establecido previamente una relación con el proveedor de servicios de aplicaciones, por ejemplo mediante el registro de una cuenta de usuario con un nombre de usuario y una contraseña mantenida por el servidor 116. De acuerdo con los modos de realización de la presente divulgación, el servidor 116 del proveedor de servicios de aplicaciones también replica varios aspectos de un servidor de abonado doméstico (HSS), incluidos aquellos aspectos que pueden ser necesarios o útiles para los procedimientos de conexión de UE con la red de servicio 112. Esto puede incluir un nombre de usuario y contraseña (y cualquier hash/etc. del mismo) del usuario asociado con el UE 102 y las funciones de autentificación (incluida la administración de la generación de información de seguridad a partir de las claves de identidad del usuario y el suministro de la información de seguridad a las entidades de red), por nombrar algunos ejemplos.

[0032] Como se describirá en más detalle a continuación con respecto a las figuras posteriores, incluyendo diagramas de protocolo que ilustran aspectos de señalización entre un UE, la red de servicio, y el servidor de un proveedor de servicios de aplicaciones, el UE 102 puede comunicarse con la red de servicio 112 y el servidor 116 utilizando un token de cliente. El token del cliente puede basarse en (por ejemplo, obtenerse a partir de) una credencial preexistente (por ejemplo, alguna variante de una contraseña, clave de alta entropía, etc.) previamente establecida entre el usuario del UE 102 (o el propio UE 102) y el proveedor de servicios de aplicaciones. El token de cliente/credencial preexistente se puede usar de acuerdo con los modos de realización de la presente divulgación para obtener conectividad patrocinada a través de la red de servicio 112. Al usar una credencial preexistente, los UE que no tienen tarjetas SIM y/o no tienen suscripciones todavía pueden obtener conectividad patrocinada a través de un proveedor de servicios de aplicaciones asociado con la credencial preexistente, así como los UE que pueden tener suscripciones (por ejemplo, para que se cubra su uso de datos u otro tipo de servicio cubierto basándose en el patrocinio particular del proveedor de servicios de aplicaciones).

[0033] En un modo de realización, la conectividad patrocinada puede referirse a una variedad de diferentes aspectos. Por ejemplo, la conectividad patrocinada puede referirse al acceso total a la red de servicio 112 (por ejemplo, con el propósito de acceder/usar un servicio de aplicaciones provisto por el servidor 116 o un servicio de un proveedor diferente bajo el patrocinio). Otros escenarios incluyen acceso total o parcial al servicio por un tiempo predeterminado (y/o número de veces), acceso total o parcial a la red en general por un período específico de tiempo/cantidad de datos/ancho de banda de datos, acceso total o parcial al servicio y/o a la red en general para una cantidad predeterminada de datos (por ejemplo, como se rastrea en bytes o algún otro tamaño/métrica), por nombrar algunos ejemplos.

[0034] En un ejemplo, el UE 102 puede enviar, como parte de su petición de conexión inicial a la RAN 104, un token de cliente basado en una credencial preexistentes en lugar de otros identificadores tradicionales. Un ejemplo de un identificador tradicional es una identidad de abonado móvil internacional (IMSI). Esto se debe a que los modos de realización de la presente divulgación permiten el uso de una credencial preexistente en lugar de algún tipo de identificador de abonado, de modo que los UE que no tienen una tarjeta SIM o una suscripción a una red doméstica todavía pueden utilizar la conectividad patrocinada de una manera que da como resultado una mayor eficiencia y seguridad en la red de servicio 112 (por ejemplo, al no permitir ningún tráfico de IP en la red de servicio 112 que se filtra por primera vez en el P-GW 110). La petición de conexión también puede identificar el proveedor de servicios de aplicaciones con el que el UE 102 desea comunicarse (es decir, el proveedor de servicios de aplicaciones con el que el usuario tiene una credencial preexistente (contraseña/nombre de usuario con función hash, clave de alta entropía, etc.)). La RAN 104 reenvía la petición de conexión con el token de cliente del UE y la identificación del servicio a la MME 106. La MME 106 incluye un identificador de red de servicio con la información en la petición de conexión y la reenvía como una petición de información de autentificación a S-GW 108 y luego a P-GW 110. El servidor 116 es capaz de identificar el UE 102 basándose en el token de acceso proporcionado en la petición de información de autentificación de la red de servicio 112 (por ejemplo, activado por una petición de conexión desde el UE 102). El uso de una credencial existente para obtener conectividad patrocinada puede aumentar la cantidad de UE que se conectan al servicio patrocinado por el proveedor de servicios de aplicaciones (u otro servicio de otro proveedor patrocinado por el servidor 116 del proveedor de servicios de aplicaciones).

[0035] La FIG. 2 es un diagrama de bloques de un UE 102 a modo de ejemplo de acuerdo con un modo de realización de la presente divulgación. El UE 102 puede tener cualquiera de las muchas configuraciones descritas en el presente documento. El UE 102 puede incluir un procesador 202, una memoria 204, un módulo de acceso 208, un transceptor 210 y una antena 216. Estos elementos pueden estar en comunicación directa o indirecta entre sí, por ejemplo, a través de uno o más buses.

[0036] El procesador 202 puede tener varias características como un procesador de un tipo específico. Por ejemplo, pueden incluirse una unidad central de procesamiento (CPU), un procesador de señal digital (DSP), un circuito integrado específico de la aplicación (ASIC), un controlador, un dispositivo de matriz de puertas programables en campo (FPGA), otro dispositivo de hardware, un dispositivo de firmware, o cualquier combinación de los mismos configurada para realizar las operaciones descritas en el presente documento con referencia al UE 102 introducido anteriormente con respecto a la FIG. 1 y analizado en más detalle a continuación. El procesador 202 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.

[0037] La memoria 204 también puede tener varias características. Por ejemplo, pueden incluirse una memoria caché (por ejemplo, una memoria caché del procesador 442), memoria de acceso aleatorio (RAM), RAM magnetoresistiva (MRAM), memoria de solo lectura (ROM), memoria de solo lectura programable (PROM), memoria de solo lectura programable y borrable (EPROM), memoria de solo lectura programable y borrable eléctricamente (EEPROM), memoria flash, dispositivo de memoria de estado sólido, unidades de disco duro, matrices basadas en memristores, otras formas de memoria volátil y no volátil, o una combinación de diferentes tipos de memoria. En algunos modos de realización, la memoria 204 puede incluir un medio legible por ordenador no transitorio.

[0038] La memoria 204 puede almacenar instrucciones 206. Las instrucciones 206 pueden incluir instrucciones que, cuando son ejecutadas por el procesador 202, hacen que el procesador 202 realice las operaciones descritas en el presente documento con referencia al UE 102 en relación con los modos de realización de la presente divulgación. Las instrucciones 206 también pueden denominarse código. Los términos "instrucciones" y "código" deberían interpretarse en sentido amplio para incluir cualquier tipo de sentencia(s) legible(s) por ordenador. Por ejemplo, los términos "instrucciones" y "código" pueden referirse a uno o más programas, rutinas, subrutinas, funciones, firmware, middleware, microcódigo, procedimientos, etc. "Instrucciones" y "código" pueden comprender una única secuencia legible por ordenador o muchas secuencias legibles por ordenador.

[0039] El módulo de acceso 208 puede ser utilizado para diversos aspectos de la presente divulgación. Por ejemplo, el módulo de acceso 208 puede controlar el almacenamiento y la recuperación de una o más credenciales preexistentes (y/o sus derivadas) mantenidas por el UE 102. El módulo de acceso 208 puede recibir una contraseña, una combinación de nombre de usuario/contraseña, clave de alta entropía, token o certificado de identidad (por nombrar algunos ejemplos) de una fuente de entrada, por ejemplo, bajo la dirección de un usuario del UE 102, y dirigir la credencial (como el nombre de usuario y la contraseña) a una ubicación de almacenamiento. En un modo de realización, el UE 102 puede recibir la credencial preexistente del proveedor de servicios de aplicaciones como una versión con hash ya generado de la contraseña establecida por el usuario con el proveedor de servicios de aplicaciones. Además, el módulo de acceso 208 puede determinar un token de cliente que se utilizará en una petición de conexión de una credencial preexistente. El token del cliente se puede determinar a partir de una credencial de contraseña. Por ejemplo, el token del cliente se puede determinar mediante la generación de hash de la contraseña con una o más adiciones, como un salt, un valor para la ocasión y/u otros valores, como se analizará más detalladamente a continuación con respecto a las figuras posteriores.

[0040] El módulo de acceso 208 también puede usarse durante el procedimiento de conexión. Por ejemplo, cuando el UE 102 intenta conectarse a una red de servicio 112 mediante una conexión patrocinada, el módulo de acceso 208 puede recuperar (u obtener/determinar dinámicamente en el momento solicitado) el token del cliente basado en la credencial preexistente para incluir en la petición de conexión. Más adelante, cuando el UE 102 recibe un token de autentificación durante la autentificación mutua con la red de servicio 112, el módulo de acceso 208 puede ayudar a determinar y crear la respuesta de autentificación al token de autentificación, por ejemplo, accediendo (o determinando) una o más claves mantenidas (o determinado) por el módulo de acceso 208 para este propósito.

[0041] El transceptor 210 puede incluir un subsistema de módem 212 y una unidad de frecuencia de radio (RF) 214. El transceptor 210 puede ser una interfaz de comunicaciones para el UE 102 o ser un componente de una interfaz de comunicaciones para el UE 102. El transceptor 210 está configurado para comunicarse bidireccionalmente con otros dispositivos, como las estaciones base en la RAN 104. El subsistema de módem 212 puede configurarse para modular y/o codificar los datos del módulo de acceso 208 y/o la memoria 204 de acuerdo con un esquema de modulación y codificación (MCS), por ejemplo, un esquema de codificación de comprobación de paridad de baja densidad (LDPC), un esquema de codificación turbo, un esquema de codificación convolucional, etc. La unidad RF 214 puede configurarse para procesar (por ejemplo, realizar una conversión analógica a digital o conversión digital a analógica, etc.) datos modulados/codificados del subsistema de módem 212 (en las transmisiones de salida) o de transmisiones que se originan de otra fuente, como una estación base en la RAN 104. Aunque se muestra como integrado en el transceptor 210, el subsistema de módem 212 y la unidad de RF 214 pueden ser dispositivos separados que se acoplan entre sí en el UE 102 para permitir que el UE 102 se comunique con otros dispositivos.

[0042] La unidad de RF 214 puede proporcionar los datos modulados y/o procesados, por ejemplo paquetes de datos (o, más en general, mensajes de datos que pueden contener uno o más paquetes de datos y otra información, incluyendo los valores PMSI), a la antena 216 para transmisión a uno o más dispositivos. Esto puede incluir, por ejemplo, la transmisión de mensajes de datos a la RAN 104 de acuerdo con modos de realización de la presente

divulgación. La antena 216 puede recibir además mensajes de datos transmitidos desde la RAN 104 y proporcionar los mensajes de datos recibidos para su procesamiento y/o desmodulación en el transceptor 210. Aunque la FIG. 2 ilustra la antena 216 como una sola antena, la antena 216 puede incluir múltiples antenas de diseños similares o diferentes para mantener múltiples enlaces de transmisión.

[0043] La FIG. 3 es un diagrama de bloques de un servidor a modo de ejemplo 116 de acuerdo con modos de realización de la presente divulgación. El servidor 116 puede incluir un procesador 302, una memoria 304, un módulo de acceso 308, un servicio 310, una base de datos 312 y un transceptor 314. Estos elementos pueden estar en comunicación directa o indirecta entre sí, por ejemplo, a través de uno o más buses. Como se mencionó anteriormente con respecto a la FIG. 1, el servidor 116 puede alojar uno o más servicios, mantener una base de datos de credenciales de usuario (nombre de usuario/contraseña, token, certificado y/o credenciales preexistentes obtenidas a partir de credenciales de contraseña y/o tokens de clientes obtenidos a partir de credenciales preexistentes) y también replicar varios aspectos de un HSS.

[0044] El procesador 302 puede tener varias características como un procesador de un tipo específico. Por ejemplo, estos pueden incluir una CPU, un DSP, un ASIC, un controlador, un dispositivo FPGA, otro dispositivo de hardware, un dispositivo de firmware o cualquier combinación de los mismos configurados para realizar las operaciones descritas en el presente documento con referencia al servidor 116 introducido en la FIG. 1 anterior. El procesador 302 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.

[0045] La memoria 304 puede incluir una memoria caché (por ejemplo, una memoria caché del procesador 302), RAM, MRAM, ROM, PROM, EPROM, EEPROM, memoria flash, un dispositivo de memoria de estado sólido, una o más unidades de disco duro, matrices basadas en memristores, otras formas de memoria volátil y no volátil, o una combinación de diferentes tipos de memoria. En algunos modos de realización, la memoria 304 puede incluir un medio no transitorio legible por ordenador. La memoria 304 puede almacenar instrucciones 306. Las instrucciones 306 pueden incluir instrucciones que, cuando son ejecutadas por el procesador 302, hacen que el procesador 302 realice las operaciones descritas en el presente documento con referencia al servidor 116 en relación con modos de realización de la presente divulgación. Las instrucciones 306 también pueden denominarse código, que puede interpretarse de manera amplia para incluir cualquier tipo de declaración(ones) legible(s) por ordenador como se analizó anteriormente con respecto a la FIG. 2.

[0046] El módulo de acceso 308 puede ser utilizado para diversos aspectos de la presente divulgación. Por ejemplo, el módulo de acceso 308 puede estar involucrado en el aprovisionamiento inicial de la red de servicios para establecer la conectividad patrocinada de uno o más servicios identificados a través de una o más redes de servicio 112. Además, el módulo de acceso 308 puede recuperar una o más credenciales almacenadas (preexistentes) asociadas con el UE 102 y/o el usuario del UE 102 en cooperación con el servicio 310 específico de la aplicación. Por ejemplo, el módulo de acceso 308 puede recuperar la credencial preexistente de la base de datos 312 después de que el servicio 310 la almacenó allí.

[0047] El módulo de acceso 308 puede, además, estar involucrado en el procedimiento de conexión inicial con el UE 102. El servidor 116 puede recibir el token del cliente basándose en una credencial preexistente proporcionada con la petición de conexión inicial del UE 102 y comparar la credencial preexistente correspondiente (y el nombre de usuario, en modos de realización donde eso se incluye en la petición de conexión) con la información de usuario almacenada en la base de datos 312. En respuesta a la petición de conexión del UE 102, el servidor 116 del proveedor de servicios de aplicaciones puede generar o acceder a una o más claves y una respuesta esperada basada en la credencial preexistente y transmitirlas al UE 102 como parte de una respuesta de petición de autentificación (por ejemplo, un vector de autentificación) a la petición de conexión inicial.

[0048] El servicio 310 puede ser cualquier servicio en particular de entre muchos, por ejemplo, un mercado en línea, una red social, un proveedor de búsqueda, un proveedor de servicios, etc. En un modo de realización, el proveedor de servicios de aplicaciones representado por el servidor 116 patrocina la conectividad al servicio 310. En un modo de realización alternativo, el servicio 310 es representativo de uno o más servicios ofrecidos por entidades diferentes del proveedor de servicios de aplicaciones, pero para el cual el proveedor de servicios de aplicaciones (representado por el servidor 116) proporciona patrocinio a través de la red de servicio 112 para el acceso del UE 102.

[0049] El proveedor de servicios de aplicaciones que opera el servidor 116 puede interactuar con el usuario del UE 102 a través de un canal fuera de banda para establecer derechos de acceso al servicio específico de la aplicación, por ejemplo a través del UE 102 o algún otro dispositivo habilitado para comunicaciones. Esto puede incluir el registro con el proveedor de servicios de aplicaciones, el establecimiento de las preferencias del usuario, el pago de una tarifa de acceso o uso (cuando corresponda), por ejemplo. El establecimiento del nombre de usuario y la contraseña con el proveedor de servicios de aplicaciones (como se representa aquí mediante el servidor 116) a través del canal fuera de banda puede ocurrir en algún momento antes de la petición de conexión de conectividad patrocinada y puede ocurrir, por ejemplo, a través de WLAN, LAN, Wi-Fi, igual a igual, malla o alguna otra red además de una red celular como la red de servicio 112 de la FIG. 1. El proveedor de servicios de aplicaciones puede, por ejemplo, mediante el

módulo de acceso 308, determinar la(s) credencial(es) preexistente(s) que el UE 102 puede usar más adelante como base para obtener conectividad patrocinada, por ejemplo, generando hash de la contraseña con una o más adiciones, como un salt, un valor para la ocasión, y/u otros valores.

[0050] La base de datos 312 puede incluir una o más bases de datos mantenidas por el servidor 116, por ejemplo una base de datos que mantiene los nombres de usuario y las correspondientes credenciales preexistentes (o contraseñas en modos de realización alternativos) en nombre del proveedor de servicios de aplicaciones y el módulo de acceso 308 específicamente. La base de datos 312 puede rastrear la información de acceso patrocinado, como la identificación y el direccionamiento del usuario (incluido, por ejemplo, uno o más números de teléfono móvil de todos o un subconjunto de UE que obtienen o solicitan conectividad patrocinada a través del proveedor de servicios de aplicaciones), información del perfil, así como la información de seguridad asociada con cada UE que tiene, o está asociada con un usuario que tiene credenciales preexistentes (por ejemplo, credenciales preexistentes, contraseña, certificado de identidad, clave de alta entropía y/o una o más claves de seguridad).

[0051] El transceptor 314 permite al servidor 116 comunicarse para transmitir y recibir datos de fuentes externas, tales como la red de servicio 108. El transceptor 314 puede habilitar comunicaciones inalámbricas y/o por cable. El transceptor 314 puede incluir, por ejemplo, una conexión Ethernet, una conexión WiFi u otros tipos de subsistemas de módem y/o RF como se reconocerá. El transceptor 314 puede ser una interfaz de comunicaciones para el servidor 116 o un componente de una interfaz de comunicaciones para el servidor 116.

[0052] La FIG. 4 es un diagrama de bloques que ilustra un sistema transmisor a modo de ejemplo 410 (por ejemplo, una estación base en RAN 104) y un sistema receptor 450 (por ejemplo, un UE 102) en un sistema MIMO 400, de acuerdo con ciertos aspectos de la presente divulgación. En el sistema transmisor 410, se proporcionan datos de tráfico para varios flujos de datos desde una fuente de datos 412 hasta un procesador de datos de transmisión (TX) 414. Los datos de tráfico pueden incluir todo tipo de tráfico, incluidas las peticiones de autentificación de una o más entidades MME de acuerdo con los aspectos de la presente divulgación.

[0053] En una transmisión de enlace descendente, por ejemplo, cada flujo de datos se transmite a través de una respectiva antena de transmisión. El procesador de datos de TX 414 da formato, codifica y entrelaza los datos de tráfico para cada flujo de datos basándose en un esquema de codificación particular seleccionado para que ese flujo de datos proporcione datos codificados.

[0054] Los datos codificados para cada flujo de datos pueden multiplexarse con datos piloto usando técnicas OFDM. Los datos piloto, por ejemplo una secuencia piloto, son típicamente un patrón de datos conocido que se procesa de una manera conocida y que puede usarse en el sistema receptor para estimar la respuesta de canal u otros parámetros de canal. Los datos piloto pueden formatearse convirtiéndose en símbolos piloto. El número de símbolos piloto y la ubicación de los símbolos piloto dentro de un símbolo OFDM pueden determinarse mediante instrucciones realizadas por el procesador 430.

[0055] A continuación, los datos piloto multiplexados y codificados para cada flujo de datos se modulan (es decir, se les asignan símbolos) basándose en un esquema de modulación particular (por ejemplo, BPSK, QPSK, M-PSK o M-QAM) seleccionado para ese flujo de datos para proporcionar símbolos de modulación. La velocidad de transferencia de datos, la codificación y la modulación para cada flujo de datos pueden determinarse mediante instrucciones realizadas por el procesador 430. El número de símbolos piloto y la ubicación de los símbolos piloto en cada trama también pueden determinarse mediante instrucciones realizadas por el procesador 430, por ejemplo, como se describió anteriormente con respecto a las FIGs. 2 o 3. El sistema transmisor 410 incluye además una memoria 432, por ejemplo como se describe anteriormente con respecto a las FIGs. 2 o 3 también.

[0056] Los símbolos de modulación para todos los flujos de datos se proporcionan a continuación a un procesador TX MIMO 420, que puede procesar adicionalmente los símbolos de modulación (por ejemplo, para OFDM). A continuación, el procesador MIMO TX 420 proporciona N_T flujos de símbolos de modulación a los N_T transmisores (TMTR) 422_a a 422_t. En determinados modos de realización, el procesador TX MIMO 420 aplica ponderaciones de formación de haces a los símbolos de los flujos de datos y a la antena desde la cual se está transmitiendo el símbolo. El sistema transmisor 410 incluye modos de realización que tienen solo una antena o que tienen múltiples antenas.

[0057] Cada transmisor 422 recibe y procesa un flujo de símbolos respectivo para proporcionar una o más señales analógicas y acondiciona adicionalmente las señales analógicas (por ejemplo, las amplifica, filtra y eleva su frecuencia) para proporcionar una señal modulada adecuada para la transmisión a través del canal MIMO. A continuación, N_T señales moduladas desde los transmisores 422*a* a 422*t* se transmiten desde N_T antenas 424_a a 424_t, respectivamente. Las técnicas descritas en el presente documento se aplican también a los sistemas con una sola antena de transmisión. La transmisión con una antena es más simple que el escenario de múltiples antenas. Por ejemplo, es posible que no haya necesidad de un procesador MIMO TX 420 en un solo escenario de antena.

[0058] En el sistema receptor 450, las señales moduladas transmitidas son recibidas mediante las N_R antenas 452_a a 452_r y la señal recibida desde cada antena 452 se proporciona a un transceptor respectivo (RCVR) 454_a a 454_r. Cada receptor 454 acondiciona una respectiva señal recibida (por ejemplo, la filtra, amplifica y reduce su frecuencia),

digitaliza la señal acondicionada para proporcionar muestras y procesa además las muestras para proporcionar un flujo de símbolos "recibido" correspondiente. Las técnicas descritas en el presente documento también se aplican a modos de realización del sistema receptor 450 que tienen solo una antena 452.

[0059] A continuación, un procesador de datos RX 460 recibe y procesa los N_R flujos de símbolos recibidos desde los receptores 454_a a 454_r basándose en una técnica de procesamiento de receptor particular a fin de proporcionar N_T flujos de símbolos detectados. A continuación, el procesador de datos de RX 460 desmodula, desintercala y descodifica según sea necesario cada flujo de símbolos detectado para recuperar los datos de tráfico para el flujo de datos. El tráfico recuperado puede incluir, por ejemplo, información en una petición de información de autentificación de una MME de acuerdo con aspectos de la presente divulgación. El procesamiento realizado por el procesador de datos RX 460 puede ser complementario al realizado por el procesador TX MIMO 420 y el procesador de datos TX 414 en el sistema transmisor 410.

[0060] La información proporcionada por el procesador de datos RX 460 permite que el procesador 470 genere informes tales como información de estado de canal (CSI) y otra información para proporcionar al procesador de datos de TX 438. El procesador 470 formula un mensaje de enlace inverso que comprende la petición de CSI y/o piloto para transmitir al sistema transmisor.

[0061] El procesador 470 puede ser implementado, por ejemplo, como se describe anteriormente con respecto a los procesadores descritos en las FIGs. 2 o 3. Además de los mensajes de enlace inverso, el sistema receptor 450 puede transmitir otros diversos tipos de información, incluidas las peticiones de conexión que incluyen tokens de clientes basadas en credenciales preexistentes para la conectividad patrocinada a la red de servicio 112, respuestas para la autentificación mutua y otra información para establecer una sesión de comunicación patrocinada, así como datos durante la sesión de comunicación. El mensaje puede ser procesado por un procesador de datos de TX 438, modulado por un procesador TX MIMO 480, acondicionado por los transmisores 454_a a 454_r y transmitido de nuevo al sistema transmisor 410. Como se muestra, el procesador de datos de TX 438 también puede recibir datos de tráfico para una serie de flujos de datos desde una fuente de datos 436.

[0062] En el sistema transmisor 410, las señales moduladas del sistema receptor 450 se reciben mediante las antenas 424, se acondicionan mediante los receptores 422, se desmodulan mediante un desmodulador 440 y se procesan mediante un procesador de datos RX 442 para extraer el mensaje de enlace inverso transmitido por el sistema receptor 450. Como resultado, los datos pueden enviarse y recibirse entre el sistema transmisor 410 y el sistema receptor 450. El sistema transmisor 410 también se puede usar para transmitir la información que recibe del sistema receptor 450 a otros elementos de red dentro de su red de servicio y recibir información de uno o más elementos de red adicionales en la red de servicio, como se reconocerá. El modo de realización ilustrado en la FIG. 4 es solo un ejemplo, y los modos de realización de la presente divulgación son aplicables a otros sistemas transmisores/receptores no ilustrados en la FIG. 4.

[0063] La FIG. 5 es un diagrama de protocolo que ilustra algunos aspectos de señalización entre un UE, una red de servicio y un proveedor de servicios de aplicaciones para proporcionar conectividad patrocinada de acuerdo con diversos aspectos de la presente divulgación. Para simplificar el análisis, se hará referencia a los elementos mostrados en la FIG. 1 (por ejemplo, UE 102, RAN 104 (que se muestra como eNB 104 en la FIG. 5), MME 106, GW 110 y el servidor 116 como el proveedor de servicios de aplicaciones que aloja el servicio específico de la aplicación) al describir las acciones en el diagrama de protocolo de la FIG. 5. Además, para simplificar, el análisis se centrará en aquellos aspectos del flujo del protocolo que describen aspectos de los modos de realización de la presente divulgación en lugar de todos los aspectos de un procedimiento de conexión. El enfoque ilustrado en la FIG. 5 describe un modo de realización en la que el token de cliente se basa en una credencial preexistente (basada en una contraseña) compartida entre el UE 102 y el servidor 116.

[0064] En la acción 502, el UE 102 lleva a cabo un procedimiento de descubrimiento de servicio con la red de servicio 112. El descubrimiento de servicio puede habilitarse mediante una función de provisión de servicios que el servidor 116 realizó anteriormente con la red de servicio 112. En un modo de realización, un resultado de la función de provisión de servicios incluye la red de servicio 112 que radiodifunde a algunos o todos los destinatarios (por ejemplo, los UE 102) información que identifica la conectividad patrocinada por el proveedor de servicios de aplicaciones alojado por el servidor 116. En otro modo de realización, el UE 102 puede haber recibido información del servidor 116 que identifica algunas o todas las redes de confianza, o redes que han entrado en acuerdos para proporcionar la conectividad patrocinada en nombre del proveedor de servicios de aplicaciones alojado por el servidor 116.

[0065] Después de que el UE 102 ha descubierto la red de servicio 112, en la acción 504, el UE 102 envía una petición de autentificación al eNB 104. Esto se hace en un intento de conectarse a la red de servicio 112. Al recibir la petición de autentificación, el eNB 104 reenvía la petición de autentificación a la MME 106. La petición de autentificación incluye un token de cliente que se basa en una credencial preexistente que se estableció previamente entre el UE 102 (o el usuario del UE 102 y se proporcionó al UE 102) y el proveedor de servicios de aplicaciones alojado por el servidor 116. La petición de autentificación no incluye un identificador de abonado (por ejemplo, IMSI, etc.). En un modo de realización, la petición de autentificación no incluye una credencial asociada con una red celular existente. La petición de autentificación también puede incluir un nombre de usuario asociado con la credencial preexistente como se

estableció previamente con el proveedor de servicios de aplicaciones. Para ayudar a la red de servicio 112 a enrutar la petición de autentificación correctamente, el UE 102 también puede incluir información para identificar el servidor 116, como el nombre de dominio del proveedor de servicios de aplicaciones en el servidor 116 o un ID de la aplicación.

[0066] El token de cliente puede asumir una variedad de formas y tienen una serie de características diferentes. Por ejemplo, se puede generar una credencial preexistente colocando primero la contraseña establecida entre el UE 102 y el proveedor de servicios de aplicaciones (por ejemplo, a través de un canal fuera de banda como una conexión WLAN) con un salt concatenado con un nombre del proveedor de servicios de aplicaciones en un código de autentificación de mensaje de función hash (HMAC). La salida de la función HMAC puede designarse como la "credencial preexistente" para los fines de este análisis. El valor resultante de la "credencial preexistente" puede introducirse en otra función HMAC donde la entrada adicional es un valor para la ocasión, siendo la salida el token del cliente. El token del cliente permite al proveedor de servicios de aplicaciones verificar la posesión de una credencial preexistente válida. Se puede usar un token de cliente en lugar de la credencial (o contraseña) preexistente para que ningún atacante malintencionado pueda interceptar la información e intentar enmascararse como un usuario asociado con el UE 102 de manera no autorizada. Aunque el token del cliente se describe aquí como el valor que se incluye con la petición de autentificación, se reconocerá que la credencial preexistente puede incluirse en su lugar, aunque puede exponer al usuario a riesgos de seguridad adicionales de lo que sería el caso con token de cliente. La generación de estos valores se ilustra en las ecuaciones 1 y 2:

credencial preexistente = HMAC (contraseña, salt | nombre del servicio), donde | es el operador de concatenación; **(Ec. 1)**

token de cliente = HMAC (credencial preexistente, para la ocasión). **(Ec. 2)**

[0067] El token de cliente, a su vez, está incluido en un vector de cliente para su inclusión en la petición de conexión, por ejemplo, vector de cliente = [nombre de usuario, para la ocasión, token de cliente]. Como otro ejemplo, en un modo de realización, el UE 102 puede usar un hash de una sola vez de Lamport para generar el token de cliente. Para llegar a la credencial preexistente bajo este modo de realización alternativo, las ecuaciones 1 y 2 cambian para verse de la forma siguiente en las ecuaciones 3 y 4:

credencial preexistente = $HMAC^{i}$ (contraseña, salt | nombre del servicio), donde **i** es el índice de hash; **(Ec. 3)**

token de cliente = HMAC (credencial preexistente, para la ocasión). **(Ec. 4)**

[0068] El token de cliente, a su vez, está incluido en un vector de cliente para su inclusión en la petición de conexión, por ejemplo, vector de cliente = [nombre de usuario, i, para la ocasión, token de cliente]. Como se ve en la ecuación 3, se agrega un índice i. $HMAC^{i}$ simboliza que "i" se ejecuta en la operación de hash. Por lo tanto, la credencial preexistente incluye además el índice de hash i para que el servidor 116 pueda saber cuántas veces se realizó la operación de hash para que pueda pasar por pasos similares al final.

[0069] Como otro ejemplo, en lugar de la credencial preexistente basada en una contraseña, la credencial preexistente puede ser un valor de clave u otro aprovisionado previamente por el servidor 116 con el UE 102. La clave puede ser, por ejemplo, una clave de alta entropía (por ejemplo, una clave de 256 bits) que el servidor 116 ha asociado con la cuenta del usuario del UE 102. La clave de alta entropía se puede generar de acuerdo con un proceso de selección aleatoria o de alguna otra manera, como se reconocerá. En esta situación, para crear el token del cliente, la clave se toma como la entrada preexistente en la ecuación 2 o 4 en lugar de la credencial preexistente generada a partir de las ecuaciones 1 o 3, respectivamente.

[0070] Para mayor seguridad para cualquiera de las ecuaciones descritas anteriormente, también se puede utilizar la autentificación de múltiples factores (MFA). Cuando se usa, la obtención del token del cliente puede incorporar otra credencial denominada código de acceso único (OTP). Así, las ecuaciones 2 y 4 se modificarían de la siguiente manera:

token de cliente = HMAC(credencial preexistente, para la ocasión | OTP). **(Ec. 2)**

token de cliente = HMAC(credencial preexistente, para la ocasión | OTP). **(Ec. 4)**

[0071] El token de cliente, a su vez, está incluido en un vector de cliente para su inclusión en la petición de conexión, por ejemplo, vector de cliente = [nombre de usuario, para la ocasión, i (donde se utiliza la ec. 4), token de cliente]. Aunque se describió anteriormente como una serie de obtenciones, se reconocerá que la determinación de la

credencial preexistente y el token de acceso puede implicar buscar uno o más valores en una tabla de consulta (que, por ejemplo, se obtuvieron previamente mediante el UE 102 o el servidor 116 o alguna otra entidad y se proporcionaron al UE 102/servidor 116).

[0072] La MME 106 recibe la petición de autentificación que se envía desde el eNB 104, y en la acción 506 añade un identificador de red de servicio a la petición de autentificación correspondiente a la red de servicio 112. La MME 106 puede establecer adicionalmente una conexión segura al servidor 116 a través de la GW 110 (por ejemplo, un protocolo de transferencia de hipertexto seguro (HTTPS) o seguridad de capa de transporte (TLS) por nombrar dos ejemplos) para transmitir la petición de autentificación modificada al servidor 116.

[0073] En la acción 508, la MME 106 transmite la petición de autentificación modificada al servidor 116.

[0074] En la acción 510, una vez que el servidor 116 recibe la petición de autentificación modificada el servidor 116 procede con la verificación de la petición de autentificación modificada. Esto puede incluir obtener la credencial preexistente del token del cliente y comparar la credencial preexistente con una base de datos local de credenciales preexistentes asociadas con cuentas previamente establecidas para determinar si existe una coincidencia entre la credencial preexistente del token de cliente y uno en la base de datos. Por ejemplo, la comparación puede incluir restar un valor del otro y determinar si se obtiene como resultado un valor cero, o algún valor dentro de un rango predeterminado de cero (ya sea positivo o negativo). Como se reconocerá, también se pueden usar otros procedimientos de comparación sin apartarse del alcance de la presente divulgación.

[0075] Esto es posible porque el servidor 116 también sigue el mismo enfoque que se describe anteriormente en llegar al token de cliente para una credencial preexistente dada (y para llegar a la credencial preexistente para una contraseña dada). En un modo de realización, esto es un resultado de que el UE 102 y el servidor 116 concuerden de antemano, por ejemplo en el canal fuera de banda, en un enfoque de obtención particular para el token de cliente (y credencial preexistente en algunos modos de realización). En otro modo de realización, esto es un resultado del UE 102 que incluye en la petición de autentificación una identificación de qué tipo de autentificación se usó (por ejemplo, de acuerdo con las Ecuaciones 1/2 o Ecuaciones 3/4, o una clave, certificado de identidad, etc.). Como resultado, el servidor 116 puede acceder a la credencial (o contraseña) preexistente asociada con el nombre de usuario incluido en la petición de autentificación y realizar las mismas operaciones en la credencial (o contraseña) preexistente en el servidor 116 como se hizo sobre la credencial preexistente en el UE 102. De forma alternativa, el token del cliente se puede obtener de antemano y el token del cliente recibido puede compararse con la versión local en el servidor 116.

[0076] Si el servidor 116 no puede verificar la credencial preexistente asociada con la petición del UE 102 (por ejemplo, no puede confirmar que el valor de la credencial preexistente del token del cliente coincida con el valor de una credencial preexistente en la base de datos), el servidor 116 denegará la petición. Si el servidor 116 verifica la credencial preexistente (por ejemplo, confirmando una coincidencia), el servidor 116 continúa con la compilación de un vector de autorización. Por lo tanto, en respuesta a la recepción de la petición de autentificación que incluía un token de cliente del UE 102, de acuerdo con los modos de realización de la presente divulgación, el UE 102 se autentifica en el servidor 116 antes de que se realice una autentificación mutua entre el UE 102 y la red de servicio 112 (en contraste con las prácticas actuales donde un UE no se autentifica al HSS como parte de una petición de autentificación). En un modo de realización, los componentes del vector de autorización se obtienen basándose en la credencial preexistente de la Ecuación 1 o la Ecuación 3 anterior, dependiendo del enfoque adoptado en el UE 102 (el mismo enfoque puede tomarse tanto en el UE 102 como en el servidor 116, por lo que esa autentificación mutua será posible entre el UE 102 y la MME 106 más adelante). El vector de autorización puede incluir K_{ASME} (entidad de administración de seguridad de acceso), un token de autentificación (AUTN), un número aleatorio (RAND) y una respuesta esperada del UE (XRES). La K_{ASME} es una clave base de MME 106 que tanto MME 106 como el servidor 116 conocen porque el servidor 116 la comparte con la MME 106. De acuerdo con este modo de realización, K_{ASME} se basa en el valor de "credencial preexistente" de las ecuaciones 1 o 3, así como en los valores para la ocasión y RAND.

[0077] En otro modo de realización, antes de compilar el vector de autentificación del servidor 116 puede utilizar un PAKE (clave de acuerdo autentificada con contraseña) para llegar a una nueva clave secreta compartida entre el UE 102 y el servidor 116. Por ejemplo, como parte del procedimiento PAKE, el servidor 116 puede participar en un handshake de cuatro vías con el UE 102. Otros niveles de handshake (por ejemplo, de dos vías, de tres vías, etc.) pueden ser posibles como se reconocerá. Los elementos de la red de servicio 112 pueden transmitir las comunicaciones entre el UE 102 y el servidor 116 durante el handshake de 4 vías (incluso aunque el procedimiento de conexión aún no se haya completado). Una vez que se acuerda una clave secreta compartida, tanto el UE 102 como el servidor 116 almacenan la clave secreta compartida y el servidor 116 usa la clave secreta compartida para obtener K_{ASME}. La finalización de un procedimiento PAKE hace que el UE 102 y el servidor 116 se autentifiquen mutuamente antes de que el UE 102 realice la autentificación mutua con la red de servicio 112.

[0078] En aspectos de la presente divulgación, el servidor 116 utiliza uno o el otro - obtención de K_{ASME} basándose en la "credencial preexistente" (Ec. 1 o 3) o basándose en una nueva clave secreta compartida. En otro aspecto, el servidor 116 puede intentar la obtención de K_{ASME} basándose en la "credencial preexistente" primero y, si eso fallara por alguna razón, a continuación debe pasar a usar PAKE para establecer una nueva clave secreta compartida para usar en la obtención. K_{ASME}, si ambos enfoques son compatibles tanto con el UE 102 como con el servidor 116. K_{ASME}

puede permanecer válido durante la sesión de autentificación. Además, K_{ASME} se puede usar para obtener claves subsiguientes, incluidas las claves de integridad y cifrado de NAS y las claves de integridad y cifrado del servidor de aplicaciones (AS).

[0079] Una vez que se compila el vector de autentificación, en la acción 512 el servidor 116 envía la respuesta de autentificación de nuevo a la MME 106 a través de la conexión segura.

[0080] En la acción 514, la MME 106 extrae K_{ASME} y la respuesta esperada XRES del vector de autentificación. La MME 106 almacena estos valores y los reenvía en el valor aleatorio RAND y el token de autentificación AUTN al UE 102 en la acción 516 en una petición de autentificación al UE 102 (por ejemplo, para la autentificación mutua en la red de servicio 112).

[0081] En la acción 518, una vez que el UE 102 recibe la petición de autentificación con el token de autentificación AUTN y RAND desde la MME 106, el UE 102 intenta validar el token de autentificación AUTN. El UE 102 valida el token de autentificación AUTN basándose en la clave secreta compartida con el servidor 116. En los modos de realización en los que no se utiliza PAKE, este es el valor de la "credencial preexistente" según se obtiene de acuerdo con las ecuaciones 1 o 3 anteriores. Cuando se usa PAKE, es la clave secreta compartida almacenada en el UE 102 después de un acuerdo con el servidor 116 del handshake de cuatro vías. Por ejemplo, el UE 102 determina su propia versión de AUTN basándose en el secreto compartido (credencial preexistente o clave secreta compartida) y se compara con el AUTN recibido de la MME 106. Si los valores no coinciden, el UE 102 no puede validar AUTN y la autentificación falla. Si hay una coincidencia, entonces se valida AUTN y el UE 102 procede a la determinación de una respuesta RES y su propia versión de K_{ASME}, que el UE 102 y MME 106 usarán más adelante para obtener otras claves para el cifrado y la protección de integridad de la señalización de NAS.

[0082] En la acción 520, el UE 102 envía los RES a la MME 106 de modo que la MME 106 puede comparar XRES que almacena previamente desde el servidor 116 a la RES recibida desde el UE 102. Si los dos coinciden, entonces la autentificación ha sido exitosa y el proceso puede continuar con la configuración de las claves NAS y AS. Como resultado, el UE 102 puede acceder al servicio, a través de la red de servicio 112, con el proveedor de servicios de aplicaciones hospedado por el servidor 116 que patrocina (por ejemplo, que cubre parte o todo el coste del acceso específico) la conexión del UE 102 con la red de servicio 112. Esto es cierto incluso cuando el UE 102 no tiene una tarjeta SIM o una suscripción existente con ningún proveedor de red/servicio doméstico.

[0083] La FIG. 6 es un diagrama de protocolo que ilustra aspectos de señalización entre un UE, una red de servicio y un proveedor de servicios de aplicaciones para proporcionar conectividad patrocinada de acuerdo con diversos aspectos de la presente divulgación. Para simplificar el análisis, se hará referencia a los elementos mostrados en la FIG. 1 (por ejemplo, el UE 102, MME 106, el servidor 116 operado por el proveedor de servicios de aplicaciones y un servidor de autorización 120 que puede estar separado o integrado con el servidor 116) al describir las acciones en el diagrama de protocolo de la FIG. 6. La FIG. 6 describe un modo de realización en la que el UE 102 autoriza a la MME 106 a acceder a las credenciales asociadas con el usuario del UE 102 en el servidor 116.

[0084] En la acción 602, el UE 102 envía una petición de conexión a la red de servicio 112, que recibe la MME 106, para acceder a un servicio patrocinado a través del servidor 116 (el proveedor de servicios de aplicaciones). La petición de conexión incluye información que indica que el UE 102 desea autentificarse directamente con el servidor 116, en lugar de proporcionar el token del cliente que se basa en una credencial preexistente como parte de una petición de autentificación como en la acción 504 de la FIG. 5 analizada anteriormente. Por ejemplo, el UE 102 puede incluir un nombre de usuario asociado con el proveedor de servicios de aplicaciones sin proporcionar un token de cliente basado en una credencial preexistente. La petición de conexión puede incluir explícitamente un identificador de que la MME 106 entiende para indicar que el UE 102 necesita autentificarse directamente con el servidor 116, o esto puede ser inferido indirectamente por la MME 106 en virtud del hecho de que la petición de conexión carece de una credencial. El UE 102 también puede incluir información para identificar el servidor 116 (tal como el nombre de dominio del proveedor de servicios de aplicaciones en el servidor 116 o un ID de aplicación) para ayudar a la red de servicio 112 en aspectos de enrutamiento de la petición al servidor 116. La petición de conexión no incluye ningún tipo de identificador de abonado (por ejemplo, IMSI, etc.). La petición de conexión también puede identificar el alcance solicitado de su acceso a la red de servicio 112 (por ejemplo, para la conectividad patrocinada al servicio por el servidor 116).

[0085] En la acción 604, la MME 106 determina que no hay ningún token de cliente basado en una credencial preexistente y/o localiza la información de identificación explícita, y por lo tanto envía una petición de autentificación al servidor de autorización 120. Como se indicó anteriormente, el servidor de autorización 120 puede ser una entidad separada del servidor 116 o estar integrado con él. La MME 106 puede incluir en la petición de autentificación un identificador de la red de servicio 112. El identificador puede haber sido proporcionado o recibido del servidor de autorización 120 en un momento anterior cuando la relación patrocinada se aprovisionó entre el proveedor de servicios de aplicaciones (representado como el servidor 116) y la red de servicio 112.

[0086] En la acción 606, el servidor de autorización 120 inicia la comunicación con el UE 102 a través de la red de servicio 112 para autentificar el UE 102. Los elementos de la red de servicio 112 pueden transmitir las comunicaciones

entre el UE 102 y el servidor de autentificación 120 durante el proceso de autentificación de usuario y autorización de acceso, lo cual puede implicar una o más peticiones y respuestas entre el UE 102 y el servidor de autorización 120 (aunque el procedimiento de conexión aún no se ha completado). Por ejemplo, una interfaz de usuario del UE 102 puede dirigir o solicitar a un usuario del UE 102 que introduzca un nombre de usuario y contraseña a través de una interfaz de usuario (no se muestra) para autentificar (por ejemplo, un nombre de usuario, una contraseña que coincida con uno en una perfil almacenado en, o accesible por, el servidor de autorización) al usuario que ya está asociado con el servidor de funcionamiento del proveedor de servicios 116. Como otro ejemplo, el UE 102 puede acceder a una credencial (o clave, o certificado de identidad) preexistente para el proveedor de servicios de aplicaciones que se almacenó previamente en la memoria 204 (por ejemplo, a través del módulo de acceso 208) sin requerir que el usuario interactúe a través de la interfaz de usuario.

[0087] Además de la autentificación del usuario asociado con el proveedor de servicios de aplicaciones en la acción 606, el servidor de autorización 120 también obtiene una autorización de acceso desde el UE 102 permitiendo que la MME 106 (u otro elemento de red adecuado en la red de servicio 112) para acceder el perfil de usuario asociado con el UE 102 desde el servidor 116. En un modo de realización, la autorización de acceso se obtiene por separado y distinta de la autentificación del usuario (por ejemplo, una consulta separada). En otro modo de realización, la autorización de acceso puede estar implícita en la autentificación exitosa del usuario. Si la autentificación del usuario y/o la autorización de acceso fallan, entonces el proceso se detiene y el UE 102 es notificado por la MME 106, que es notificada por el servidor de autorización 120.

[0088] Si la autentificación de usuario y la autorización de acceso tienen éxito, en la acción 608 el servidor de autorización 120 envía un código de autorización a la MME 106 (en lugar de, por ejemplo, al UE 102 y a continuación se redirige de nuevo a la MME 106). El código de autorización es un valor diferente de la credencial, contraseña u otra credencial relacionada del usuario preexistente y, por lo tanto, está protegido de la MME 106. Con el código de autorización, el servidor de autorización 120 también puede incluir una instrucción para que la MME 106 use el código de autorización para la verificación cuando solicite un token de acceso como se describe a continuación.

[0089] Con el código de autorización, la MME 106 está listo para solicitar un token de acceso desde el servidor de autorización 120 para tener acceso al perfil de usuario asociado con el UE 102 desde el servidor 116. En la acción 610, la MME 106 envía una petición al servidor de autorización 120 para un token de acceso. Como parte de la petición, la MME 106 incluye el código de autorización recibido en la acción 608. La petición puede incluir además una identificación de la red de servicio 112 (o al menos la MME 106).

[0090] En la acción 612, el servidor de autorización 120 responde a la petición de token de acceso de acción 610 después de la autentificación de la MME 106 (o, más en general, la red de servicio 112) y validar el código de autorización. Si no tiene éxito, la respuesta indica la denegación y, en algunos modos de realización, una razón o una indicación sobre la denegación. Si tiene éxito (por ejemplo, se proporciona el código de autorización adecuado), el servidor de autorización 120 responde con el token de acceso solicitado a la MME 106. La respuesta puede incluir, además del token de acceso, una descripción del tipo de token de acceso, un período específico de tiempo después del cual el token de acceso expirará (ya no será válido), y un token de actualización en caso de que el token de acceso expire (que se puede usar para obtener un nuevo token de acceso).

[0091] En la acción 614, la MME 106, ahora con el token de acceso, procede a solicitar y recibir las credenciales de usuario. Esto se puede hacer para que la MME 106 ayude a completar una conexión del UE 102 a la red de servicio 112, donde la conectividad a la red de servicio 112 ahora está patrocinada por el proveedor de servicios de aplicaciones alojado por el servidor 116. Como resultado, los modos de realización de la FIG. 6 permiten que un UE 102 se conecte a una red de servicio 112 sin proporcionar un token de cliente basado en una credencial preexistente (p. ej., Contraseña, contraseña con función hash o token de acceso previamente almacenado en el UE 102, etc.) en la petición de conexión.

[0092] Volviendo ahora a la FIG. 7A, un diagrama de flujo ilustra un procedimiento a modo de ejemplo 700 para acceder a una red para un servicio patrocinado por un proveedor de servicios de aplicaciones que opera un servidor de acuerdo con varios aspectos de la presente divulgación. El procedimiento 700 puede implementarse en el UE 102. El procedimiento 700 se describirá con respecto a un solo UE 102 para simplificar el análisis, aunque se reconocerá que los aspectos descritos en el presente documento pueden ser aplicables a una pluralidad de UE 102. Se entiende que las "acciones" anteriores y los "pasos" siguientes se pueden usar de manera intercambiable. También se entiende que se pueden proporcionar pasos adicionales antes, durante y después de los pasos del procedimiento 700, y que algunos de los pasos descritos se pueden reordenar, reemplazar o eliminar para otros modos de realización del procedimiento 700.

[0093] En el paso 702, el UE 102 identifica una o más redes de servicio 112 a través de las cuales podría estar disponible una conexión patrocinada. Por ejemplo, el UE 102 puede recibir una o más radiodifusiones de una o más redes de servicio 112 anunciando conectividad patrocinada para uno o más servicios. Como otro ejemplo, el UE 102 puede verificar la memoria 204 para una lista de redes fiables que pueden haberse almacenado en el UE 102 previamente basándose en la información del servidor que aloja al proveedor de servicios de aplicaciones.

[0094] Hay varias maneras diferentes en las que el UE 102 puede usar una credencial preexistente para autentificar a la red de servicio 112 para aprovecharse de un patrocinio de conectividad ofrecido. Si el UE 102 configura un nombre de usuario y una contraseña con el servidor 116, el paso de decisión 704 puede dirigir el procedimiento 700 al paso 706.

[0095] En el paso 706, el UE 102 genera un hash de contraseña con un valor de salt, por ejemplo como se describe anteriormente con respecto a cualquiera de las ecuaciones 1 o 3, que da como resultado la credencial preexistente. En modos de realización alternativos, este paso puede no ser necesario cuando el servidor 116 (por ejemplo, a través del canal fuera de banda) aprovisionó al UE 102 con la credencial preexistente de la contraseña previamente.

[0096] En el paso 708, el UE 102 toma la credencial preexistente y genera un hash con un valor para la ocasión (y/u otros valores) para dar como resultado en el token de cliente, por ejemplo como se describe anteriormente con respecto a cualquiera de las ecuaciones 2 o 4.

[0097] Volviendo al paso de decisión 704, si el UE 102 en lugar de eso recibió una clave, tal como una clave de alta entropía, desde el servidor 116 en un momento anterior para su uso al iniciar sesión en el servidor de proveedor de servicios de aplicaciones 116, entonces el procedimiento 700 continúa con el paso 708 (omitiendo el paso 706), donde la credencial preexistente es la clave que se usa en las ecuaciones 2 o 4.

[0098] En el paso 710, el UE 102 envía una petición de conexión a la red de servicio 112 en un intento de aprovecharse de la conectividad patrocinada. El UE 102 envía, como parte de su petición de conexión, el token del cliente en lugar de otros identificadores tradicionales, como un IMSI. El token de cliente puede incluirse como parte de un vector de cliente que, además del token de cliente, incluye el nombre de usuario asociado con la credencial preexistente y un valor para la ocasión (e índice, cuando se usa).

[0099] Después de que el UE 102 ha enviado la petición de conexión a la red de servicio 112, tal como se describe con respecto a las diversas figuras anteriores, la red de servicio 112 envía la petición en el servidor 116 como una petición de información de autentificación al servidor 116. El servidor 116 puede entonces verificar la petición. La verificación puede incluir la comparación de aspectos del vector del cliente, como el nombre de usuario y/o la contraseña proporcionados por el UE 102 (asociado a un usuario del UE 102) con la información de acceso mantenida por el servidor 116 del proveedor de servicios de aplicaciones. La verificación puede ocurrir cuando la comparación da como resultado una determinación de una coincidencia entre los valores comparados. Después de la verificación, el servidor 116 continúa con la compilación de una respuesta de autentificación (vector). La respuesta de autorización (vector) puede incluir K_{ASME}, AUTN, RAND y XRES, donde un elemento de nodo de red de la red de servicio 112 (por ejemplo, MME 106) puede almacenar XRES y K_{ASME} localmente y reenviarlos en RAND y AUTN al UE 102.

[0100] Si el UE 102 y el servidor 116 están configurados para PAKE, entonces, en el paso de decisión 712 el procedimiento 700 pasa al paso 714.

[0101] En el paso 714, el UE 102 recibe una comunicación desde el servidor 116 que se transportó a través de la red de servicio 112. La comunicación es el mensaje inicial de un handshake (por ejemplo, de cuatro vías) entre el UE 102 y el servidor 116.

[0102] En el paso 716, el UE 102 y el servidor 116 acuerdan una clave secreta compartida actualizada durante el handshake. Una vez que se acuerda una clave secreta compartida, tanto el UE 102 como el servidor 116 almacenan la clave secreta compartida y el servidor 116 usa la clave secreta compartida para obtener una o más claves, como K_{ASME}.

[0103] Después de que el UE 102 y el servidor 116 hayan acordado una clave secreta compartida, el servidor 116 usa la clave secreta compartida para generar uno o más aspectos del vector de autentificación que se proporcionarán en la respuesta a la red de servicio 112 y, en parte, al UE 102.

[0104] El procedimiento 700 pasa al paso 718, donde el UE 102 recibe una petición de autentificación desde la red de servicio 112 que se basa en una respuesta de autentificación recibida en la red de servicio 112 desde el servidor 116. La petición de autentificación incluye un token de autentificación que fue generado o determinado por el servidor 116 y enviado por la red de servicio 112. La petición de autentificación también puede incluir un número aleatorio del servidor 116.

[0105] Volviendo al paso de decisión 712, si el UE 102 y el servidor 116 no están configurados para PAKE, entonces el procedimiento 700 continúa con el paso 718 como ya se ha descrito.

[0106] En el paso 720, el UE 102 valida el token de autentificación. El UE 102 valida el token de autentificación AUTN basándose en la clave secreta compartida con el servidor 116 (donde se usó PAKE) o la credencial de contraseña intermedia. Por ejemplo, el UE 102 determina su propia versión de AUTN basándose en el secreto compartido (la credencial preexistente o la clave secreta compartida) y se compara con el AUTN recibido de la red de servicio 112.

[0107] Si hay una coincidencia, entonces el procedimiento 700 avanza al paso 722 donde el UE 102 determina una respuesta RES y su propia versión de K_{ASME}, que luego utilizarán el UE 102 y la red de servicio 112 (por ejemplo, MME 106) para obtener otras claves para el cifrado y la protección de la integridad de la señalización NAS.

[0108] Si la RES del UE 102 coincide con la XRES del servidor 116 en la MME 106, entonces la autentificación ha sido exitosa y el proceso puede continuar con la configuración de las claves NAS y AS. Como resultado, el UE 102 puede acceder al servicio, a través de la red de servicio 112, con el servidor de proveedor de servicios de aplicaciones 116 patrocinando (por ejemplo, cubriendo parte o todo el coste del acceso específico) la conexión del UE 102 con la red de servicio 112. Esto es cierto incluso cuando el UE 102 no tiene una tarjeta SIM o una suscripción existente con ningún proveedor de red/servicio doméstico.

[0109] La FIG. 7B es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo 740 para otorgar acceso a la red para un servicio patrocinado por un proveedor de servicios de aplicaciones de acuerdo con varios aspectos de la presente divulgación. El procedimiento 740 puede implementarse en el servidor 116. El procedimiento 740 se describirá con respecto a un único servidor 116 para simplificar el análisis, aunque se reconocerá que los aspectos descritos aquí pueden ser aplicables a una pluralidad de servidores 116. Se entiende que se pueden proporcionar pasos adicionales antes, durante y después de los pasos del procedimiento 740, y que algunos de los pasos descritos se pueden reordenar, reemplazar o eliminar para otros modos de realización del procedimiento 740.

[0110] En el paso 742, el servidor 116 establece un acuerdo de nivel de servicio con la red de servicio 112 (por ejemplo, a modo de una función de provisión de servicios). Como resultado de la función de provisión de servicios, la red de servicio 112 puede radiodifundir a los destinatarios información que identifica la conectividad patrocinada al servicio en nombre del servidor 116. En un modo de realización, esto también puede implicar que el servidor 116 proporcione al UE 102 información que identifique algunas o todas las redes de confianza, o redes que han suscrito acuerdos para proporcionar la conectividad patrocinada al servicio en nombre del servidor 116.

[0111] En el paso 744, el servidor 116 recibe una petición de autentificación desde la red de servicio 112 en respuesta a la red de servicio 112 que recibe una petición de conexión desde el UE 102 (que incluye un token de cliente en lugar de IMSI u otro identificador celular).

[0112] Hay varios tipos diferentes de credenciales preexistentes que un UE 102 puede usar para autentificarse en la red de servicio 112 para aprovechar el patrocinio de conectividad ofrecido por el servidor 116. Si el UE 102 ha configurado un nombre de usuario y una contraseña con el servidor 116, el paso de decisión 746 puede dirigir el procedimiento 740 al paso 746.

[0113] En el paso 746, el servidor 116 genera un hash de la contraseña, asociado con el usuario cuyo UE 102 está tratando de aprovecharse de la conectividad patrocinada, con un valor de salt, por ejemplo como se describe anteriormente con respecto a cualquiera de las ecuaciones 1 o 3, dando como resultado la credencial preexistente. En un modo de realización alternativo, este paso puede omitirse donde el servidor 116 aprovisionó la credencial preexistente de la contraseña previamente.

[0114] En el paso 748, el servidor 116 toma la credencial preexistente y genera un hash con un valor para la ocasión (y/u otros valores), por ejemplo como se describe anteriormente con respecto a cualquiera de las Ecuaciones 2 o 4 para dar como resultado una copia lateral del servidor del token del cliente.

[0115] En el paso 750, el servidor 116 comprueba la petición de autentificación con el perfil del usuario (por ejemplo, comparación de nombre de usuario, credenciales, etc.). En un modo de realización, esto puede incluir comparar el token del cliente recibido con la copia del lado del servidor determinada. Una coincidencia es posible porque el servidor 116 y el UE 102 pueden, cada uno de ellos, generar un hash de la credencial preexistente de la misma manera para llegar al token del cliente.

[0116] Volviendo al paso de decisión 746, si el servidor 116 y el UE 102 hubieran confiado en una clave (como una clave de alta entropía) enviada desde el servidor 116 en un momento anterior para su uso en el inicio de sesión en el proveedor de servicios de aplicaciones representado por el servidor 116, entonces el procedimiento 740 avanza al paso 748, donde la credencial preexistente es la clave de alta entropía. El procedimiento 740 puede avanzar después hasta el paso 750 como se ha analizado.

[0117] Si el servidor 116 y el UE 102 están configurados para PAKE, en el paso de decisión 752, el procedimiento 740 pasa al paso 754.

[0118] En el paso 754, el servidor 116 inicia la comunicación con el UE 102 a través de la red de servicio 112. La comunicación es el mensaje inicial de un handshake (por ejemplo, de cuatro vías) entre el servidor 116 y el UE 102.

[0119] En el paso 756, el servidor 116 y el UE 102 acuerdan una clave secreta compartida actualizada durante el handshake. Una vez que se acuerda una clave secreta compartida, tanto el UE 102 como el servidor 116 almacenan la clave secreta compartida (por ejemplo, durante la sesión de autentificación).

[0120] En el paso 758, el servidor 116 utiliza la clave secreta compartida para obtener una o más claves, tales como $K_{ASME,}$ y generar otros aspectos de un vector de autentificación incluyendo AUTN. El servidor 116 también genera/determina otros valores para su inclusión en el vector de autentificación, incluidos XRES y un número aleatorio RAND.

[0121] Volviendo al paso de decisión 752, si el UE 102 y el servidor 116 no están configurados para PAKE, el procedimiento 740 pasa al paso 758 como ya se describió, donde la clave secreta compartida es, en su lugar, la credencial preexistente.

[0122] En el paso 760, el servidor 116 transmite el vector de autentificación a la red de servicio 112 (por ejemplo, a la MME 106). La MME 106 almacena K_{ASME} así como la XRES y reenvía otros aspectos, incluidos el AUTN y el RAND al UE 102 para la autentificación mutua. Si la autentificación mutua es exitosa entre la MME 106 y el UE 102, entonces el proceso puede continuar con la configuración de la clave AS y NAS entre la red de servicio 112 y el UE 102, y finalmente el UE 102 puede continuar accediendo al servicio a través de la red de servicio 112 basada en la conexión patrocinada. La red de servicio 112 rastrea aspectos de la conexión patrocinada (por ejemplo, contabilidad, medición, facturación y otras funciones).

[0123] En el paso 762, en algún momento después de la exitosa conexión del UE 102 a la red de servicio 112, el servidor 116 recibe una carga de la red de servicio 112 para los aspectos de la conectividad patrocinada utilizados por el UE 102. A continuación, el servidor 116 aborda la carga recibida de acuerdo con uno o más enfoques, como reconocerán los expertos en la(s) técnica(s) relevante(s). Como resultado, el UE 102 puede acceder al servicio, a través de la red de servicio 112, con el proveedor de servicios de aplicaciones patrocinando (por ejemplo, cubriendo parte o todo el coste del acceso específico) la conexión del UE 102 con la red de servicio 112.

[0124] La FIG. 7C es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo 770 para facilitar el acceso a la red para un servicio patrocinado de acuerdo con diversos aspectos de la presente divulgación. El procedimiento 770 puede implementarse en la MME 106 (y/u otros elementos de red de la red de servicio 112). El procedimiento 770 se describirá con respecto a la MME 106 para simplificar el análisis, aunque se reconocerá que los aspectos descritos en el presente documento pueden ser aplicables a uno o más elementos de la red en la red de servicio 112. Se entiende que se pueden proporcionar pasos adicionales antes, durante y después de los pasos del procedimiento 770, y que algunos de los pasos descritos se pueden reordenar, reemplazar o eliminar para otros modos de realización del procedimiento 770.

[0125] En el paso 772, la MME 106 recibe una petición de descubrimiento de servicio desde el UE 102 y responde. Por ejemplo, la MME 106 puede haber causado que elementos de la red, como uno o más eNB, radiodifundan la conectividad patrocinada por el proveedor de servicios de aplicaciones alojado en el servidor 116. La petición de descubrimiento de servicio puede ser un intento del UE 102 de confirmar la existencia de la conectividad patrocinada y/o la disponibilidad de la red de servicio 112 en ese momento.

[0126] En el paso 774, la MME 106 recibe una petición de conexión desde el UE 102. La petición de conexión incluye en ella un token de cliente que se basa en una credencial preexistente establecida previamente entre el UE 102 (y/o el usuario del UE 102) y el proveedor de servicios de aplicaciones alojado por el servidor 116 en lugar de otros identificadores tradicionales, como IMSI.

[0127] En el paso 776, la MME 106 añade un identificador de red de servicio a la petición de conexión que corresponde a la red de servicio 112, y formula una petición de autentificación para la transmisión en el servidor 116. Además, la MME 106 puede establecer una conexión segura (por ejemplo, TLS o HTTPS) al servidor 116 para transmitir la petición de autentificación al servidor 116.

[0128] En el paso 778, la MME 106 envía la petición de autentificación al servidor 116, por ejemplo, a través de la conexión segura establecida en el paso 776.

[0129] Si el servidor 116 y el UE 102 están configurados para PAKE, en el paso de decisión 780, el procedimiento 770 pasa al paso 782.

[0130] En el paso 782, la petición MME 106 transmite mensajes de petición y respuesta entre el servidor 116 y el UE 102 durante un handshake (por ejemplo, cuatro direcciones) entre el servidor 116 y el UE 102 (u otro nivel de handshake). La MME 106 transmite los mensajes de petición/respuesta hasta que el servidor 116 y el UE 102 acuerdan una clave secreta compartida.

[0131] En el paso 784, después de haberse acordado la clave secreta compartida, la MME 106 recibe un vector de autentificación del servidor 116. El vector de autentificación puede incluir K_{ASME}, AUTN, un número aleatorio RAND y XRES.

[0132] Volviendo al paso de decisión 780, si el UE 102 y el servidor 116 no están configurados para PAKE, entonces el procedimiento 770 continúa con el paso 784 como ya se ha descrito.

[0133] En el paso 786, los extractos MME 106 K_{ASME} y XRES para su uso en la autentificación mutua con el UE 102 a partir del vector de autentificación recibido en el paso 784.

[0134] En el paso 788, la MME 106 envía una petición de autentificación al UE 102 que incluye los valores AUTN y RAND. El UE 102 valida AUTN basándose en la clave secreta compartida con el servidor 116 (donde se usó PAKE) o la credencial preexistente y determina una respuesta RES. Por ejemplo, el UE 102 determina su propia versión de AUTN basándose en la clave secreta compartida y la compara con el AUTN recibido de la MME 106. Si los valores no coinciden, el UE 102 no puede validar AUTN y la autentificación falla. Si hay una coincidencia, entonces se valida AUTN.

[0135] En el paso 790, la MME 106 recibe las RES desde el UE 102 y la compara con la XRES que la MME 106 ha almacenado en el paso 786. Si la RES del UE 102 coincide con la XRES del servidor 116 en la MME 106, entonces la autentificación ha sido exitosa y el proceso puede continuar con la configuración de las claves NAS y AS. Como resultado, el UE 102 puede acceder al servicio, a través de la red de servicio 112, con el proveedor de servicios de aplicaciones patrocinando (por ejemplo, cubriendo parte o todo el coste del acceso específico) la conexión del UE 102 con la red de servicio 112. Esto es cierto incluso cuando el UE 102 no tiene una tarjeta SIM o una suscripción existente con ningún proveedor de red/servicio doméstico.

[0136] La FIG. 8A es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo 800 para acceder a una red para un servicio patrocinado por un proveedor de servicios de aplicaciones de acuerdo con diversos aspectos de la presente divulgación. El procedimiento 800 puede implementarse en el UE 102. El procedimiento 800 se describirá con respecto a un solo UE 102 para simplificar el análisis, aunque se reconocerá que los aspectos descritos en el presente documento pueden ser aplicables a una pluralidad de UE 102. Además, como se ha mencionado con respecto a la FIG. 6 anterior, el servidor de autorización 120 y el servidor 116 pueden ser entidades iguales o diferentes. Para simplificar el análisis, lo siguiente hará referencia al servidor 116 al tiempo que analizará aspectos relacionados con el servidor de autorización 120. Se entiende que se pueden proporcionar pasos adicionales antes, durante y después de los pasos del procedimiento 800, y que algunos de los pasos descritos se pueden reordenar, reemplazar o eliminar para otros modos de realización del procedimiento 800.

[0137] En el paso 802, el UE 102 identifica una o más redes de servicio 112 a través de las cuales puede estar disponible una conexión patrocinada, por ejemplo como se describe anteriormente con respecto al paso 702 de la FIG. 7A.

[0138] En el paso 804, el UE 102 envía una petición de conexión a la red de servicio 112 en un intento de aprovecharse de la conectividad patrocinada. En contraste con el paso 710 de la FIG. 7A, sin embargo, el UE 102 no envía un token de cliente que se basa en una credencial preexistente con la petición de conexión (el UE 102 tampoco envía IMSI u otra credencial celular). En cambio, de acuerdo con los modos de realización de las FIGs. 8A-8C, el UE 102 se basará en una comunicación de autentificación de usuario y autorización de acceso con el servidor 116 para ayudar a autentificar al servidor 116. La MME 106 envía una petición de autentificación al servidor 116.

[0139] En el paso 806, en respuesta a la petición de autentificación que la MME 106 envió, el UE 102 recibe una petición de autentificación de usuario y autorización acceso desde el servidor 116 a través de la red de servicio 112. El UE 102 responde a la petición con la información requerida (por ejemplo, al introducir o proporcionar un nombre de usuario y/o contraseña (en forma de una credencial de acceso preexistente, por ejemplo) donde o cuando se solicite) al servidor 116. Como se analizó con respecto a la FIG. 6 anterior y se describirá más adelante en las FIGs. 8B y 8C, la MME 106 recibe un código de autorización del servidor 116 después de que el UE 102 y el servidor 116 completen la autentificación de usuario/autorización de acceso. La MME 106 utiliza este código de autorización para solicitar y recibir un token de acceso que a continuación la MME 106 puede usar para solicitar y recibir información de perfil de usuario del servidor 116 que utiliza para autentificar el UE 102 a la red de servicio 112 con el fin de aprovechar la conectividad patrocinada.

[0140] Volviendo ahora a la FIG. 8B, un diagrama de flujo ilustra un procedimiento a modo de ejemplo 820 para otorgar acceso a la red para un servicio patrocinado por un proveedor de servicios de aplicaciones de acuerdo con diversos aspectos de la presente divulgación. El procedimiento 820 puede implementarse en el servidor 116 (que a los fines de este análisis también describe la funcionalidad del servidor de autorización 120). Se entiende que se pueden proporcionar pasos adicionales antes, durante y después de los pasos del procedimiento 820, y que algunos de los pasos descritos se pueden reordenar, reemplazar o eliminar para otros modos de realización del procedimiento 820.

[0141] En el paso 822, el servidor 116 recibe una petición de autentificación desde la red de servicio 112, por ejemplo de la MME 106 (que envió la petición en respuesta a una petición de conexión desde un UE 102).

[0142] En el paso 824, el servidor 116 inicia una petición con el UE 102 a través de la red de servicio 112 para completar la autentificación de usuario y la autorización de acceso con el UE 102. Por ejemplo, los elementos de la

red de servicio 112 pueden transmitir las comunicaciones entre el UE 102 y el servidor 116 durante el proceso de autentificación de usuario y autorización de acceso, lo cual puede implicar una o más peticiones y respuestas de ida y vuelta con respecto a una credencial preexistente entre El UE 102 y el servidor 116 como se describió anteriormente con respecto a la acción 606 de la FIG. 6.

[0143] En el paso 826, el servidor 116 como parte del proceso de autentificación de usuario/autorización de acceso analiza las respuestas desde el UE 102 para determinar si el UE 102 se ha autentificado con éxito (por ejemplo, proporcionando el nombre de usuario y/o credenciales de contraseña apropiados en comparación con los valores correspondientes almacenados en un perfil almacenado en, o accesible por, el servidor 116). El servidor 116 determina además si el UE 102 ha completado la autorización de acceso (por ejemplo, otorgando un permiso o ubicando un permiso previamente almacenado en el servidor 116 para el usuario asociado con el UE 102). Si la autentificación de usuario y/o la autorización de acceso fallan, entonces el procedimiento 820 avanza al paso 842, donde finaliza el proceso (y el servidor 116 puede enviar información al UE 102 indicando por qué falló el proceso, como una combinación incorrecta de nombre de usuario/contraseña y/o falta de permiso otorgado para que la red de servicio 112 acceda al perfil de usuario asociado con el usuario del UE 102).

[0144] Si la autentificación de usuario y la autorización de acceso tienen éxito, el procedimiento 820 continúa hasta el paso 828, donde el servidor 116 envía un código de autorización a la MME 106 (en lugar de, por ejemplo, al UE 102 y luego se redirige de nuevo a la MME 106), por ejemplo, como se describió anteriormente con respecto a la acción 608 de la FIG. 6.

[0145] En el paso 830, el servidor 116 recibe una petición de la MME 106, incluyendo el código de autorización, para un token de acceso.

[0146] En el paso 832, el servidor 116 analiza el código de autorización que se incluye con la petición de token de la MME 106. Si hay una discrepancia entre el código de autorización otorgado a la MME 106 (que el servidor 116 mantuvo almacenado) y el código de autorización recibido de la MME 106 en el paso 830, entonces se rechaza la petición y el procedimiento 820 continúa hasta el paso 842, donde el proceso finaliza (y el servidor 116 puede enviar información al UE 102 indicando por qué falló el proceso).

[0147] Si tiene éxito, el procedimiento 820 avanza al paso 834 donde el servidor 116 responde a la petición del token de acceso con el token de acceso solicitado a la MME 106, por ejemplo, como se describió anteriormente con respecto a la acción 612 de la FIG. 6.

[0148] En el paso 836, el servidor 116 recibe una petición de la MME 106 para un perfil de usuario del usuario del UE 102 para unir el UE 102 a la red de servicio 112. La petición del perfil de usuario incluye el token de acceso que la MME 106 recibió del servidor 116 como resultado del paso 834.

[0149] En el paso 838, el servidor 116 analiza la petición y el token de acceso incluida para determinar si se debe liberar la información solicitada a la MME 106. Si hay una discrepancia entre el token de acceso dado a la MME 106 y el token de acceso recibido de la MME 106 en el paso 836, entonces la petición se deniega y el procedimiento 820 pasa al paso 842, donde finaliza el proceso (y el servidor 116 puede enviar información al UE 102 indicando por qué falló el proceso).

[0150] Si tiene éxito, en el paso 840 el servidor 116 envía el perfil de usuario solicitado a la MME 106. Como resultado, el UE 102 puede conectarse a la red de servicio 112 sin proporcionar una credencial preexistente (p. ej., contraseña, contraseña de función hash, o token de acceso previamente almacenado en el UE 102, etc.) en la petición de conexión a la MME 106, en lugar de permitir que MME 106 se corresponda con el servidor 116 para obtener la información adecuada.

[0151] La FIG. 8C es un diagrama de flujo que ilustra un procedimiento 850 a modo de ejemplo para facilitar el acceso a la red para un servicio patrocinado por un proveedor de servicios de aplicaciones de acuerdo con diversos aspectos de la presente divulgación. El procedimiento 850 puede implementarse en la MME 106 (y/u otros elementos de red de la red de servicio 112). El procedimiento 850 se describirá con respecto a la MME 106 para simplificar el análisis, aunque se reconocerá que los aspectos descritos en el presente documento pueden ser aplicables a uno o más elementos de la red en la red de servicio 112. Se entiende que se pueden proporcionar pasos adicionales antes, durante y después de los pasos del procedimiento 850, y que algunos de los pasos descritos se pueden reordenar, reemplazar o eliminar para otros modos de realización del procedimiento 850.

[0152] En el paso 852, la MME 106 recibe una petición de conexión a partir de un UE 102 (que no incluye un token de cliente que se basa en una credencial preexistente o una credencial de celular/identificador de abonado) y, en respuesta, envía una petición de autentificación al servidor 116. La petición de conexión incluye información que indica que el UE 102 desea autentificarse directamente con el servidor 116, en lugar de proporcionar el token del cliente como parte de una petición de autentificación como en la acción 504 de la FIG. 5 analizada anteriormente. La petición de conexión puede incluir explícitamente un identificador que la MME 106 entiende para indicar que el UE 102 necesita

autentificarse directamente con el servidor 116, o esto puede inferirse indirectamente por la MME 106 en virtud del hecho de que la petición de conexión carece de token de cliente.

[0153] En el paso 854, la MME 106 retransmite una petición de autentificación de usuario/autorización de acceso al UE 102 desde el servidor 116, así como las respuestas de nuevo al servidor 116 desde el UE 102 (que puede incluir, por ejemplo, alguna forma de credencial preexistente).

[0154] Si la autentificación de usuario/autorización de acceso es exitosa entre el UE 102 y el servidor 116, en el paso 856, la MME 106 recibe un código de autorización del servidor 116 que se puede usar para solicitar un token de acceso. El código de autorización se envía a la MME 106 en lugar de, por ejemplo, el UE 102 y se redirige de nuevo a la MME 106.

[0155] En el paso 858, la MME 106 envía una petición de un token de acceso al servidor 116 con el fin de obtener acceso al perfil de usuario asociado con el UE 102 desde el servidor 116. Como parte de la petición, la MME 106 incluye el código de autorización recibido en el paso 856.

[0156] En el paso 860, la MME 106 recibe el token de acceso solicitado después de que el servidor 116 autentifica la MME 106 y valida el código de autorización proporcionado por la MME 106.

[0157] En el paso 862, la MME 106 envía una petición del perfil de usuario asociado con el usuario del UE 102 de manera que la MME 106 puede ayudar a la red de servicio 112 a completar la conexión del UE 102 de manera que pueda utilizar la conectividad patrocinada por el proveedor de servicios de aplicaciones alojado por el servidor 116.

[0158] En el paso 864, la MME 106 recibe el perfil de usuario solicitado después de que el servidor 116 analiza la petición y el token de acceso incluido en la petición en el paso 862. Como resultado, el UE 102 se conecta a la red de servicio 112 sin proporcionar una credencial preexistente (p. ej., Contraseña, contraseña de función hash o token de acceso previamente almacenado en el UE 102, etc.) en la petición de conexión.

[0159] La información y las señales se pueden representar utilizando cualquiera de diversas tecnologías y técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips que puedan haberse mencionado a lo largo de la descripción anterior pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos o cualquier combinación de los mismos.

[0160] Los diversos bloques ilustrativos y módulos descritos en relación con la divulgación del presente documento se pueden implementar o realizar con un procesador de propósito general, un DSP, un ASIC, una FPGA u otro dispositivo lógico programable, puerta discreta o lógica de transistores, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de uso general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos (*por ejemplo*, una combinación de un DSP y un microprocesador, múltiples microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de ese tipo).

[0161] Las funciones descritas en el presente documento se pueden implementar en hardware, software ejecutado por un procesador, firmware, o cualquier combinación de los mismos. Si se implementan en software ejecutado por un procesador, las funciones, como una o más instrucciones o código, pueden ser almacenadas en, o transmitidas por, un medio legible por ordenador. Otros ejemplos e implementaciones están dentro del alcance de la divulgación y de las reivindicaciones adjuntas. Por ejemplo, debido a la naturaleza del software, las funciones que se han descrito anteriormente se pueden implementar utilizando software ejecutado por un procesador, hardware, firmware, cableado o combinaciones de cualquiera de estos. Las características que implementan funciones también pueden estar localizadas físicamente en diversas posiciones, incluyendo el estar distribuidas de manera que se implementen partes de funciones en diferentes ubicaciones físicas.

[0162] Además, como se usa en el presente documento, incluyendo en las reivindicaciones, "o" como se usa en una lista de artículos (por ejemplo, una lista de artículos anticipados por una frase tal como "al menos uno de" o "uno o más de") indica una lista inclusiva de tal forma que, por ejemplo, una lista de [al menos uno de A, B o C] se refiere a o B o C o AB o AC o BC o ABC (es decir A y B y C). También se contempla que las características, componentes, acciones y/o pasos descritos con respecto a un modo de realización pueden estructurarse en un orden diferente al que se presenta en el presente documento y/o combinarse con las características, componentes, acciones y/o pasos descritos con respecto a otros modos de realización de la presente divulgación.

[0163] Los modos de realización de la presente divulgación incluyen un equipo de usuario (UE) para acceder a un servicio que comprende medios para identificar una red de servicio a través de la cual un servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio; medios para enviar una petición de conexión a la red de servicio con un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de

servicios de aplicaciones, con el token de cliente no reconocible como una credencial de acceso celular a la red de servicio; y medios para autentificarse en la red de servicio a través del servidor de proveedor de servicios de aplicaciones para el acceso patrocinado al servicio basado en la credencial preexistente.

[0164] El equipo de usuario incluye además medios para incluir, en la petición de conexión, una identificación de tipo de autentificación usada por el UE para la autentificación de utilizar el acceso patrocinado al servicio. El UE incluye además medios para incluir, en la petición de conexión, información que identifica cómo localizar el servidor de proveedor de servicios de aplicaciones. El UE incluye además el hecho de que la credencial preexistente se basa en una contraseña establecida con el servidor de proveedor de servicios de aplicaciones generado a través de un canal fuera de banda, que además comprende medios para incluir, con la petición de conexión, un nombre de usuario asociado con la contraseña y el servidor de proveedor de servicios de aplicaciones; medios para generar un hash de la contraseña con un primer valor para generar la credencial preexistente; y medios para generar un hash de la credencial preexistente con un segundo valor para generar el token de cliente que se envía desde el UE en la petición de conexión. El UE incluye además medios para recibir, en el UE, un token de autentificación desde el servidor de proveedor de servicios de aplicaciones a través de la red de servicio, en el que la red de servicio almacena una clave determinada por el servidor de proveedor de servicios de aplicaciones basándose en la credencial preexistente; medios para validar el token de autentificación; y medios para determinar, en respuesta a la validación, una clave basada en el UE basada en la credencial de contraseña intermedia generada por el UE. El UE incluye además en el que el token del cliente se incluye como una prueba de la credencial preexistente, y en el que la credencial preexistente se establece entre el UE y el servidor de proveedor de servicios de aplicaciones antes de enviar la petición de conexión. El UE incluye además medios para realizar, después del envío, un handshake entre el UE y el servidor de proveedor de servicios de aplicaciones para acordar una clave secreta compartida; medios para determinar una clave base basada en la clave secreta compartida que es válida durante una sesión de autentificación entre el UE y el servidor de proveedor de servicios de aplicaciones; y medios para validar la información de autentificación recibida en respuesta a la petición de conexión después del handshake basado en la clave base. El UE incluye además medios para recibir un anuncio del acceso patrocinado desde la red de servicio. El UE incluye además medios para autorizar a un elemento de red de la red de servicio a recuperar, desde el servidor de proveedor de servicios de aplicaciones, un perfil de usuario asociado con la credencial preexistente. El UE incluye además en el que el UE funciona sin una tarjeta de módulo de identidad de abonado (SIM).

[0165] Los modos de realización de la presente divulgación incluyen además un servidor de proveedor de servicios de aplicaciones que patrocina el acceso a un servicio que comprende medios para recibir, desde una red de servicio intermedio a través de la cual el servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio, una petición de información de autentificación basada en una petición de conexión de un equipo de usuario (UE), la petición de información de autentificación que comprende un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones y que no es reconocible como una credencial de acceso celular a la red de servicio; medios para determinar la información de autentificación basada en la credencial preexistente a la que puede acceder el servidor de proveedor de servicios de aplicaciones en respuesta a la petición de información de autentificación; y medios para transmitir la información de autentificación en una respuesta a la red de servicio, en el que la información de autentificación ayuda en la autentificación entre el UE y la red de servicio para el acceso patrocinado al servicio basado en la credencial preexistente.

[0166] El proveedor de servicios de aplicaciones incluye, además, en el que la credencial preexistente se basa en una contraseña establecida con el servidor de proveedor de servicios de aplicaciones generado a través de un canal fuera de banda y la petición de información de autentificación incluye un nombre de usuario asociado con la contraseña y el servidor de proveedor de servicios de aplicaciones, que comprende además medios para verificar el nombre de usuario y el token del cliente basándose en uno o más registros accesibles por el servidor de proveedor de servicios de aplicaciones, en el que el token del cliente comprende la credencial preexistente con hash con un primer valor y la credencial existente comprende la contraseña con hash con un segundo valor. El proveedor de servicios de aplicaciones incluye además medios para generar un vector de autentificación que comprende una clave compartida, un token de autentificación y una respuesta esperada basada en la credencial preexistente. El proveedor de servicios de aplicaciones incluye además medios para proporcionar el token de cliente al UE para que el UE lo utilice como prueba de poseer la credencial preexistente antes de recibir la petición de información de autentificación. El proveedor de servicios de aplicaciones incluye además medios para aceptar, después de la recepción, una clave secreta compartida basada en un handshake entre el UE y el servidor de proveedor de servicios de aplicaciones; medios para determinar una clave base basándose en la clave secreta compartida; y medios para generar un vector de autentificación que comprende la clave base, un token de autentificación y una respuesta esperada basada en la credencial preexistente. El proveedor de servicios de aplicaciones incluye además medios para proporcionar un perfil de usuario asociado con la credencial preexistente a un elemento de red desde la red de servicio basándose en una autorización del UE para que el elemento de red acceda al perfil de usuario en nombre del UE. El proveedor de servicios de aplicaciones incluye además medios para establecer un acuerdo de nivel de servicio entre el servidor de proveedor de servicios de aplicaciones y la red de servicio, en el que, en respuesta al acuerdo de nivel de servicio, la red de servicio anuncia el acceso patrocinado a los dispositivos disponibles. El proveedor de servicios de aplicaciones incluye además en el que el UE completa la autentificación entre el UE y la red de servicio y utiliza el acceso patrocinado, que comprende además medios para recibir, desde la red de servicio, un cargo asociado con el acceso patrocinado al servicio por el UE en el red de servicio. El proveedor de servicios de aplicaciones incluye además

medios para proporcionar, antes de recibir la petición de información de autentificación, una lista de redes de servicio fiables para el UE. El proveedor de servicios de aplicaciones incluye además en el que la red de servicio que interviene comprende una red de núcleo de paquete evolucionado (EPC) y el servidor de proveedor de servicios de aplicaciones es parte de una red de datos externa a la red de EPC.

[0167] Como los expertos en esta técnica ahora apreciarán y dependiendo de la aplicación particular en cuestión, se pueden hacer muchas modificaciones, sustituciones y variaciones en y a los materiales, aparatos, configuraciones y procedimientos de uso de los dispositivos de la presente divulgación sin apartarse del ámbito de la misma. A la luz de esto, el alcance de la presente divulgación no debe limitarse al de los modos de realización particulares ilustrados y descritos en el presente documento, ya que son simplemente a modo de ejemplo, sino que, más bien, debe ser totalmente proporcional al de las reivindicaciones adjuntas a continuación.

REIVINDICACIONES

1. Un procedimiento para acceder a un servicio, que comprende:

identificar (702), mediante un equipo de usuario, UE, una red a través de la cual un servidor de proveedor de servicios de aplicaciones permite el acceso al servicio;

enviar (710), desde el UE, una petición de conexión a la red con un token de cliente basado en una credencial preexistente asociada con el UE y establecida con el servidor de proveedor de servicios de aplicaciones, con el token del cliente que no es reconocible como una credencial de acceso celular a la red y

autentificar, mediante el UE, a la red a través del servidor de proveedor de servicios de aplicaciones para el acceso patrocinado al servicio basado en la credencial preexistente.

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

incluir, en la petición de conexión, una identificación del tipo de autentificación utilizada por el UE para la autentificación para utilizar el acceso patrocinado al servicio,

en el que el envío comprende además incluir, en la petición de conexión, información que identifica cómo localizar al proveedor de servicios de aplicaciones.

3. El procedimiento de la reivindicación 1, en el que la credencial preexistente se basa en una contraseña establecida con el servidor de proveedor de servicios de aplicaciones generado a través de un canal fuera de banda, con el envío que comprende además:

incluir, con la petición de conexión, un nombre de usuario asociado con la contraseña y el servidor de proveedor de servicios de aplicaciones;

generar un hash (706), mediante el UE, de la contraseña con un primer valor para generar la credencial preexistente; y

generar un hash (708), mediante el UE, de la credencial preexistente con un segundo valor para generar el token de cliente que se envía desde el UE en la petición de conexión.

4. El procedimiento de acuerdo con la reivindicación 3, que comprende además:

recibir (718), en el UE, un token de autentificación del servidor de proveedor de servicios de aplicaciones a través de la red, en el que la red almacena información de autentificación que comprende una clave de sesión determinada por el servidor de proveedor de servicios de aplicaciones basándose en la credencial preexistente, con la clave de sesión que permite que la red se autentifique con el UE;

validar (720), mediante el UE, el token de autentificación; y

en respuesta a la validación, determinar una clave basada en el UE basada en la credencial de contraseña intermedia generada por el UE.

5. El procedimiento según la reivindicación 1, en el que el envío (710) comprende además:

incluir el token del cliente como prueba de poseer la credencial preexistente, en el que la credencial preexistente se establece entre el UE y el servidor de proveedor de servicios de aplicaciones antes de enviar la petición de conexión.

6. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

realizar (714), después del envío, un handshake o establecimiento de comunicación entre el UE y el servidor de proveedor de servicios de aplicaciones para acordar una clave secreta compartida;

determinar (716), mediante el UE, una clave base basada en la clave secreta compartida que es válida durante la duración de una sesión de autentificación entre el UE y el servidor de proveedor de servicios de aplicaciones; y

validar, mediante el UE, la información de autentificación recibida en respuesta a la petición de conexión después del handshake basado en la clave base, y/o

autorizar un elemento de red de la red para recuperar, desde el servidor de proveedor de servicios de aplicaciones, un perfil de usuario asociado con la credencial preexistente.

7. El procedimiento, de acuerdo con la reivindicación 1, en el que se aplica al menos una de las siguientes condiciones al UE:

carece de una suscripción a un proveedor de servicios celulares; y

funciona sin tarjeta de módulo de identidad de abonado, SIM.

8. Un procedimiento para habilitar el acceso a un servicio patrocinado mediante un servidor de proveedor de servicios de aplicaciones, que comprende:

recibir, desde una red intermedia a través de la cual el servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio, una petición de información de autentificación basada en una petición de conexión de un equipo de usuario, UE, la petición de información de autentificación que comprende un token de cliente basado en una credencial preexistente asociada con el UE y establecida con el servidor de proveedor de servicios de aplicaciones, con el token del cliente que no es reconocible como una credencial de acceso celular a la red;

determinar, mediante el servidor de proveedor de servicios de aplicaciones, la información de autentificación basada en la credencial preexistente a la que puede acceder el servidor de proveedor de servicios de aplicaciones en respuesta a la petición de información de autentificación; y

transmitir, desde el servidor de proveedor de servicios de aplicaciones, la información de autentificación en una respuesta a la red, en el que la información de autentificación sirve para facilitar la autentificación entre el UE y la red para el acceso patrocinado al servicio basado en la credencial preexistente.

9. El procedimiento de la reivindicación 8, en el que la credencial preexistente se basa en una contraseña establecida con el servidor de proveedor de servicios de aplicaciones generado a través de un canal fuera de banda y la petición de información de autentificación incluye un nombre de usuario asociado con la contraseña y el servidor de proveedor de servicios de aplicaciones, con la determinación que comprende además:

verificar, mediante el servidor de proveedor de servicios de aplicaciones, el nombre de usuario y el token del cliente basándose en uno o más registros accesibles por el servidor de proveedor de servicios de aplicaciones, en el que el token del cliente comprende la credencial preexistente con hash con un primer valor y la credencial preexistente comprende la contraseña con función hash con un segundo valor.

10. El procedimiento de acuerdo con la reivindicación 9, que comprende además:

generar, mediante el servidor de proveedor de servicios de aplicaciones, un vector de autentificación que comprenda una clave compartida, un token de autentificación y una respuesta esperada basada en la credencial preexistente.

11. El procedimiento según la reivindicación 8, en el que la recepción comprende además:

proporcionar, mediante el servidor de proveedor de servicios de aplicaciones, el token del cliente al UE para que el UE lo utilice como prueba de poseer la credencial preexistente antes de recibir la petición de información de autentificación.

12. El procedimiento de acuerdo con la reivindicación 8, que comprende además:

acordar, después de la recepción, una clave secreta compartida basada en un handshake entre el UE y el servidor de proveedor de servicios de aplicaciones;

determinar, mediante el servidor de proveedor de servicios de aplicaciones, una clave base basada en la clave secreta compartida; y

generar, mediante el servidor de proveedor de servicios de aplicaciones, un vector de autentificación que comprenda la clave base, un token de autentificación y una respuesta esperada basada en la credencial preexistente, y/o.

proporcionar, antes de recibir la petición de información de autentificación, una lista de redes fiables para el UE.

13. Un equipo de usuario, UE, para acceder a un servicio, que comprende:

un transceptor configurado para:

ayudar a identificar (702) una red a través de la cual un servidor de proveedor de servicios de aplicaciones permite el acceso al servicio; y

enviar (710) una petición de conexión a la red con un token de cliente basado en una credencial preexistente asociada con el UE y establecida con el servidor de proveedor de servicios de aplicaciones, con el token del cliente que no es reconocible como una credencial de acceso celular a la red; y

un procesador configurado para autentificarse en la red a través del servidor de proveedor de servicios de aplicaciones para el acceso patrocinado al servicio basado en la credencial preexistente.

14. Un servidor de proveedor de servicios de aplicaciones que patrocina el acceso a un servicio, que comprende:

un transceptor configurado para recibir, desde una red intermedia a través de la cual el servidor de proveedor de servicios de aplicaciones patrocina el acceso al servicio, una petición de información de autentificación basada en una petición de conexión de un equipo de usuario, UE, con la petición de información de autentificación que comprende un token de cliente basado en una credencial preexistente establecida con el servidor de proveedor de servicios de aplicaciones y no reconocible como credencial de acceso celular a la red; y

un procesador configurado para determinar la información de autentificación basada en la credencial preexistente accesible por el servidor de proveedor de servicios de aplicaciones en respuesta a la petición de información de autentificación,

en el que el transceptor está configurado además para transmitir la información de autentificación en una respuesta a la red, y

en el que la información de autentificación facilita la autentificación entre el UE y la red para el acceso patrocinado al servicio basado en la credencial preexistente.

15. Un medio legible por ordenador que tiene un código de programa grabado en el mismo, con el código de programa que comprende un código para realizar el procedimiento de cualquiera de las reivindicaciones 1 a 12.

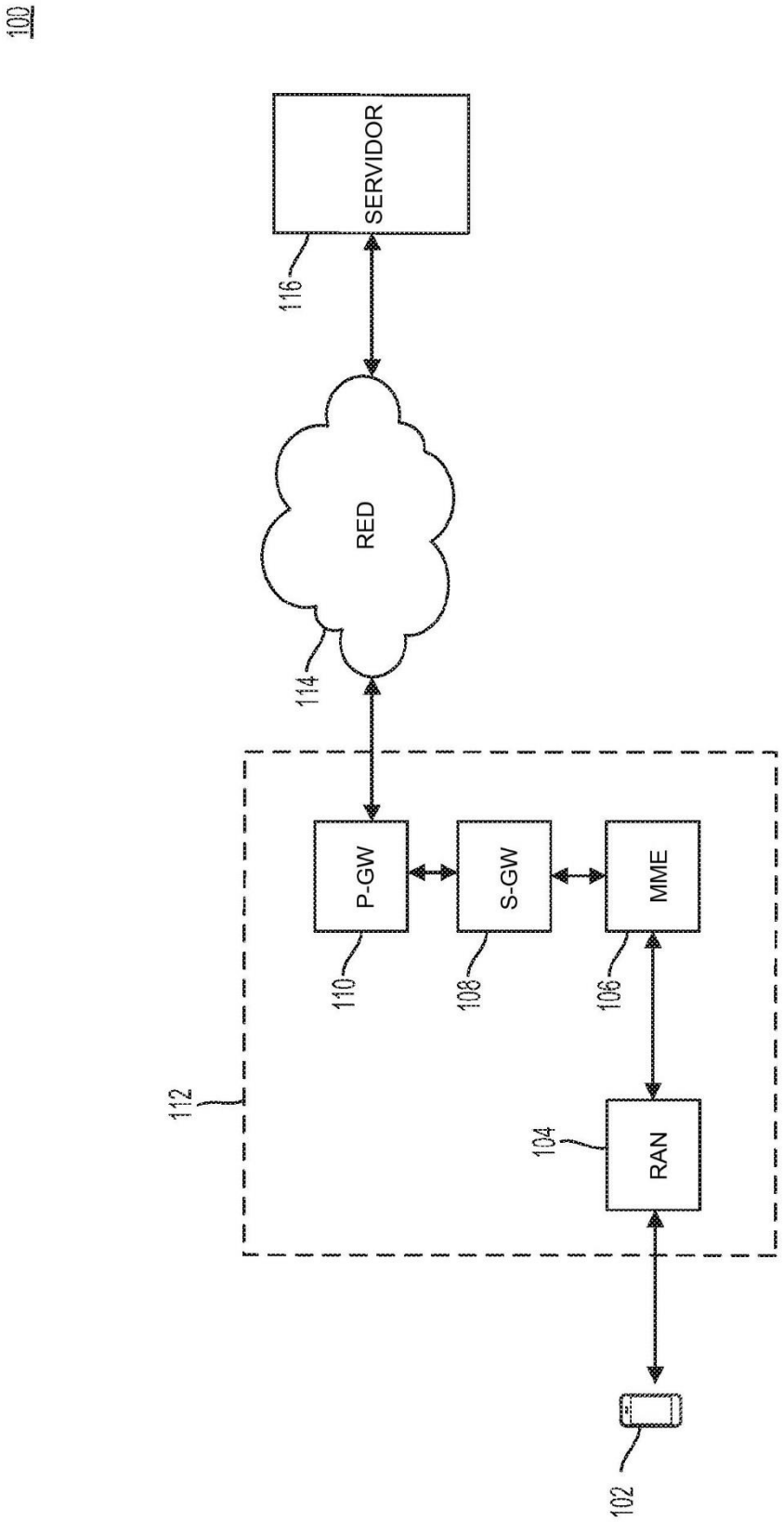
100
SERVIDOR
116
RED
114
112
P-GW
S-GW
MME
110
108
106
104
RAN
102

FIG. 1

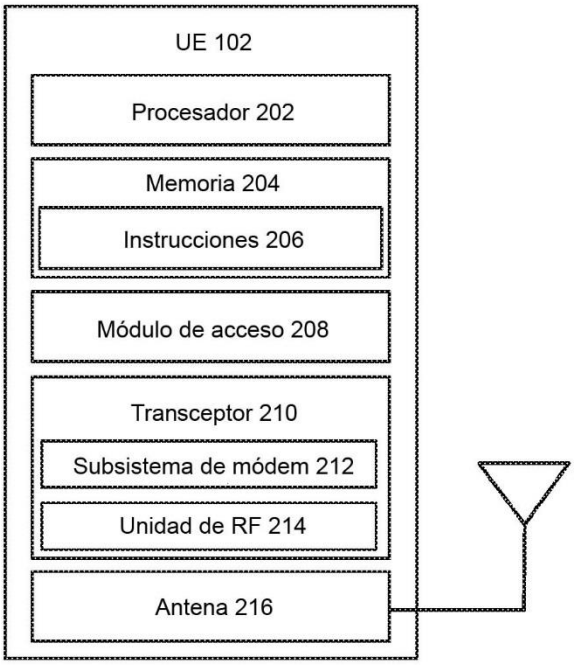
UE 102
Procesador 202
Memoria 204
Instrucciones 206
Módulo de acceso 208
Transceptor 210
Subsistema de módem 212
Unidad de RF 214
Antena 216

FIG. 2

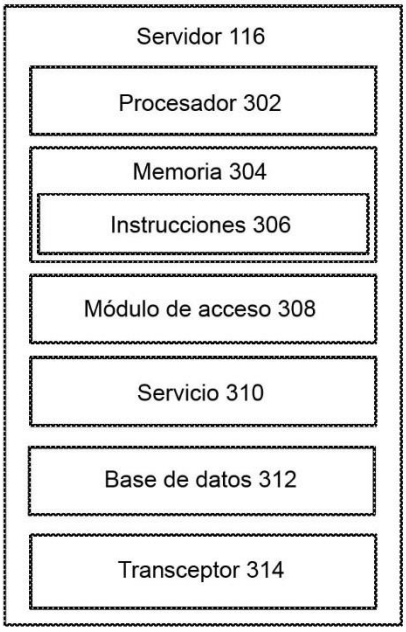
Servidor 116
Procesador 302
Memoria 304
Instrucciones 306
Módulo de acceso 308
Servicio 310
Base de datos 312
Transceptor 314

FIG. 3

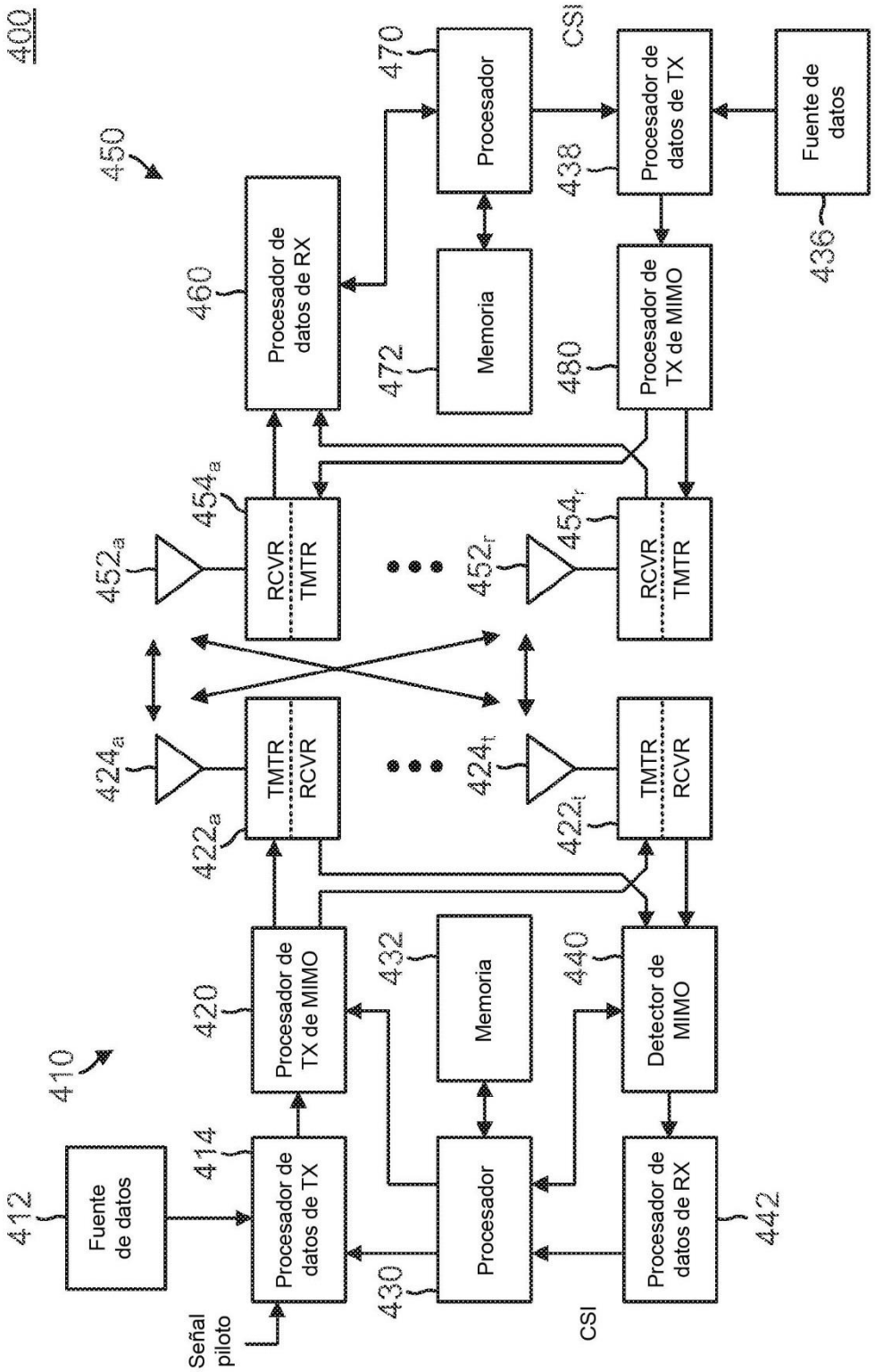
400
450
410
Fuente de datos
412
Procesador de datos de TX
414
Procesador de TX de MIMO
420
TMTR RCVR
422a
424a
RCVR TMTR
454a
452a
Procesador de datos de RX
460
Procesador
470
Memoria
472
Procesador de TX de MIMO
480
Procesador de datos de TX
438
CSI
Fuente de datos
436
Señal piloto
Procesador
430
Memoria
432
Procesador de datos de RX
442
Detector de MIMO
440
TMTR RCVR
422t
424t
RCVR TMTR
454r
452r
CSI

FIG. 4

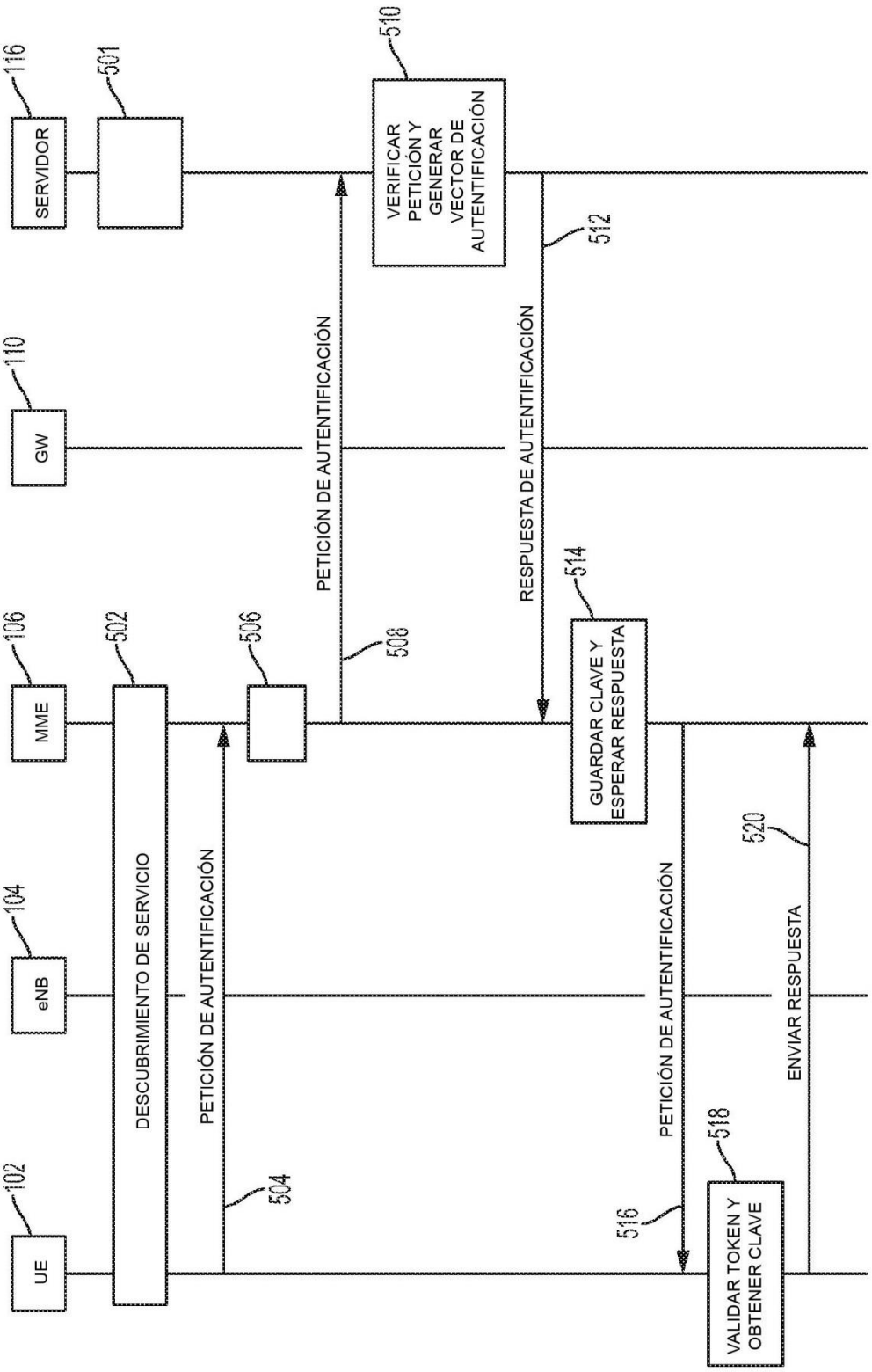
UE
102
eNB
104
MME
106
GW
110
SERVIDOR
116
DESCUBRIMIENTO DE SERVICIO
502
501
PETICIÓN DE AUTENTIFICACIÓN
504
506
PETICIÓN DE AUTENTIFICACIÓN
508
VERIFICAR PETICIÓN Y GENERAR VECTOR DE AUTENTIFICACIÓN
510
RESPUESTA DE AUTENTIFICACIÓN
512
GUARDAR CLAVE Y ESPERAR RESPUESTA
514
PETICIÓN DE AUTENTIFICACIÓN
516
VALIDAR TOKEN Y OBTENER CLAVE
518
ENVIAR RESPUESTA
520

FIG. 5

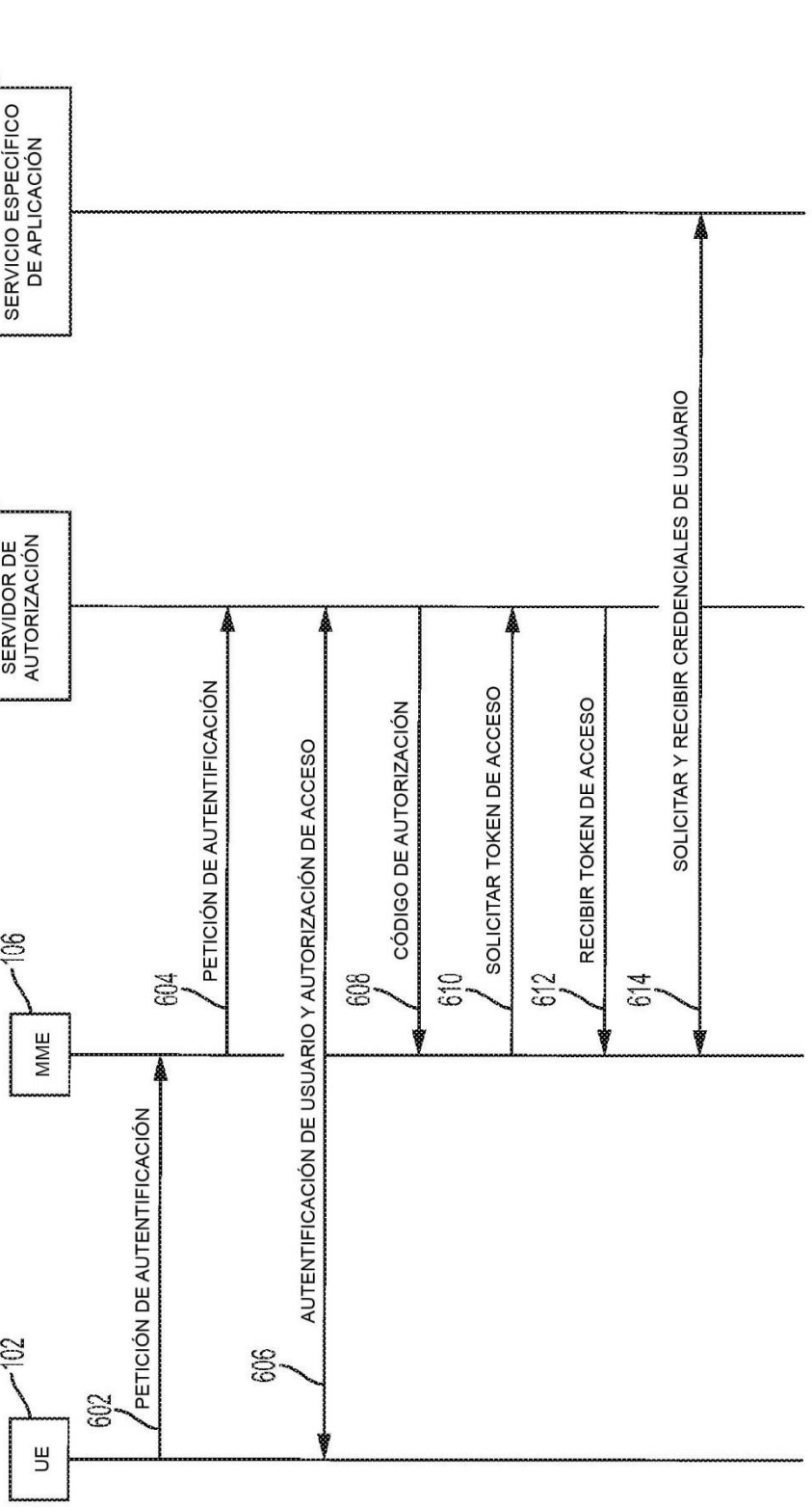
UE
102
MME
106
SERVIDOR DE AUTORIZACIÓN
120
SERVICIO ESPECÍFICO DE APLICACIÓN
116
602
PETICIÓN DE AUTENTIFICACIÓN
604
PETICIÓN DE AUTENTIFICACIÓN
606
AUTENTIFICACIÓN DE USUARIO Y AUTORIZACIÓN DE ACCESO
608
CÓDIGO DE AUTORIZACIÓN
610
SOLICITAR TOKEN DE ACCESO
612
RECIBIR TOKEN DE ACCESO
614
SOLICITAR Y RECIBIR CREDENCIALES DE USUARIO

FIG. 6

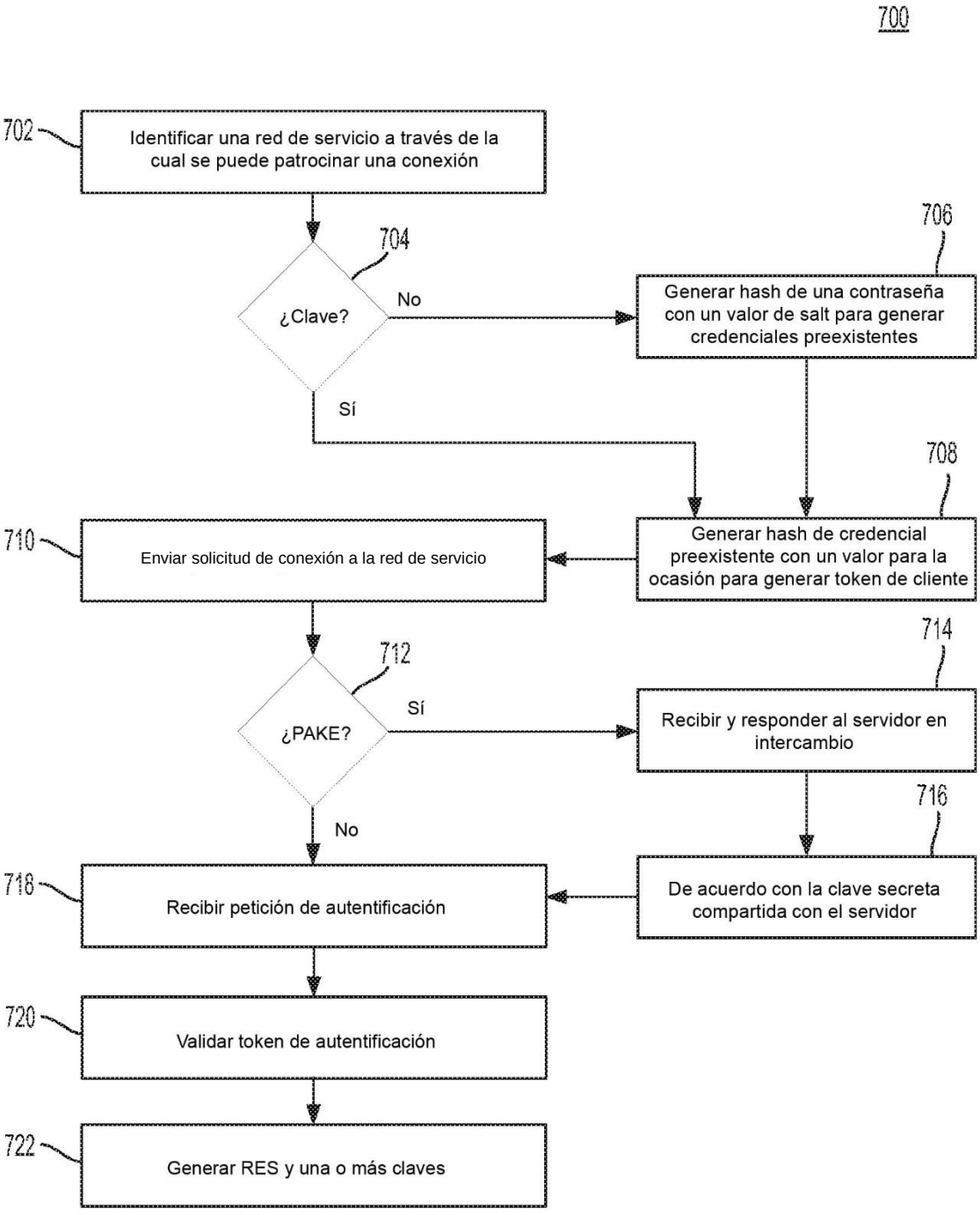
700
702
Identificar una red de servicio a través de la cual se puede patrocinar una conexión
704
¿Clave?
No
706
Generar hash de una contraseña con un valor de salt para generar credenciales preexistentes
Sí
708
Generar hash de credencial preexistente con un valor para la ocasión para generar token de cliente
710
Enviar solicitud de conexión a la red de servicio
712
¿PAKE?
Sí
714
Recibir y responder al servidor en intercambio
No
716
De acuerdo con la clave secreta compartida con el servidor
718
Recibir petición de autentificación
720
Validar token de autentificación
722
Generar RES y una o más claves

FIG. 7A

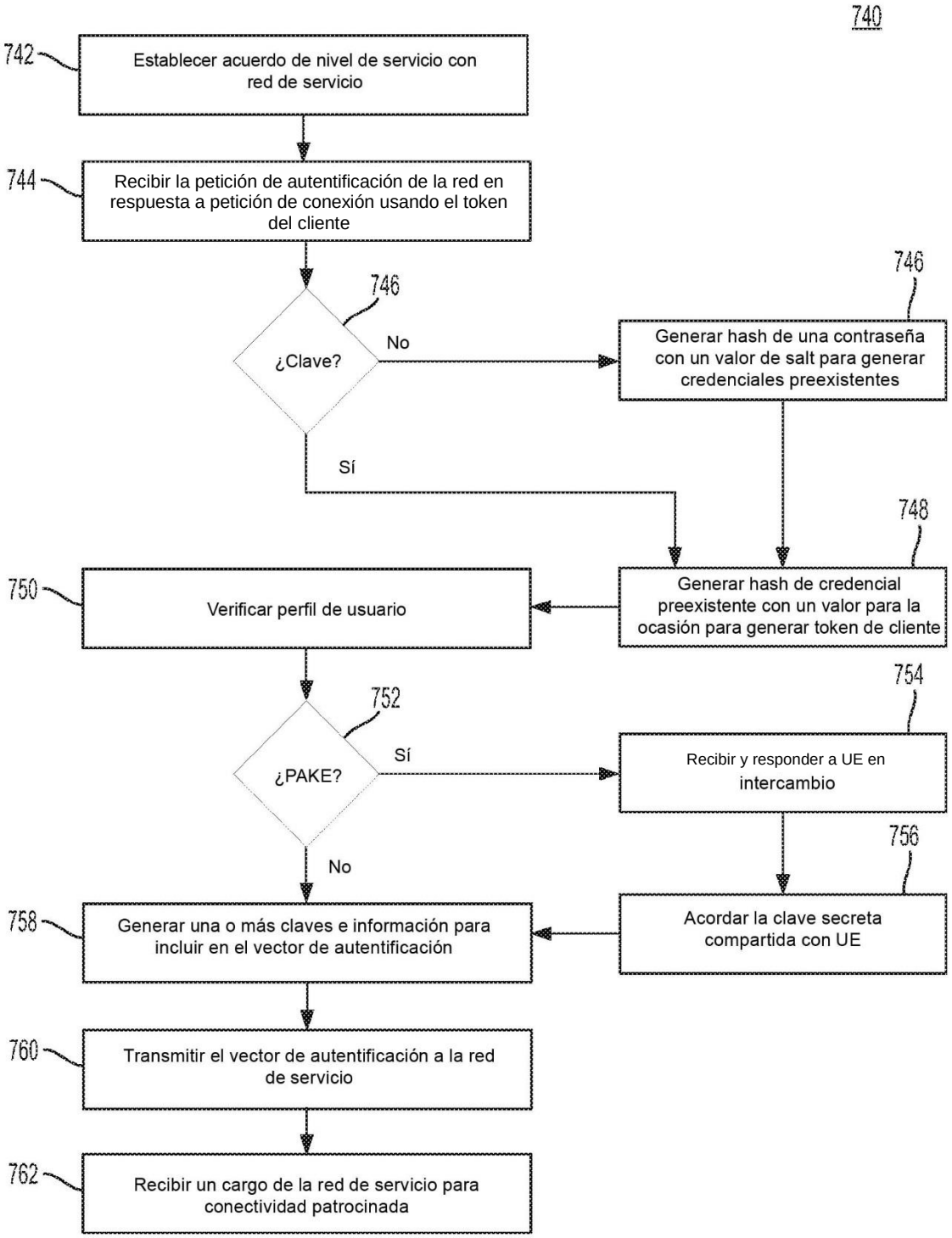
740
742
Establecer acuerdo de nivel de servicio con red de servicio
744
Recibir la petición de autentificación de la red en respuesta a petición de conexión usando el token del cliente
746
¿Clave?
No
746
Generar hash de una contraseña con un valor de salt para generar credenciales preexistentes
Sí
748
Generar hash de credencial preexistente con un valor para la ocasión para generar token de cliente
750
Verificar perfil de usuario
752
¿PAKE?
Sí
754
Recibir y responder a UE en intercambio
No
756
Acordar la clave secreta compartida con UE
758
Generar una o más claves e información para incluir en el vector de autentificación
760
Transmitir el vector de autentificación a la red de servicio
762
Recibir un cargo de la red de servicio para conectividad patrocinada

FIG. 7B

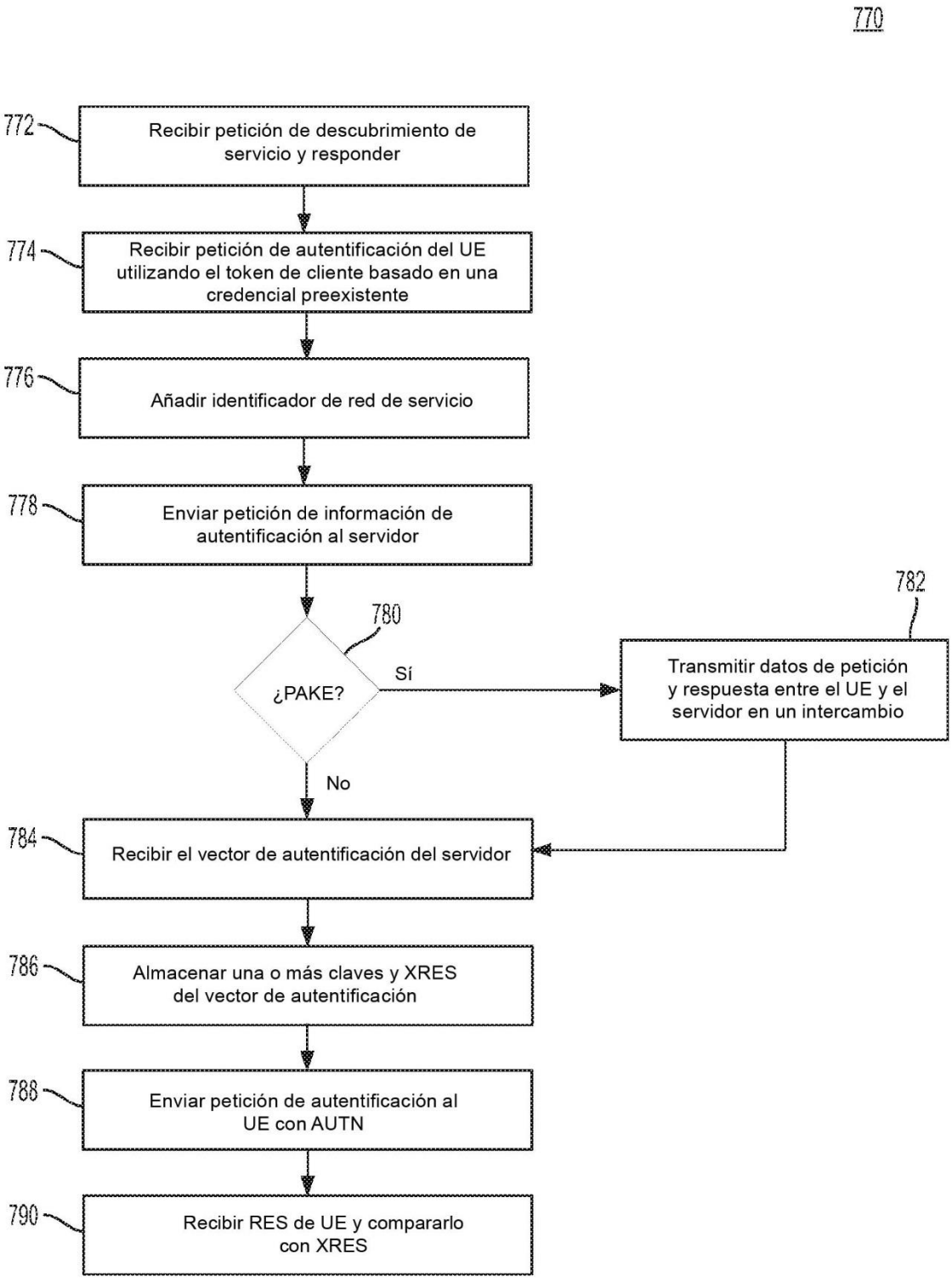
770
772
Recibir petición de descubrimiento de servicio y responder
774
Recibir petición de autentificación del UE utilizando el token de cliente basado en una credencial preexistente
776
Añadir identificador de red de servicio
778
Enviar petición de información de autentificación al servidor
780
¿PAKE?
Sí
No
782
Transmitir datos de petición y respuesta entre el UE y el servidor en un intercambio
784
Recibir el vector de autentificación del servidor
786
Almacenar una o más claves y XRES del vector de autentificación
788
Enviar petición de autentificación al UE con AUTN
790
Recibir RES de UE y compararlo con XRES

FIG. 7C

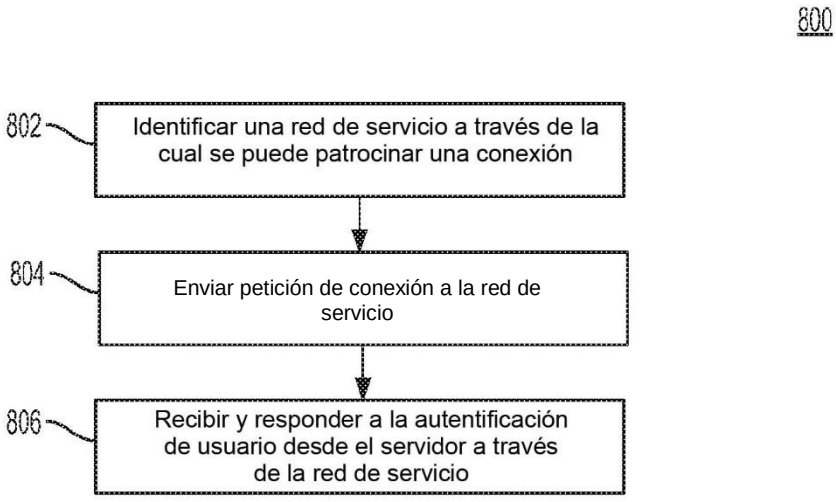
800
802
Identificar una red de servicio a través de la cual se puede patrocinar una conexión
804
Enviar petición de conexión a la red de servicio
806
Recibir y responder a la autentificación de usuario desde el servidor a través de la red de servicio

FIG. 8A

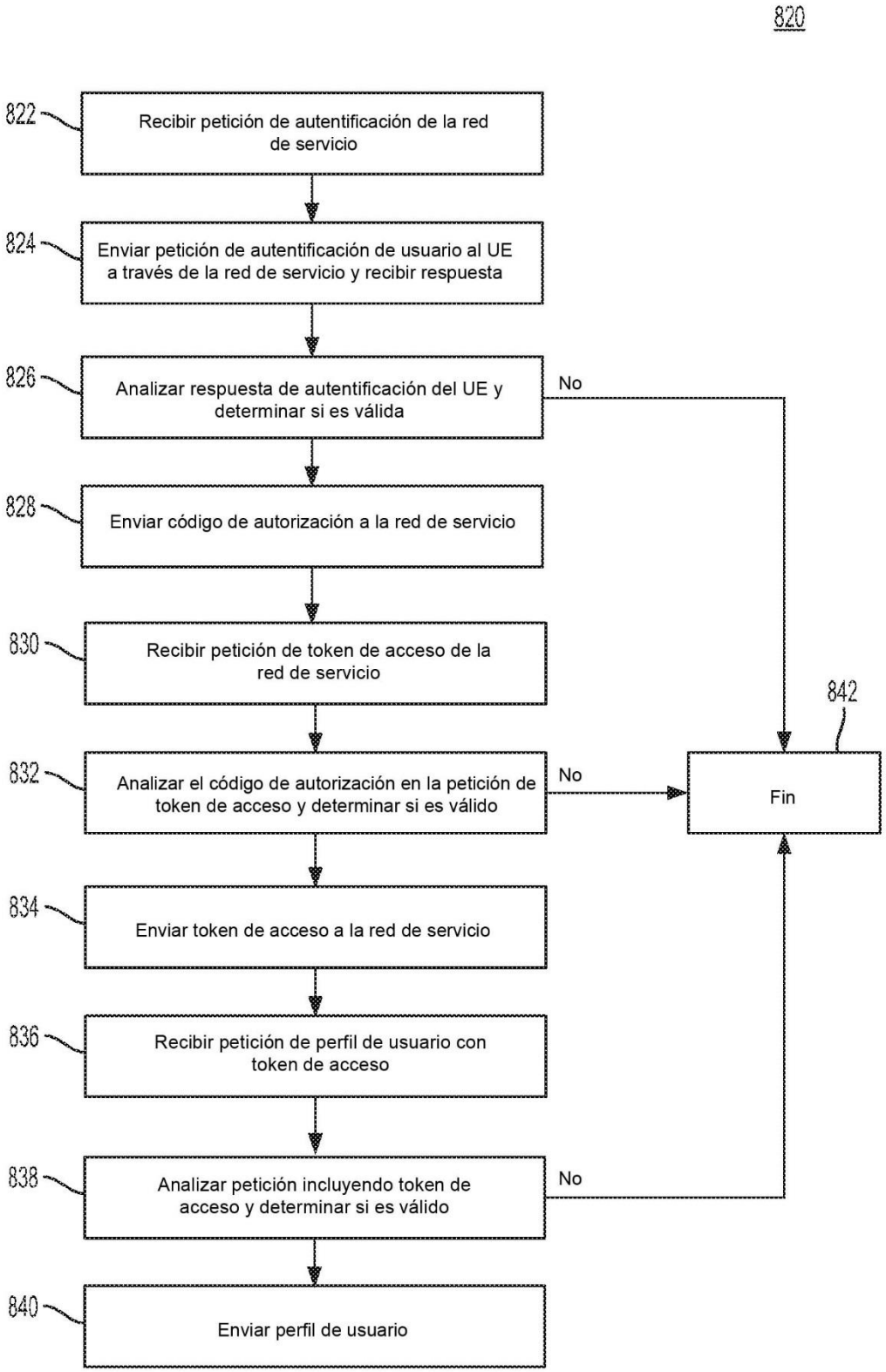
820
822
Recibir petición de autentificación de la red de servicio
824
Enviar petición de autentificación de usuario al UE a través de la red de servicio y recibir respuesta
826
Analizar respuesta de autentificación del UE y determinar si es válida
No
828
Enviar código de autorización a la red de servicio
830
Recibir petición de token de acceso de la red de servicio
842
832
Analizar el código de autorización en la petición de token de acceso y determinar si es válido
No
Fin
834
Enviar token de acceso a la red de servicio
836
Recibir petición de perfil de usuario con token de acceso
838
Analizar petición incluyendo token de acceso y determinar si es válido
No
840
Enviar perfil de usuario

FIG. 8B

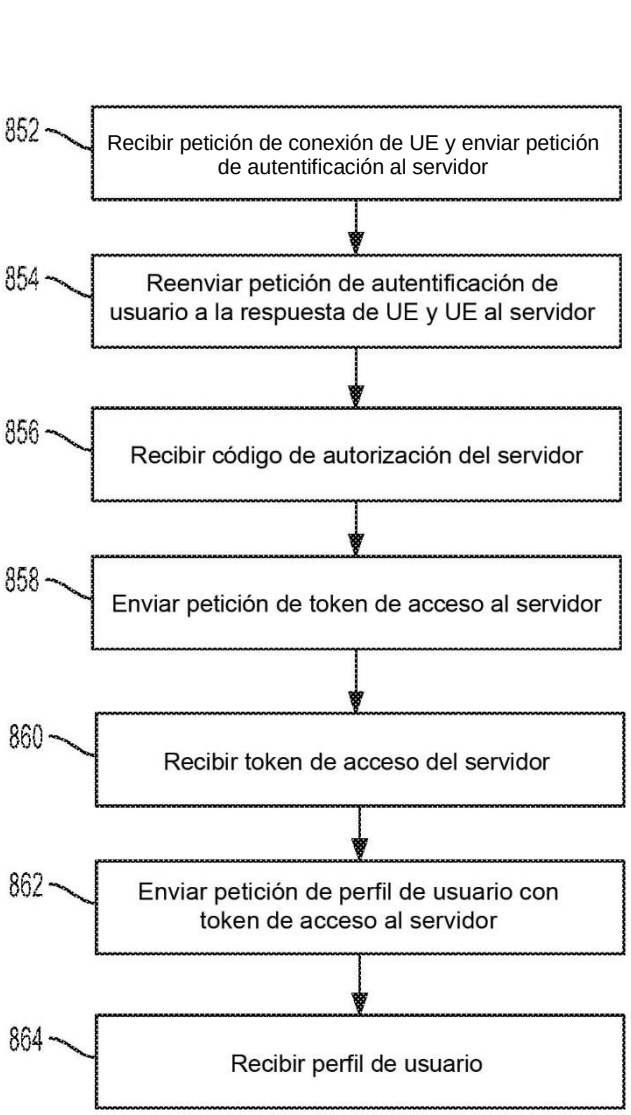
850
852
Recibir petición de conexión de UE y enviar petición de autentificación al servidor
854
Reenviar petición de autentificación de usuario a la respuesta de UE y UE al servidor
856
Recibir código de autorización del servidor
858
Enviar petición de token de acceso al servidor
860
Recibir token de acceso del servidor
862
Enviar petición de perfil de usuario con token de acceso al servidor
864
Recibir perfil de usuario

FIG. 8C