(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 894 476**

(51) Int. CI.:

H04W 12/06 (2011.01)
H04L 29/06 (2006.01)
H04W 12/04 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.08.2017 PCT/US2017/047355**

(87) Fecha y número de publicación internacional: **22.03.2018 WO18052640**

(96) Fecha de presentación y número de la solicitud europea: **17.08.2017 E 17761379 (1)**

(97) Fecha y número de publicación de la concesión europea: **15.09.2021 EP 3516894**

(54) Título: **Técnicas para derivar claves de seguridad para una red celular basándose en la realización de un procedimiento de protocolo de autenticación extensible (EAP)**

(30) Prioridad:

19.09.2016 US 201662396791 P
17.04.2017 US 201715489670

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.02.2022

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

LEE, SOO BUM;
PALANIGOUNDER, ANAND y
ESCOTT, ADRIAN EDWARD

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Técnicas para derivar claves de seguridad para una red celular basándose en la realización de un procedimiento de protocolo de autenticación extensible (EAP)

ANTECEDENTES

CAMPO DE LA DIVULGACIÓN

La presente divulgación se refiere, por ejemplo, a sistemas de comunicación inalámbricos y, más particularmente, a técnicas para derivar claves de seguridad para una red celular basadas en el rendimiento de un procedimiento de protocolo de autenticación extensible (EAP).

DESCRIPCIÓN DE TÉCNICA RELACIONADA

Los sistemas de comunicación inalámbricos se utilizan ampliamente para proporcionar diversos tipos de contenido de comunicación, tales como voz, video, paquetes de datos, mensajería, difusión, etc. Estos sistemas pueden ser sistemas de acceso múltiple capaces de soportar comunicación con múltiples usuarios por compartición de los recursos del sistema disponibles (por ejemplo, tiempo, frecuencia y energía). Algunos ejemplos de tales sistemas de acceso múltiple incluyen sistemas de acceso múltiple por división de código (CDMA), sistemas de acceso múltiple por división de tiempo (TDMA), sistemas de acceso múltiple por división de frecuencia (FDMA) y sistemas de acceso múltiple por división de frecuencia ortogonal (OFDMA).

En algunos ejemplos, un sistema de comunicación inalámbrico de acceso múltiple puede ser o incluir una red celular. Una red celular puede incluir una diversidad de dispositivos de acceso a red, soportando cada uno simultáneamente la comunicación para múltiples dispositivos de comunicación, conocidos de otro modo como equipos de usuario (UE). En una red de cuarta generación (4G), una red de Evolución a Largo Plazo (Long-Term Evolution, LTE) o una red LTE Avanzada (LTE-Advanced, LTE-A), los dispositivos de acceso a red pueden adoptar la forma de NodeB mejorados (eNB), incluyendo cada eNB un conjunto de una o más estaciones base. En una red de quinta generación (5G o NextGen), los dispositivos de acceso a la red pueden adoptar la forma de cabezales de radio inteligentes (SRH) o gNodeB (gNB) en comunicación con controladores de dispositivo de acceso a red (por ejemplo, controladores de nodo de acceso (ANC)), en los que un conjunto de uno o más dispositivos de acceso a red, en comunicación con un controlador de dispositivo de acceso a red, definen un nodo de red. Un eNB, gNB o nodo de red puede comunicarse con un conjunto de UE en canales de enlace descendente (por ejemplo, para transmisiones desde el eNB, gNB o nodo de red a los UE) y canales de enlace ascendente (por ejemplo, para transmisiones desde los UE a los eNB, gNB o nodos de red).

Cuando un UE accede a una red celular, el UE o la red celular pueden iniciar uno o más procedimientos que permiten que el UE se autentique ante un autenticador de la red celular, y que permiten que el autenticador autentique la red celular ante el UE. En algunos ejemplos, los procedimientos de autenticación pueden incluir un procedimiento de EAP, en el que un servidor de autenticación que tiene una conexión segura con el autenticador autentica el UE; permite que el UE derive una o más claves de seguridad para autenticarse ante el autenticador; y deriva una o más claves de seguridad que se transmiten al autenticador a través de la conexión segura, para permitir que el autenticador autentique la red celular ante el UE.

El documento de Patente US 2016/127903 A1 desvela sistemas, métodos y medios legibles por computadora para autenticar un dispositivo. En algunos aspectos, un método incluye determinar, usando un segundo dispositivo, una clave compartida con el primer dispositivo, generando, mediante el segundo dispositivo, una primera clave maestra por pares (PMK) basada en la clave compartida con el primer dispositivo. El método también puede incluir generar, mediante el segundo dispositivo, una segunda clave maestra por pares (PMK) para un primer punto de acceso basada en la primera clave maestra por pares, y una o más propiedades del primer punto de acceso. A continuación, el método transmite la segunda clave maestra por pares al primer punto de acceso. El primer punto de acceso puede usar la segunda clave maestra por pares para facilitar comunicación segura con el primer dispositivo. Por ejemplo, el primer punto de acceso puede codificar/encriptar y/o decodificar/desencriptar mensajes intercambiados con el primer dispositivo basándose en la segunda clave maestra por pares.

El documento de Patente WO 2009/087006 A1 describe un mecanismo para autenticación y autorización de acceso a red que usa un método de autenticación basado, por ejemplo, en el protocolo de autenticación extensible (EAP). Se ejecuta un primer proceso de autenticación y autorización en un nivel de acceso a red usando un método de autenticación predeterminado. A continuación, se determina una clave usada para un proceso de reautenticación. A continuación, se ejecuta un segundo proceso de autenticación y autorización a nivel de servicio usando un protocolo de reautenticación basado en la clave determinada, en donde el protocolo de reautenticación es independiente del método de autenticación predeterminado.

Aún existe la necesidad de un esquema de autenticación más fiable que proporcione mayor seguridad.

La presente invención proporciona una solución de acuerdo con la materia objeto de las reivindicaciones independientes.

En algunos casos, una red celular puede permitir el acceso a la red celular a través de diferentes tipos de redes de acceso, algunas de las cuales pueden ser más o menos vulnerables de atacar, y algunas de las cuales pueden estar más o menos bajo el control de un operador de la red celular. Por ejemplo, una red celular puede permitir el acceso a la red celular a través de una red de acceso celular o una red de acceso no celular (por ejemplo, una red de área local inalámbrica (WLAN)). Cuando se soporta el mismo procedimiento de EAP por parte de autenticadores asociados a diferentes redes de acceso, puede derivarse la misma clave de sesión maestra (MSK) como resultado de realizar el procedimiento de EAP a través de un autenticador asociado a una red de acceso celular o un autenticador asociado a una red de acceso no celular. De ese modo, puede proporcionarse la misma MSK, o la misma clave de seguridad derivada de la misma, al autenticador asociado a la red de acceso celular o al autenticador asociado a la red de acceso no celular. Si la red de acceso no celular está comprometida por un atacante, el acceso del atacante a la MSK o a las claves de seguridad derivadas de la misma puede permitir al atacante usar la red de acceso no celular para hacerse pasar por la red de acceso celular frente a un UE, lo que compromete la seguridad del UE y/o una aplicación ejecutada en el UE. Las técnicas descritas en la presente divulgación ayudan a mitigar tales amenazas determinando el tipo de red asociada a un autenticador y realizando un procedimiento de autenticación con el autenticador (o derivando una clave de seguridad para el autenticador) basado en un tipo de clave de sesión de EAP (por ejemplo, una MSK o una MSK extendida (EMSK)) asociada al tipo de red. En algunos ejemplos, puede usarse la MSK cuando un autenticador está asociado a una red de acceso no celular, y puede usarse la EMSK cuando un autenticador está asociado a una red de acceso celular.

En un ejemplo, se describe un método para comunicación inalámbrica en un UE. El método puede incluir realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El método también puede incluir derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; determinar un tipo de red asociado al autenticador; y realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o la EMSK al tipo de red determinado.

En un ejemplo, se describe un aparato para comunicación inalámbrica en un UE. El aparato puede incluir medios para realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El aparato también puede incluir medios para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; medios para determinar que el autenticador está asociado a una red celular; y medios para realizar al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o la EMSK al tipo de red determinado.

En un ejemplo, se describe otro aparato para la comunicación inalámbrica en un UE. El aparato puede incluir un procesador y una memoria en comunicación electrónica con el procesador. El procesador y la memoria pueden configurarse para realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El procesador y la memoria también pueden configurarse para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; determinar un tipo de red asociado al autenticador; y realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o la EMSK al tipo de red determinado.

En un ejemplo, se describe un medio legible por computadora no transitorio que almacena código ejecutable por computadora para comunicación inalámbrica en un UE. El código puede ser ejecutado por un procesador para realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El código también puede ser ejecutable por el procesador para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; determinar un tipo de red asociado al autenticador; y realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o la EMSK al tipo de red determinado.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el tipo de red determinado puede incluir un tipo de red celular y realizar el al menos un procedimiento de autenticación con el autenticador puede incluir derivar una primera clave de seguridad para una red celular. La primera clave de seguridad puede basarse al menos en parte en la EMSK y en un segundo conjunto de parámetros. En algunos

ejemplos, el segundo conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, realizar el al menos un procedimiento de autenticación con el autenticador puede incluir derivar una segunda clave de seguridad para un nodo de red de la red celular, la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros; y comunicarse con la red celular a través del nodo de red basándose al menos en parte en la segunda clave de seguridad. En algunos de estos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE y el nodo de red, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, la red celular puede incluir al menos una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el tipo de red determinado puede incluir un tipo de red no celular y realizar el al menos un procedimiento de autenticación con el autenticador puede incluir derivar una primera clave de seguridad para una red no celular. La primera clave de seguridad puede basarse al menos en parte en la MSK y un segundo conjunto de parámetros.

En un ejemplo, un método para comunicación inalámbrica en un servidor de autenticación puede incluir realizar un procedimiento de EAP con un UE a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE. El método también puede incluir derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; determinar un tipo de red asociado al autenticador; derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red, y basada al menos en parte en un segundo conjunto de parámetros; y transmitir la clave de seguridad al autenticador a través de un canal seguro.

En un ejemplo, se describe un aparato para comunicación inalámbrica en un servidor de autenticación. El aparato puede incluir medios para realizar un procedimiento de EAP con un UE a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE. El aparato también puede incluir medios para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; medios para determinar un tipo de red asociado al autenticador; medios para derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red, y basada al menos en parte en un segundo conjunto de parámetros; y medios para transmitir la clave de seguridad al autenticador a través de un canal seguro.

En un ejemplo, se describe otro aparato para comunicación inalámbrica en un servidor de autenticación. El aparato puede incluir un procesador y una memoria en comunicación electrónica con el procesador. El procesador y la memoria pueden configurarse para realizar un procedimiento de EAP con un UE a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE. El procesador y la memoria también pueden configurarse para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; determinar un tipo de red asociado al autenticador; derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red determinado, y basada al menos en parte en un segundo conjunto de parámetros; y transmitir la clave de seguridad al autenticador a través de un canal seguro.

En un ejemplo, se describe un medio legible por computadora no transitorio que almacena código ejecutable por computadora para comunicación inalámbrica en un servidor de autenticación. El código puede ser ejecutable por un procesador para realizar un procedimiento de EAP con un UE a través de un autenticador. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE. El código también puede ser ejecutable por el procesador para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros; determinar un tipo de red asociado al autenticador; derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red determinado, y basada al menos en parte en un segundo conjunto de parámetros; y transmitir la clave de seguridad al autenticador a través de un canal seguro.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el tipo de red determinado puede incluir un tipo de red celular y el segundo conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el servidor de autenticación y la red celular, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, la red celular puede incluir al menos una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

En un ejemplo, se describe un método para comunicación inalámbrica en una red celular. El método puede incluir recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. El método también puede incluir realizar al menos un procedimiento de autenticación con el UE basado al menos en parte en la primera clave de seguridad.

En un ejemplo, se describe un aparato para comunicación inalámbrica en una red celular. El aparato puede incluir medios para recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. El aparato también puede incluir medios para realizar al menos un procedimiento de autenticación con el UE basado al menos en parte en la primera clave de seguridad.

En un ejemplo, se describe otro aparato para comunicación inalámbrica en una red celular. El aparato puede incluir un procesador y una memoria en comunicación electrónica con el procesador. El procesador y la memoria pueden configurarse para recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. El procesador y la memoria también pueden configurarse para realizar al menos un procedimiento de autenticación con el UE basado al menos en parte en la primera clave de seguridad.

En un ejemplo, se describe un medio legible por computadora no transitorio que almacena código ejecutable por computadora para comunicación inalámbrica en una red celular. El código puede ser ejecutado por un procesador para recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. El código también puede ser ejecutable para realizar al menos un procedimiento de autenticación con el UE basado al menos en parte en la primera clave de seguridad.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, realizar el al menos un procedimiento de autenticación con el UE puede incluir derivar una segunda clave de seguridad para un nodo de red de la red celular, la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros; y comunicarse con el UE a través del nodo de red basándose al menos en parte en la segunda clave de seguridad. En algunos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE y el nodo de red, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el segundo conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

En algunos ejemplos del método, aparato y medio legible por computadora no transitorio descritos anteriormente, la red celular puede incluir al menos una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

Lo expuesto anteriormente ha perfilado de manera bastante amplia las técnicas y ventajas técnicas de los ejemplos de acuerdo con la divulgación para que la descripción detallada que sigue a continuación pueda entenderse mejor. En lo sucesivo en el presente documento se describirán técnicas y ventajas adicionales. La concepción y ejemplos específicos desvelados pueden utilizarse fácilmente como base para modificar o diseñar otras estructuras para realizar los mismos fines de la presente divulgación. Tales construcciones equivalentes no se apartan del alcance de las reivindicaciones adjuntas. Las características de los conceptos desvelados en el presente documento, tanto su organización como su método operativo, junto con ventajas asociadas, se entenderán mejor a partir de la siguiente descripción cuando se considera junto con las figuras adjuntas. Cada una de las figuras se proporciona con fines ilustrativos y descriptivos, y no como una definición de los límites de las reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Puede conseguirse una mejor comprensión de la naturaleza y las ventajas de la presente invención por referencia a los siguientes dibujos. En las figuras adjuntas, los componentes o funciones similares pueden tener la misma etiqueta de referencia. Además, pueden distinguirse diversos componentes del mismo tipo poniendo detrás de la etiqueta de referencia un guión y una segunda etiqueta que distinga entre los componentes similares. Si solo se usa la primera etiqueta de referencia en la memoria descriptiva, la descripción es aplicable a uno cualquiera de los componentes similares que tienen la misma primera etiqueta de referencia independientemente de la segunda etiqueta de referencia.

La Figura 1 ilustra un ejemplo de un sistema de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 2 ilustra un ejemplo de un sistema de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 3 ilustra un ejemplo de una jerarquía de claves para un sistema de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 4 ilustra un ejemplo de un sistema de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 5 muestra un ejemplo de flujo de mensajes entre un UE, una red celular y un servidor de autenticación, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 6 muestra un diagrama de bloques de un UE, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 7 muestra un diagrama de bloques de un gestor de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 8 muestra un diagrama de un sistema de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 9 muestra un diagrama de bloques de un servidor de autenticación, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 10 muestra un diagrama de bloques de un servidor de autenticación, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 11 muestra un diagrama de bloques de un nodo de red, de acuerdo con diversos aspectos de la presente divulgación;
la Figura 12 muestra un diagrama de bloques de un gestor de comunicación, de acuerdo con diversos aspectos de la presente divulgación.
La Figura 13 muestra un diagrama de un nodo de red, de acuerdo con diversos aspectos de la presente divulgación; y
las Figuras 14 a 18 muestran diagramas de flujo que ilustran métodos para comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación.

DESCRIPCIÓN DETALLADA

Las técnicas descritas en la presente divulgación permiten que los UE realicen procedimientos EAP con un servidor de autenticación a través de autenticadores asociados a diferentes tipos de redes de acceso. Tras la realización satisfactoria de un procedimiento de EAP a través de un autenticador, un UE y un servidor de autenticación pueden derivar claves de seguridad para el autenticador basadas al menos en parte en un tipo de red asociada al autenticador. En algunos ejemplos, el UE y el servidor de autenticación pueden derivar claves de seguridad para el autenticador basadas en una MSK cuando el autenticador está asociado a una red de acceso no celular, y pueden derivar claves de seguridad para el autenticador basadas en una EMSK cuando el autenticador está asociado a una red de acceso celular.

La siguiente descripción proporciona ejemplos, y no limita el alcance, aplicabilidad o ejemplos expuestos en las reivindicaciones. Pueden realizarse cambios en la función y disposición de los elementos discutidos sin apartarse del alcance de la divulgación. Diversos ejemplos pueden omitir, sustituir o añadir varios procedimientos o componentes según sea apropiado. Por ejemplo, los métodos descritos pueden realizarse en un orden diferente al descrito, y pueden añadirse, omitirse o combinarse diversas etapas. Además, las características descritas con respecto a algunos ejemplos pueden combinarse en algunos otros ejemplos.

La Figura 1 ilustra un ejemplo de un sistema de comunicación inalámbrica 100, de acuerdo con diversos aspectos de la divulgación. El sistema de comunicación inalámbrica 100 puede incluir dispositivos de acceso a red (por ejemplo, dispositivos de acceso a red distribuidos, unidades distribuidas, gNB, cabezales de radio (RH), SRH, puntos de transmisión/recepción (TRP), nodos frontera, unidades frontera, etc.) 105, UE 115, controladores de dispositivo de acceso a red (por ejemplo, dispositivos de acceso a red centralizados, nodos centrales, unidades centrales, controladores de nodos de acceso (ANC), etc.) 125, y una red central 130. La red central 130 puede proporcionar autenticación de usuario, autorización de acceso, rastreo, conectividad de protocolo de Internet (IP) y otras funciones de acceso, enrutamiento o movilidad. Los controladores de dispositivo de acceso a red 125 pueden interactuar con la red central 130 a través de enlaces de retorno 132 (por ejemplo, S1, S2, etc.) y pueden realizar la configuración y planificación de radio para comunicación con los UE 115. En diversos ejemplos, los controladores de dispositivo de acceso a red 125 pueden comunicarse, directa o indirectamente (por ejemplo, a través de la red central 130), entre sí a través de enlaces de retorno 134 (por ejemplo, X1, X2, etc.), que pueden ser enlaces de comunicación cableados o inalámbricos. Cada controlador de dispositivo de acceso a red 125 también puede comunicarse con diversos UE 115 a través de varios dispositivos de acceso a red (por ejemplo, RH) 105. En una configuración alternativa del sistema de comunicación inalámbrica 100, la funcionalidad de un controlador de dispositivo de acceso a red 125 puede proporcionarse mediante un dispositivo de acceso a red 105 o distribuirse a través de los dispositivos de acceso a red 105 de un nodo de red (por ejemplo, un nodo de acceso, una estación base de nueva radio (NR BS), etc.) 135. En otra configuración alternativa del sistema de comunicación inalámbrica 100, los nodos de red 135 pueden reemplazarse por eNB, los dispositivos de acceso a red 105 pueden reemplazarse con estaciones base, y los controladores de dispositivo de acceso a red 125 pueden reemplazarse por controladores de estaciones base (o enlaces a la red central 130).

Los controladores de dispositivo de acceso a red 125 pueden comunicarse con los UE 115 a través de uno o más dispositivos de acceso a red 105, teniendo cada dispositivo de acceso a red 105 una o más antenas para comunicarse de forma inalámbrica con diversos UE 115. Cada uno de los nodos de red 135 puede proporcionar cobertura de comunicación para un área de cobertura geográfica 110 respectiva, y puede proporcionar uno o más transceptores remotos asociados a uno o más dispositivos de acceso a red 105. Un dispositivo de acceso a red 105 puede realizar muchas de las funciones de una estación base LTE/LTE-A. En algunos ejemplos, un controlador de dispositivo de acceso a red 125 puede implementarse de forma distribuida, proporcionándose una parte del controlador de dispositivo de acceso a la red 125 en cada dispositivo de acceso a red 105. El área de cobertura geográfica 110 para un nodo de red 135 puede dividirse en sectores que constituyen solo una parte del área de cobertura (no mostrado) y, en algunos ejemplos, un área de cobertura geográfica 110 para un nodo de red 135 puede formarse a partir de un conjunto de áreas de cobertura geográfica para un conjunto de dispositivos de acceso a red 105 asociados al nodo de red 135 (no mostrado). En algunos ejemplos, los dispositivos de acceso a red 105 pueden reemplazarse con dispositivos de acceso a red alternativos, tales como estaciones transceptoras base, estaciones base de radio, puntos de acceso, transceptores de radio, NodeB, eNB, NodeB domésticos, eNodeB domésticos, gNB, etc. El sistema de comunicación inalámbrica 100 puede incluir dispositivos de acceso a red 105 (o estaciones base u otros dispositivos de acceso a red) de diferentes tipos (por ejemplo, dispositivos de acceso a red de macrocelda y/o microcelda). Las áreas de cobertura geográfica de los dispositivos de acceso a red 105 y/o los nodos de red 135 pueden superponerse. En algunos ejemplos, diferentes dispositivos de acceso a red 105 pueden estar asociados a diferentes tecnologías de acceso por radio.

En algunos ejemplos, el sistema de comunicación inalámbrica 100 puede incluir una red 5G. En otros ejemplos, el sistema de comunicación inalámbrica 100 puede incluir una red LTE/LTE-A. El sistema de comunicación inalámbrica 100 puede ser, en algunos casos, una red heterogénea, en la que diferentes tipos de dispositivos de acceso a red 105 o nodos de red 135 proporcionan cobertura para diversas regiones geográficas. Por ejemplo, cada dispositivo de acceso a red 105 o nodo de red 135 puede proporcionar cobertura de comunicación para una macrocelda, una celda pequeña y/u otros tipos de celda. El término "celda" puede usarse para describir una estación base, RH, portadora o portadora de componentes asociada a una estación base o RH, o área de cobertura (por ejemplo, sector, etc.) de una portadora o estación base, dependiendo del contexto.

Una macrocelda puede cubrir un área geográfica relativamente grande (por ejemplo, varios kilómetros de radio) y puede permitir acceso a los UE 115 con suscripciones de servicio con un proveedor de red. Una celda pequeña puede incluir una estación base o RH de menor potencia, en comparación con una macrocelda, y puede operar en la misma banda o diferentes bandas de frecuencia que las macroceldas. Las celdas pequeñas pueden incluir picoceldas, femtoceldas y microceldas de acuerdo con diversos ejemplos. Una picocelda puede cubrir un área geográfica relativamente más pequeña y puede permitir acceso sin restricciones a los UE 115 con suscripciones de servicio con un proveedor de red. Una femtocelda también puede cubrir un área geográfica relativamente pequeña (por ejemplo, un hogar) y puede proporcionar acceso restringido a los UE 115 que tienen una asociación a la femtocelda (por ejemplo, UE en un grupo cerrado de suscriptores (CSG), UE para usuarios en el hogar y similares). Un dispositivo de acceso a red para una macrocelda puede denominarse dispositivo de acceso a macrorred. Un dispositivo de acceso a red para una celda pequeña puede denominarse dispositivo de acceso a red de celda pequeña, un dispositivo de acceso a picorred, un dispositivo de acceso a femtorred o un dispositivo de acceso a red doméstica. Un dispositivo de acceso a red puede soportar una o múltiples (por ejemplo, dos, tres, cuatro y similar) celdas (por ejemplo, portadoras de componentes).

El sistema de comunicación inalámbrica 100 puede soportar operación síncrona o asíncrona. Para la operación síncrona, los nodos de red 135 o dispositivos de acceso a red 105 pueden tener una temporización de trama similar, y las transmisiones desde diferentes dispositivos de acceso a red 105 pueden estar aproximadamente alineadas en el tiempo. Para la operación asíncrona, los nodos de red 135 o dispositivos de acceso a red 105 pueden tener diferentes temporizaciones de trama, y las transmisiones desde diferentes dispositivos de acceso a red 105 pueden no estar alineadas en el tiempo. Las técnicas descritas en el presente documento pueden usarse para operaciones síncronas o asíncronas.

Las redes de comunicación que pueden acomodar algunos de los diversos ejemplos desvelados pueden ser redes basadas en paquetes que operan de acuerdo con una pila de protocolos en capas. En el plano del usuario, las comunicaciones en la capa portadora o de protocolo de convergencia de paquetes de datos (PD-CP) pueden basarse en IP. En algunos casos, una capa de control de enlace de radio (RLC) puede realizar la segmentación y el reensamblaje de paquetes para comunicarse a través de canales lógicos. Una capa de control de acceso al medio (MAC) puede realizar la manipulación de prioridad y multiplexación de canales lógicos en canales de transporte. La capa MAC también puede utilizar Hybrid ARQ (HARQ) para proporcionar retransmisión en la capa MAC para mejorar la eficacia de enlace. En el plano de control, la capa de protocolo de control de recursos de radio (RRC) puede proporcionar el establecimiento, configuración y mantenimiento de una conexión RRC entre un UE 115 y un dispositivo de acceso a red 105, controlador del dispositivo de acceso a red 125 o red central 130 que soporta portadoras de radio para datos del plano de usuario. En la capa física (PHY), los canales de transporte se pueden mapearse en canales físicos.

Los UE 115 pueden estar dispersos por todo el sistema de comunicación inalámbrica 100, y cada UE 115 puede ser estacionario o móvil. Un UE 115 también puede incluir, o denominarse por los expertos en la materia, una estación móvil, estación de suscriptor, unidad móvil, unidad de suscriptor, unidad inalámbrica, unidad remota, dispositivo móvil, dispositivo inalámbrico, dispositivo de comunicación inalámbrica, dispositivo remoto, estación de suscriptor móvil, terminal de acceso, terminal móvil, terminal inalámbrico, terminal remoto, teléfono, agente de usuario, cliente móvil, cliente, o alguna otra terminología adecuada. Un UE 115 puede ser un teléfono celular, asistente digital personal (PDA), módem inalámbrico, dispositivo de comunicación inalámbrica, dispositivo portátil, tableta, computadora portátil, teléfono inalámbrico, estación de bucle local inalámbrico (WLL), dispositivo de Internet de todo (IdT), automóvil, electrodoméstico u otro dispositivo electrónico que tenga una interfaz de comunicación inalámbrica. Un UE puede comunicarse con varios tipos de nodos de red 135 o dispositivos de acceso a la red 105, incluidos nodos de células pequeñas, nodos de retransmisión y similares. Un UE también puede ser capaz de comunicarse directamente con otros UE (por ejemplo, usando un protocolo entre pares (P2P)).

Los enlaces de comunicación 122 mostrados en el sistema de comunicación inalámbrica 100 pueden incluir canales de enlace ascendente (UL), desde un UE 115 a un dispositivo de acceso a red 105, y/o canales de enlace descendente (DL), desde un dispositivo de acceso a red 105 a un UE 115. El Los canales de enlace descendente también pueden denominarse canales de enlace directo, mientras que los canales de enlace ascendente también pueden denominarse canales de enlace inverso.

Cada enlace de comunicación 122 puede incluir una o más portadoras, donde cada portadora puede ser una señal compuesta por múltiples subportadoras o tonos (por ejemplo, señales de forma de onda de diferentes frecuencias) modulados de acuerdo con una o más tecnologías de acceso por radio. Cada señal modulada puede enviarse en una subportadora diferente y puede transportar información de control (por ejemplo, señales de referencia, canales de control, etc.), información general, datos de usuario, etc. Los enlaces de comunicación 122 pueden transmitir comunicaciones bidireccionales usando técnicas de duplexación por división de frecuencia (FDD) (por ejemplo, usando recursos de espectro emparejados) o técnicas de duplexación por división de tiempo (TDD) (por ejemplo, usando recursos de espectro no emparejados). Pueden definirse estructuras de trama para FDD (por ejemplo, estructura de trama de tipo 1) y TDD (por ejemplo, estructura de trama de tipo 2).

En algunos ejemplos del sistema de comunicación inalámbrica 100, los dispositivos de acceso a red 105 y/o los UE 115 pueden incluir múltiples antenas para emplear esquemas de diversidad de antenas para mejorar la calidad y fiabilidad de comunicación entre los dispositivos de acceso a red 105 y los UE 115. Además, o alternativamente, los dispositivos de acceso a red 105 y/o los UE 115 pueden emplear técnicas de múltiples entradas y múltiples salidas (MIMO) que pueden aprovechar entornos de múltiples trayectorias para transmitir múltiples capas espaciales que transportan datos codificados iguales o diferentes.

El sistema de comunicación inalámbrica 100 puede soportar operación en múltiples celdas o portadoras, una característica que puede denominarse agregación de portadoras (CA) u operación de múltiples portadoras. Una portadora también puede denominarse portadora de componentes (CC), capa, canal, etc. Los términos y expresiones "portadora", "portadora de componentes", "celda" y "canal" pueden usarse de forma intercambiable en el presente documento. Un UE 115 puede estar configurado con múltiples CC de enlace descendente y una o más CC de enlace ascendente para agregación de portadoras. La agregación de portadoras puede usarse con portadoras de componentes tanto FDD como TDD.

Uno o más de los UE 115 pueden incluir un gestor de comunicación inalámbrica 140. En algunos ejemplos, el gestor de comunicación inalámbrica 140 puede usarse para realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador asociado a la red central 130. Puede accederse al servidor de autenticación a través de la red central 130, como se describe por referencia a la Figura 2. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El gestor de comunicación inalámbrica 140 también puede usarse para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros (denominado colectivamente método EAP o método de autenticación); determinar que el autenticador está asociado a una red celular; y realizar al menos un procedimiento de autenticación con la red celular basado al menos en parte en la EMSK. En algunos ejemplos, el gestor de comunicación inalámbrica 140 puede ser un ejemplo de aspectos de los gestores de comunicación inalámbrica descritos por referencia a las Figuras 6-8.

La Figura 2 ilustra un ejemplo de un sistema de comunicación inalámbrica 200, de acuerdo con diversos aspectos de la presente divulgación. El sistema de comunicación inalámbrica 200 puede incluir una red celular doméstica 205 de un UE 115-a, y una red celular visitada por el UE 115-a (es decir, una red celular visitada 205-a).

La red celular doméstica 205 puede incluir un primer autenticador 235 (por ejemplo, un servidor o dispositivo que proporciona una función de anclaje de seguridad doméstica (H-SEAF)) y una pasarela de plano de usuario doméstico (H-UP-GW) 210. Los expertos en la materia entenderán que la red celular doméstica 205 también puede incluir otros servidores o dispositivos que proporcionen otras funciones (no mostrado). La red celular visitada 205-a puede incluir un segundo autenticador 235-a (por ejemplo, un servidor o dispositivo que proporciona una SEAF visitante (V-SEAF)), una UP-GW visitada (V-UP-GW) 210-a, una función de red central de plano de control de red celular visitada (V-CP-CN) 215, y una red de acceso por radio (RAN) 220. En algunos ejemplos, la RAN 220 puede incluir uno o más de los nodos de red 135, dispositivos de acceso a red 105, y controladores de dispositivo de acceso a red 125 descritos por referencia a la Figura 1. El primer autenticador 235, H-UP-GW 210, el segundo autenticador 235-a, V-UP-GW 210-a y V-CP-CN 215 pueden ser componentes a modo de ejemplo de la red central 130 descrita por referencia a la Figura 1.

La red celular doméstica 205 puede estar en comunicación con (o puede proporcionar) un servidor de autenticación 245. El servidor de autenticación 245 puede proporcionar una función de servidor de autenticación (AUSF). El servidor de autenticación 245 puede acceder a y/o invocar un repositorio de credenciales de autenticación y una función de procesamiento (ARPF) 240.

El UE 115-a puede conectarse a la red celular visitada 205-a a través de un nodo (por ejemplo, un dispositivo de acceso a red) de la RAN 220. La Figura 2 supone que el UE 115-a accedió a la red celular visitada 205-a mientras operaba en un modo de itinerancia. En un escenario sin itinerancia, el UE 115-a puede acceder a la red celular doméstica 205 en lugar de la red celular visitada 205-a a través de una RAN de la red celular doméstica 205 (no mostrado en la Figura 2).

La V-CP-CN 215 puede incluir o gestionar uno o más aspectos de funciones de gestión de movilidad (MM) y/o funciones de gestión de sesión (SM) para el UE 115-a, así como mantener los contextos de seguridad correspondientes. El segundo autenticador 235-a puede facilitar y gestionar la autenticación del UE 115-a para la red celular visitada 205-a, y puede mantener una clave de sesión de anclaje a partir de la que pueden derivarse claves de seguridad posteriores. La V-UP-GW 210-a puede mantener un contexto de seguridad de plano de usuario (por ejemplo, una clave de seguridad) para el UE 115-a cuando la seguridad de plano de usuario termina en la V-UP-GW 210-a. La seguridad de plano de usuario puede terminarse por la RAN 220 y/o la V-UP-GW 210-a y puede configurarse por la red. Generalmente, el UE 115-a puede mantener un contexto de seguridad con cada nodo de la red celular visitada 205-a.

Tras acceder a la red celular visitada 205-a, el segundo autenticador 235-a puede facilitar un procedimiento de EAP realizado por el UE 115-a y el servidor de autenticación 245. El segundo autenticador 235-a puede establecer o mantener, a través del primer autenticador 235 (de la red celular doméstica 205), un canal seguro para realizar el procedimiento de EAP con el servidor de autenticación 245.

El procedimiento de EAP realizado por el UE 115-a y el servidor de autenticación 245 puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE 115-a y el servidor de autenticación 245. Como parte de la realización del procedimiento de EAP, el UE 115-a y el servidor de autenticación 245 pueden derivar cada uno una MSK y una EMSK. La MSK y la EMSK pueden basarse al menos en parte en las credenciales de autenticación y el primer conjunto de parámetros. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE o una combinación de los mismos.

Cuando el procedimiento de EAP tiene éxito (por ejemplo, cuando el UE 115-a y el servidor de autenticación 245 se autentican con éxito entre sí), el servidor de autenticación 245 puede transmitir una clave de anclaje de sesión (por ejemplo, una primera clave de seguridad) al segundo autenticador 235-a. De acuerdo con las técnicas descritas en la

presente divulgación, la clave de anclaje de sesión puede basarse al menos en parte en la EMSK. La clave de anclaje de sesión también puede basarse al menos en parte en un segundo conjunto de parámetros. El segundo conjunto de parámetros puede incluir un identificador de la red celular visitada 205-a, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE 115-a y la segunda red celular 205-a, o una combinación de los mismos.

El UE 115-a puede derivar independientemente la clave de anclaje de sesión. Basándose al menos en parte en la clave de anclaje de sesión, el UE 115-a y el segundo autenticador 235-a pueden autenticarse entre sí y derivar claves de seguridad adicionales (por ejemplo, claves de seguridad para otros nodos o funciones de la segunda red celular 205-a), como se muestra en la Figura 3.

En una alternativa a lo que se muestra en la Figura 2, los servidores o dispositivos que proporcionan H-SEAF y V-SEAF pueden no asumir el papel de autenticador en un procedimiento de EAP realizado entre el UE 115-a y el servidor de autenticación 245 y, en su lugar, puede situarse conjuntamente un autenticador con el servidor de autenticación 245 (por ejemplo, el servidor que proporciona AUSF). En estos ejemplos, el servidor de autenticación 245 puede derivar una clave de anclaje de sesión para H-SEAF o V-SEAF basada en MSK o EMSK y el segundo conjunto de parámetros, y transmitir la clave de anclaje de sesión a H-SEAF (en un escenario sin itinerancia) o V-SEAF (en un escenario de itinerancia).

La Figura 3 ilustra un ejemplo de una jerarquía de claves 300 para un sistema de comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación. Esta solución proporciona un enlace de red de servicio a la clave suministrada a la red de servicio 3GPP para protocolos EAP generales mediante el uso de una EMSK para derivar la clave (por ejemplo, K_{SEAF}) que se transmite desde el servidor EAP (por ejemplo, el servidor de autenticación 245 descrito por referencia a la Figura 2). En algunos ejemplos, la jerarquía de claves 300 puede usarse por los sistemas de comunicación inalámbrica 100 y 200 descritos por referencia a las Figuras 1 y 2. Por ejemplo, un UE y/o nodos de red pueden usar la jerarquía de claves 300 para implementar uno o más aspectos de las funciones de autenticación o seguridad descritas por referencia a las Figuras 1 y 2.

La jerarquía de claves 300 puede incluir una clave raíz K 305 usada como contexto de seguridad entre un módulo de identidad de suscriptor universal (USIM) y una ARPF. La clave raíz K 305 puede usarse como base para realizar un procedimiento de EAP y derivar las claves 310 (por ejemplo, una MSK y una EMSK) para proporcionar un contexto de seguridad entre un servidor de autenticación y un UE (por ejemplo, entre el servidor de autenticación 245 y el UE 115-a descritos por referencia a la Figura 2). La clave raíz K 305 puede usarse para realizar un procedimiento de EAP basado en clave compartida, pero pueden usarse una o más claves distintas (por ejemplo, una clave derivada basada de certificados) cuando se realiza un procedimiento de EAP basado en certificado. La EMSK puede usarse por el servidor de autenticación (por ejemplo, AUSF) y el UE para derivar una clave de sesión de anclaje K_{SEAF} 315 para un autenticador (por ejemplo, para el segundo autenticador 235-a descrito por referencia a la Figura 2). Debido a que se usa EMSK (en lugar de MSK) para derivar K_{SEAF}, puede no haber necesidad de restringir el uso de credenciales al acceso de 3GPP. Por ejemplo, cuando una entidad que no es 3GPP obtiene la MSK basándose en autenticación EAP, la entidad que no es 3GPP no puede derivar K_{SEAF} porque K_{SEAF} se deriva de la EMSK que no conoce la entidad que no es 3GPP. La clave de sesión de anclaje de K_{SEAF} 315 puede mantenerse por parte del autenticador y el UE.

La clave de sesión de anclaje K_{SEAF} 315 puede usarse por el autenticador para derivar una clave $K_{CP\text{-}CN}$ 320 y una clave $K_{UP\text{-}GW}$ 325. La clave $K_{CP\text{-}CN}$ 320 puede mantenerse por una función de CP-CN (por ejemplo, la V-CP-CN 215 descrita por referencia a la Figura 2) y el UE. La clave $K_{UP\text{-}GW}$ 325 puede mantenerse por una función de UP-GW (por ejemplo, la V-UP-GW 210-a descrita por referencia a la Figura 2) y el UE. La clave $K_{UP\text{-}GW}$ 325 puede usarse por la UP-GW para establecer la clave $K_{UP\text{-}GWenc}$ 340 y la clave $K_{UP\text{-}GWint}$ 345. La clave $K_{UP\text{-}GWenc}$ 340 y la clave $K_{UP\text{-}GWint}$ 345 pueden usarse para protección de integridad y codificación de paquetes del plano de usuario.

La clave $K_{CP\text{-}CN}$ 320 puede usarse por la función de CP-CN para derivar la clave K_{NASenc} 330, la clave K_{NASint} 335 y la clave K_{AN}/NH 350. La clave K_{AN}/NH 350 puede usarse por el nodo de acceso para derivar la clave K_{UPint} 355, la clave K_{UPenc} 360, la clave K_{RRCint} 365 y la clave K_{RRCenc} 370, que pueden usarse para protección de integridad y codificación de paquetes del plano de usuario y RRC.

La Figura 4 ilustra un ejemplo de un sistema de comunicación inalámbrica 400, de acuerdo con diversos aspectos de la presente divulgación. El sistema de comunicación inalámbrica 400 puede incluir una red celular doméstica 205-b de un UE 115-b, y una red celular visitada por el UE 115-b (es decir, una red celular visitada 205-c).

La red celular doméstica 205-b puede incluir un primer autenticador 235-b (por ejemplo, un servidor o dispositivo que proporciona una H-SEAF) y una H-UP-GW 210-b. La red celular doméstica 205-b también puede incluir otros servidores o dispositivos que proporcionen otras funciones (no mostrado). La red celular visitada 205-c puede incluir un segundo autenticador 235-c (por ejemplo, un servidor o dispositivo que proporcione una V-SEAF), una V-UP-GW 210-c, una V-CP-CN 215-a y una RAN 220-a. En algunos ejemplos, la RAN 220-a puede incluir uno o más de los nodos de red 135, dispositivos de acceso a red 105 y controladores de dispositivo de acceso a red 125 descritos por referencia a la Figura 1. El primer autenticador 235-b, H-UP-GW 210-b, segundo autenticador 235-c, V-UP-GW 210-c

y V-CP-CN 215-a pueden ser componentes a modo de ejemplo de la red central 130 descrita por referencia a la Figura 1.

La red celular doméstica 205-b puede estar en comunicación con (o puede proporcionar) un servidor de autenticación 245-a. El servidor de autenticación 245-a puede proporcionar una AUSF. El servidor de autenticación 245-a puede acceder a y/o invocar una ARPF 240-a.

Cada uno del primer autenticador 235-b, H-UP-GW 210-b, segundo autenticador 235-c, V-UP-GW 210-c, V-CP-CN 215-a, RAN 220-a, servidor de autenticación 245-a y ARPF 240-a pueden ser ejemplos de componentes, funciones o nodos numerados de forma similar descritos por referencia a la Figura 2.

La Figura 4 también muestra una red no celular 405 que incluye un nodo de acceso no celular 410 (por ejemplo, un punto de acceso WLAN (AP) o controlador de LAN inalámbrica (WLC)). Como se muestra, el UE 115-b puede conectarse a la RAN 220-a o al nodo de acceso no celular 410 y, en cada caso, el mismo servidor de autenticación 245-a puede realizar un procedimiento de EAP con el UE 115-b. Cuando el UE 115-b se conecta al RAN 220-a, el segundo autenticador 235-c puede servir como autenticador en un procedimiento de EAP realizado por el UE 115-by el servidor de autenticación 245-a. Cuando el UE 115-b se conecta al nodo de acceso no celular 410, el nodo de acceso no celular 410 puede servir como autenticador en un procedimiento de EAP realizado por el UE 115-b y el servidor de autenticación 245-a.

Si el UE 115-b y el servidor de autenticación 245-a son ambos capaces de realizar el mismo procedimiento de EAP y derivar la misma clave de anclaje de sesión (por ejemplo, para realizar un procedimiento de autenticación entre el UE 115-b y el segundo autenticador 235-c, o para realizar un procedimiento de autenticación entre el UE 115-b y el nodo de acceso no celular 410), un atacante que comprometa el nodo de acceso no celular 410 puede ser capaz de obtener la clave de anclaje de sesión del nodo de acceso no celular 410 y usarla para hacerse pasar por un nodo de la red celular visitada 205-c o la red celular doméstica 205-b. Para resolver el problema mencionado anteriormente, el UE 115-b y el servidor de autenticación 245-a pueden determinar el tipo de red asociada a un autenticador (por ejemplo, el tipo de red asociada al segundo autenticador 235-c o al nodo de acceso no celular 410) y determinar qué clave usar (entre una MSK y una EMSK) para derivar una clave de anclaje de sesión (es decir, derivar la clave de anclaje de sesión basada en el tipo de red). En algunos ejemplos, puede usarse la MSK cuando un autenticador (por ejemplo, el nodo de acceso no celular 410) está asociado a una red de acceso no celular (por ejemplo, la red no celular 405), y puede usarse la EMSK cuando un autenticador (por ejemplo, el segundo autenticador 235-c) está asociado a una red de acceso celular (por ejemplo, la red celular visitada 205-c). Además, una clave de anclaje de sesión derivada para un autenticador asociado a una red celular puede derivarse basándose al menos en parte en un conjunto de parámetros asociados a la red celular. Por ejemplo, puede derivarse una clave K_{SEAF} por parte del UE 115-b y el servidor de autenticación 245-a basándose en la fórmula de derivación de clave (KDF)

$$K_{SEAF} = KDF(EMSK, PLMN\ ID, CTX)$$

donde PLMN ID es un identificador de red móvil terrestre pública asociado a la red celular de servicio (por ejemplo, visitada) 205-b y proporcionado al servidor de autenticación 245-a durante el procedimiento de EAP, y CTX es un contexto que describe una tecnología de acceso (por ejemplo, acceso a red celular, tal como acceso a red 5G (NextGen), 4G, LTE/LTE-A o 3G). Los expertos en la materia entenderán que K_{SEAF} también puede derivarse basándose al menos en parte en otros parámetros adecuados.

Por derivación de la clave de anclaje de sesión para un autenticador basándose en un tipo de red asociada al autenticador, una red de un tipo de red es incapaz de obtener una clave de anclaje de sesión para una red de otro tipo y hacerse pasar por un nodo de un tipo de red diferente. Por tanto, puede usarse el mismo procedimiento de EAP (o método de autenticación) para redes de diferentes tipos sin afectar a la seguridad de las redes de diferentes tipos.

La Figura 5 muestra un ejemplo de flujo de mensajes 500 entre un UE 115-c, una red celular 205-d, y un servidor de autenticación 245-b, de acuerdo con diversos aspectos de la presente divulgación. El UE 115-c puede ser un ejemplo de aspectos de los UE 115 descritos por referencia a las Figuras 1, 2 y 4. La red celular 205-d puede ser un ejemplo de las redes celulares 205 descritas por referencia a las Figuras 2 y 4 y, en algunos casos, pueden incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G o una combinación de las mismas. El servidor de autenticación 245-b puede ser un ejemplo de aspectos de los servidores de autenticación 245 descritos por referencia a las Figuras 2 y 4. La red celular 205-d puede incluir una RAN 220-b y una CN celular 550. La RAN 220-b y CN 550 pueden ser ejemplos de las RAN 220 y CN descritas por referencia a las Figuras 2 y 4. En algunos ejemplos, la RAN 220-b puede incluir uno o más de los nodos de red 135, dispositivos de acceso a red 105 o controladores de dispositivo de acceso a red 125 descritos por referencia a la Figura 1. La CN 550 puede incluir un autenticador 235-d (por ejemplo, un nodo de la CN 550), que puede ser un ejemplo de aspectos de los autenticadores 235 descritos por referencia a las Figuras 2 y 4.

En 505, el UE 115-c puede acceder a la red celular 205-d, y el UE 115-c o la red celular 205-d pueden iniciar un procedimiento de EAP. En algunos ejemplos, el UE 115-c puede acceder a la red celular 205-d a través de un dispositivo de acceso a red (por ejemplo, un nodo de red) de la RAN 220-b. La RAN 220-b puede estar en comunicación

con la CN 550. El autenticador 235-d de la CN550 puede facilitar la realización del procedimiento de EAP. En una configuración alternativa de la red celular, el autenticador 235-d puede ser parte de la RAN 220-b o estar situado conjuntamente con el servidor de autenticación 245-b.

En 510, la red celular 205-d puede transmitir una solicitud para realizar un procedimiento de EAP al servidor de autenticación 245-b. En algunos ejemplos, la solicitud transmitida en 510 puede transmitirse a través de un canal seguro entre el autenticador 235-d y el servidor de autenticación 245-b (por ejemplo, la solicitud puede transmitirse entre el autenticador 235-d y el servidor de autenticación 245-b usando un protocolo Diameter (por ejemplo, usando encapsulación Diameter)).

En 515, el UE 115-c y el servidor de autenticación 245-b pueden realizar un procedimiento de EAP a través del autenticador 235-d, proporcionando el autenticador 235-d transporte para los mensajes transmitidos entre el UE 115-c y el servidor de autenticación 245-b. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE 115-c y el servidor de autenticación 245-b. Como parte de la realización del procedimiento de EAP, cada uno del UE 115-c y el servidor de autenticación 245-b pueden derivar una MSK y una EMSK. La MSK y EMSK pueden derivarse basándose al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

Antes, durante o después de las operaciones en 505, 510 o 515, el UE 115-c y el servidor de autenticación 245-b pueden determinar cada uno que el autenticador 235-d está asociado a una red celular (es decir, a la red celular 205-d).

En 520 y 525, cada uno del UE 115-c y el servidor de autenticación 245-b pueden derivar independientemente una primera clave de seguridad para la red celular 205-d. Debido a que el UE 115-c y el servidor de autenticación 245-b determinan cada uno que el autenticador 235-d está asociado a la red celular 205-d, cada uno del UE 115-c y el servidor de autenticación 245-b pueden derivar la primera seguridad clave basándose al menos en parte en EMSK. La primera clave de seguridad también puede derivarse basándose al menos en parte en un segundo conjunto de parámetros. En algunos ejemplos, el segundo conjunto de parámetros puede incluir un identificador de la red celular 205-d, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE 115-c o el servidor de autenticación 245-b y la red celular 205-c, o una combinación de los mismos.

En 530, el servidor de autenticación 245-b puede transmitir la primera clave de seguridad al autenticador 235-d a través del canal seguro entre el autenticador 235-d y el servidor de autenticación 245-b (por ejemplo, la primera clave de seguridad puede transmitirse entre el servidor de autenticación 245-b y el autenticador 235-d usando el protocolo Diameter (por ejemplo, usando encapsulación Diameter)).

En 535, el UE 115-c y la red celular 205-d pueden realizar un procedimiento de autenticación. En 540 y 545, tras realizar con éxito el procedimiento de autenticación en 535, el UE 115-c y la red celular 205-d pueden derivar una o más claves de seguridad adicionales (por ejemplo, una segunda clave de seguridad) para un nodo o nodos de red de la red celular 205-d. En algunos ejemplos, la segunda clave de seguridad puede basarse al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros. En algunos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE 115-c y el nodo de red, o una combinación de los mismos.

En 555, el UE 115-c puede comunicarse con la red celular 205-d basándose al menos en parte en las claves de seguridad derivadas.

La Figura 6 muestra un diagrama de bloques 600 de un UE 115-d, de acuerdo con diversos aspectos de la presente divulgación. El UE 115-d puede ser un ejemplo de aspectos de los UE 115 descritos por referencia a las Figuras 1, 2, 4 y 5. El UE 115-d puede incluir un receptor 610, un gestor de comunicación inalámbrica 620 y un transmisor 630. El UE 115-d también puede incluir un procesador. Cada uno de estos componentes puede estar en comunicación entre sí.

El receptor 610 puede recibir señales o información tales como señales de referencia, información de control o datos de usuario asociados a diversos canales (por ejemplo, canales de control, canales de datos, canales de difusión, canales de multidifusión, canales de unidifusión, etc.). Las señales e información recibidas pueden usarse por el receptor 610 (por ejemplo, para seguimiento de frecuencia/tiempo) o pasarse a otros componentes del UE 115-d, incluyendo el gestor de comunicación inalámbrica 620. El receptor 610 puede ser un ejemplo de aspectos del transceptor 825 descrito por referencia a la Figura 8. El receptor 610 puede incluir o estar asociado a una única antena o una pluralidad de antenas.

El gestor de comunicación inalámbrica 620 puede usarse para gestionar uno o más aspectos de la comunicación inalámbrica para el UE 115-d. En algunos ejemplos, parte del gestor de comunicación inalámbrica 620 puede incorporarse a o compartirse con el receptor 610 o el transmisor 630. El gestor de comunicación inalámbrica 620 puede

incluir un gestor de EAP 635, un identificador de tipo de red 640 y un autenticador de red 645. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses).

El gestor de EAP 635 puede usarse para realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador, como se ha descrito anteriormente por referencia a la Figura 5. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El gestor de EAP 635 también puede usarse para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

El identificador de tipo de red 640 puede usarse para determinar un tipo de red asociado al autenticador, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el tipo de red determinado puede incluir un tipo de red celular o un tipo de red no celular (por ejemplo, un tipo de WLAN).

El autenticador de red 645 puede usarse para realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o EMSK al tipo de red determinado, como se ha descrito anteriormente por referencia a la Figura 5.

El transmisor 630 puede transmitir señales o información recibida de otros componentes del UE 115-d, incluyendo el gestor de comunicación inalámbrica 620. Las señales o información pueden incluir, por ejemplo, señales de referencia, información de control o datos de usuario asociados a diversos canales (por ejemplo, canales de control, canales de datos, canales de transmisión, canales de multidifusión, canales de unidifusión, etc.). En algunos ejemplos, el transmisor 630 puede estar ubicado conjuntamente con el receptor 610 en un transceptor. El transmisor 630 puede ser un ejemplo de aspectos del transceptor 825 descritos por referencia a la Figura 8. El transmisor 630 puede incluir o estar asociado a una sola antena o una pluralidad de antenas.

La Figura 7 muestra un diagrama de bloques 700 de un gestor de comunicación inalámbrica 720, de acuerdo con diversos aspectos de la presente divulgación. El gestor de comunicación inalámbrica 720 puede ser un ejemplo de aspectos del gestor de comunicación inalámbrica 620 descritos por referencia a la Figura 6.

El gestor de comunicación inalámbrica 720 puede incluir un gestor de EAP 635-a, un identificador de tipo de red 640-a, un autenticador de red 645-a y un gestor de comunicación de red celular 715. El gestor de EAP 635-a, el identificador de tipo de red 640-a y el autenticador de red 645-a pueden ser ejemplos del gestor de EAP 635, el identificador de tipo de red 640 y el autenticador de red 645 descritos por referencia a la Figura 6. El autenticador de red 645-a puede incluir un derivador de claves de red 705 y un derivador de claves de nodo de red 710. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses).

El gestor de EAP 635-a puede usarse para realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador, como se ha descrito anteriormente por referencia a la Figura 5. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. El gestor de EAP 635-a también puede usarse para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

El identificador de tipo de red 640-a puede usarse para determinar un tipo de red asociado al autenticador, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el tipo de red determinado puede incluir un tipo de red celular o un tipo de red no celular (por ejemplo, un tipo de WLAN).

El autenticador de red 645-a puede usarse para realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o EMSK al tipo de red determinado.

Cuando el tipo de red determinado incluye un tipo de red celular, el derivador de claves de red 705 puede usarse para derivar una primera clave de seguridad para una red celular, como se ha descrito anteriormente por referencia a la Figura 5. La primera clave de seguridad puede basarse al menos en parte en la EMSK y un segundo conjunto de parámetros. En algunos ejemplos, el segundo conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos. Cuando el tipo de red determinado incluye un tipo de red no celular, el derivador de claves de red 705 puede usarse para derivar una primera clave de seguridad para una red no celular.

Cuando el tipo de red determinado incluye un tipo de red celular, el derivador de claves de nodo de red 710 puede usarse para derivar una segunda clave de seguridad para un nodo de red de la red celular, como se ha descrito anteriormente por referencia a la Figura 5. La segunda clave de seguridad puede basarse al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros. En algunos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE y el nodo de red, o una combinación de los mismos.

El gestor de comunicación de red celular 715 puede usarse para comunicarse con la red celular a través del nodo de red basándose al menos en parte en la segunda clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5.

La Figura 8 muestra un diagrama de un sistema de comunicación inalámbrica 800, de acuerdo con diversos aspectos de la presente divulgación. El sistema de comunicación inalámbrica 800 puede incluir un UE 115-e, que puede ser un ejemplo de aspectos de los UE 115 descritos por referencia a las Figuras 1, 2 y 4-6.

El UE 115-e puede incluir un gestor de comunicación inalámbrica 805, memoria 810, un procesador 820, un transceptor 825 y una antena 830. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses). El gestor de comunicación inalámbrica 805 puede ser un ejemplo de aspectos de los gestores de comunicación inalámbrica 620 y 720 descritos por referencia a las Figuras 6 y 7.

La memoria 810 puede incluir memoria de acceso aleatorio (RAM) o memoria de solo lectura (ROM). La memoria 810 puede almacenar *software* ejecutable por computadora, legible por computadora 815, incluyendo instrucciones que, cuando se ejecutan, hacen que el procesador 820 realice diversas funciones descritas en el presente documento, incluyendo funciones relacionadas con seguridad y autenticación de red. En algunos casos, el *software* 815 puede no ser directamente ejecutable por el procesador 820, pero puede hacer que el procesador 820 (por ejemplo, cuando se compila y ejecuta) realice las funciones descritas en el presente documento. El procesador 820 puede incluir un dispositivo de *hardware* inteligente (por ejemplo, una unidad central de procesamiento (CPU), un microcontrolador, un circuito integrado específico de aplicación (ASIC), etc.).

El transceptor 825 puede comunicarse bidireccionalmente, a través de una o más antenas o enlaces cableados, con una o más redes, como se describe en el presente documento. Por ejemplo, el transceptor 825 puede comunicarse bidireccionalmente con una red celular 205-e (o uno o más nodos de la misma) u otro UE 115-f. El transceptor 825 puede incluir un módem para modular paquetes y proporcionar los paquetes modulados a las antenas para su transmisión, y para demodular los paquetes recibidos desde las antenas. En algunos casos, el UE 115-e puede incluir una única antena 830. Sin embargo, en algunos casos, el UE 115-e puede tener más de una antena 830, que puede ser capaz de transmitir o recibir simultáneamente múltiples transmisiones inalámbricas.

La Figura 9 muestra un diagrama de bloques 900 de un servidor de autenticación 245-c, de acuerdo con diversos aspectos de la presente divulgación. El servidor de autenticación 245-c puede ser un ejemplo de aspectos de los servidores de autenticación 245 descritos por referencia a las Figuras 2, 4 y 5. El servidor de autenticación 245-c puede incluir un receptor 910, un gestor de autenticación 920 y un transmisor 930. El servidor de autenticación 245-c también puede incluir un procesador. Cada uno de estos componentes puede estar en comunicación entre sí.

El receptor 910 puede recibir solicitudes de autenticación de diversos nodos de red, incluyendo nodos de una red celular, una WLAN, etc. El receptor 910 también puede recibir información de autenticación de los UE a través de los nodos de red. Las solicitudes de autenticación recibidas y la información de autenticación pueden pasarse al gestor de autenticación 920. El receptor 910 puede ser un ejemplo de aspectos de la interfaz de autenticación 1025 descritos por referencia a la Figura 10. El receptor 910 puede incluir una o más interfaces cableadas y/o inalámbricas.

El gestor de autenticación 920 puede usarse para gestionar uno o más aspectos de autenticación de dispositivo para el servidor de autenticación 245-c. En algunos ejemplos, parte del gestor de autenticación 920 puede incorporarse a o compartirse con el receptor 910 o el transmisor 930. El gestor de autenticación 920 puede incluir un gestor de EAP 935, un identificador de tipo de red 940, un derivador de claves de red 945 y un instalador de claves de red 950. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses).

El gestor de EAP 935 puede usarse para realizar un procedimiento de EAP con un UE a través de un autenticador, como se ha descrito anteriormente por referencia a la Figura 5. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE. El gestor de EAP 935 también puede usarse para derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos.

El identificador de tipo de red 940 puede usarse para determinar un tipo de red asociado al autenticador, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el tipo de red determinado puede incluir un tipo de red celular o un tipo de red no celular (por ejemplo, un tipo de WLAN).

El derivador de claves de red 945 puede usarse para derivar una clave de seguridad para el tipo de red determinado basándose al menos en parte en una asociación de la MSK o EMSK al tipo de red, y basándose al menos en parte en un segundo conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. Cuando el tipo de red determinado incluye un tipo de red celular, y en algunos ejemplos, el segundo conjunto de parámetros puede incluir un identificador de una red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el servidor de autenticación y la red celular, o una combinación de los mismos. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

El instalador de claves de red 950 puede usarse para transmitir la clave de seguridad al autenticador a través de un canal seguro, como se ha descrito anteriormente por referencia a la Figura 5.

El transmisor 930 puede transmitir mensajes de retroalimentación de autenticación y claves de seguridad recibidas de otros componentes del servidor de autenticación 245-c, incluyendo el gestor de autenticación 920. El transmisor 930 puede ser un ejemplo de aspectos de la interfaz de autenticación 1025 descritos por referencia a la Figura 10. El transmisor 930 puede incluir una o más interfaces cableadas y/o inalámbricas.

La Figura 10 muestra un diagrama de bloques 1000 de un servidor de autenticación 245-d, de acuerdo con diversos aspectos de la presente divulgación. El servidor de autenticación 245-d puede ser un ejemplo de aspectos de los servidores de autenticación 245 descritos por referencia a las Figuras 2, 4, 5 y 9.

El servidor de autenticación 245-d puede incluir un gestor de autenticación 1005, memoria 1010, un procesador 1020 y una interfaz de autenticación 1025. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses). El gestor de autenticación 1005 puede ser un ejemplo de aspectos del gestor de autenticación 920 descritos por referencia a la Figura 9.

La memoria 1010 puede incluir RAM o ROM. La memoria 1010 puede almacenar *software* ejecutable por computadora, legible por computadora 1015, incluyendo instrucciones que, cuando se ejecutan, hacen que el procesador 1020 realice diversas funciones descritas en el presente documento, incluyendo funciones relacionadas con seguridad y autenticación de red. En algunos casos, el *software* 1015 puede no ser directamente ejecutable por el procesador 1020, pero puede hacer que el procesador 1020 (por ejemplo, cuando se compila y ejecuta) realice las funciones descritas en el presente documento. El procesador 1020 puede incluir un dispositivo de *hardware* inteligente (por ejemplo, una CPU, un microcontrolador, un ASIC, etc.).

La interfaz de autenticación 1025 puede comunicarse bidireccionalmente, a través de una o más antenas o enlaces cableados, con una o más redes, nodos de red o UE, como se describe en el presente documento. En algunos ejemplos, la interfaz de autenticación 1025 puede usarse para establecer una conexión segura con un nodo de red (por ejemplo, usando un protocolo Radius o Diameter) y comunicarse bidireccionalmente con un UE a través de la conexión segura y el nodo de red.

La Figura 11 muestra un diagrama de bloques 1100 de un nodo de red 1105, de acuerdo con diversos aspectos de la presente divulgación. El nodo de red 1105 puede ser un ejemplo de aspectos de los nodos de red descritos por referencia a las Figuras 2, 4 y 5 y, en algunos ejemplos, puede ser un ejemplo de los autenticadores 235 descritos por referencia a las Figuras 2, 4 y 5. El nodo de red 1105 puede incluir un receptor 1110, un gestor de comunicación 1120 y un transmisor 1130. El nodo de red 1105 también puede incluir un procesador. Cada uno de estos componentes puede estar en comunicación entre sí.

El receptor 1110 puede recibir señales o información de otros nodos de red, de UE, de un servidor de autenticación, etc. Las señales y la información recibidas pueden pasarse a otros componentes del nodo de red 1105, incluyendo el gestor de comunicación 1120. El receptor 1110 puede ser un ejemplo de aspectos de la interfaz de autenticación 1325 descritos por referencia a la Figura 13. El receptor 1110 puede incluir una o más interfaces cableadas y/o inalámbricas.

El gestor de comunicación 1120 puede usarse para gestionar uno o más aspectos de comunicación inalámbrica para el nodo de red 1105. En algunos ejemplos, parte del gestor de comunicación 1120 puede incorporarse a o compartirse con el receptor 1110 o el transmisor 1130. El gestor de comunicación 1120 puede incluir un gestor de claves de red 1135 y un autenticador de UE 1140. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses).

El gestor de claves de red 1135 puede usarse para recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse

entre un UE y el servidor de autenticación durante un procedimiento de EAP. En algunos ejemplos, el primer conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos. En algunos ejemplos, el segundo conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

El autenticador de UE 1140 puede usarse para realizar al menos un procedimiento de autenticación con el UE basándose al menos en parte en la primera clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5.

El transmisor 1130 puede transmitir señales o información recibida de otros componentes del nodo de red 1105, incluyendo el gestor de comunicación 1120. El transmisor 1130 puede ser un ejemplo de aspectos de la interfaz de autenticación 1325 descritos por referencia a la Figura 13. El receptor 1110 puede incluir una o más interfaces cableadas y/o inalámbricas.

La Figura 12 muestra un diagrama de bloques 1200 de un gestor de comunicación 1220, de acuerdo con diversos aspectos de la presente divulgación. El gestor de comunicación 1220 puede ser un ejemplo de aspectos del gestor de comunicación 1120 descritos por referencia a la Figura 11.

El gestor de comunicación 1220 puede incluir un gestor de claves de red 1135-a, un autenticador de UE 1140-a y un gestor de comunicación de UE 1210. El gestor de claves de red 1135-a y el autenticador de UE 1140-a pueden ser ejemplos del gestor de claves de red 1135 y el autenticador de UE 1140 descritos por referencia a la Figura 11. El autenticador de UE 1140-a puede incluir un derivador de claves de nodo de red 1205. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses).

El gestor de claves de red 1135-a puede usarse para recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. En algunos ejemplos, el primer conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos. En algunos ejemplos, el segundo conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE o una combinación de los mismos. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

El autenticador de UE 1140-a puede usarse para realizar al menos un procedimiento de autenticación con el UE basándose al menos en parte en la primera clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5. El derivador de claves de nodo de red 1205 puede usarse para realizar el al menos un procedimiento de autenticación con el UE que puede incluir derivar una segunda clave de seguridad para un nodo de red de la red celular. La segunda clave de seguridad puede basarse al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros. En algunos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE y el nodo de red, o una combinación de los mismos.

El gestor de comunicación de UE 1210 puede usarse para comunicarse con el UE a través del nodo de red basándose al menos en parte en la segunda clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5.

La Figura 13 muestra un diagrama 1300 de un nodo de red 1105-a, de acuerdo con diversos aspectos de la presente divulgación. El nodo de red 1105-a puede ser un ejemplo de aspectos de los nodos de red descritos por referencia a las Figuras 2, 4, 5 y 11.

El nodo de red 1105-a puede incluir un gestor de comunicación 1305, memoria 1310, un procesador 1320 y una interfaz de autenticación 1325. Cada uno de estos componentes puede comunicarse, directa o indirectamente, entre sí (por ejemplo, a través de uno o más buses). El gestor de comunicación 1305 puede ser un ejemplo de aspectos de los gestores de comunicación descritos por referencia a la Figura 11 o 12.

La memoria 1310 puede incluir RAM o ROM. La memoria 1310 puede almacenar *software* ejecutable por computadora, legible por computadora 1315, incluyendo instrucciones que, cuando se ejecutan, hacen que el procesador 1320 realice diversas funciones descritas en el presente documento, incluyendo funciones relacionadas con seguridad y autenticación de red. En algunos casos, el *software* 1315 puede no ser directamente ejecutable por el procesador 1320, pero puede hacer que el procesador 1320 (por ejemplo, cuando se compila y ejecuta) realice las funciones

descritas en el presente documento. El procesador 1320 puede incluir un dispositivo de *hardware* inteligente (por ejemplo, una CPU, un microcontrolador, un ASIC, etc.).

La interfaz de autenticación 1325 puede comunicarse bidireccionalmente, a través de una o más antenas o enlaces cableados, con una o más redes, nodos de red o UE, como se describe en el presente documento. En algunos ejemplos, la interfaz de autenticación 1325 puede usarse para establecer una conexión segura con un servidor de autenticación (por ejemplo, usando un protocolo Radius o Diameter) y facilitar un procedimiento de EAP realizado por un UE y el servidor de autenticación.

La Figura 14 muestra un diagrama de flujo que ilustra un método 1400 para comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación. Las operaciones del método 1400 pueden realizarse por un UE 115 o sus componentes, como se describe por referencia a las Figuras 1-8. En algunos ejemplos, las operaciones del método 1400 pueden realizarse por el gestor de comunicación inalámbrica descrito por referencia a las Figuras 6-8. En algunos ejemplos, un UE puede ejecutar un conjunto de códigos para controlar los elementos funcionales del UE para realizar las funciones descritas posteriormente. Además, o alternativamente, un UE puede realizar aspectos de las funciones descritas posteriormente utilizando *hardware* para usos especiales.

En el bloque 1405, un UE puede realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador, como se ha descrito anteriormente por referencia a la Figura 5. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. En ciertos ejemplos, las operaciones del bloque 1405 pueden realizarse usando el gestor de EAP 635 descrito por referencia a las Figuras 6 y 7.

En el bloque 1410, el UE puede derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos. En ciertos ejemplos, las operaciones del bloque 1410 pueden realizarse usando el gestor de EAP 635 descrito por referencia a las Figuras 6 y 7.

En el bloque 1415, el UE puede determinar un tipo de red asociado al autenticador, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el tipo de red determinado puede incluir un tipo de red celular o un tipo de red no celular (por ejemplo, un tipo de WLAN). En ciertos ejemplos, las operaciones del bloque 1415 pueden realizarse usando el identificador de tipo de red 640 descrito por referencia a las Figuras 6 y 7.

En el bloque 1420, el UE puede realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse al menos en parte en una asociación de la MSK o EMSK al tipo de red determinado, como se ha descrito anteriormente por referencia a la Figura 5. En ciertos ejemplos, las operaciones del bloque 1420 pueden realizarse usando el autenticador de red 645 descrito por referencia a las Figuras 6 y 7.

La Figura 15 muestra un diagrama de flujo que ilustra un método 1500 para comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación. Las operaciones del método 1500 pueden realizarse por un UE 115 o sus componentes, como se describe por referencia a las Figuras 1-8. En algunos ejemplos, las operaciones del método 1500 pueden realizarse por el gestor de comunicación inalámbrica descrito por referencia a las Figuras 6-8. En algunos ejemplos, un UE puede ejecutar un conjunto de códigos para controlar los elementos funcionales del UE para realizar las funciones descritas posteriormente. Además, o alternativamente, un UE puede realizar aspectos de las funciones descritas posteriormente usando *hardware* para usos especiales.

En el bloque 1505, un UE puede realizar un procedimiento de EAP con un servidor de autenticación a través de un autenticador, como se ha descrito anteriormente por referencia a la Figura 5. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación. En ciertos ejemplos, las operaciones del bloque 1505 pueden realizarse usando el gestor de EAP 635 descrito por referencia a las Figuras 6 y 7.

En el bloque 1510, el UE puede derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE o una combinación de los mismos. En ciertos ejemplos, las operaciones del bloque 1510 pueden realizarse usando el gestor de EAP 635 descrito por referencia a las Figuras 6 y 7.

En el bloque 1515, el UE puede determinar un tipo de red asociado al autenticador, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el tipo de red determinado puede incluir un tipo de red celular o un tipo de red no celular (por ejemplo, un tipo de WLAN). En ciertos ejemplos, las operaciones del bloque 1515 pueden realizarse usando el identificador de tipo de red 640 descrito por referencia a las Figuras 6 y 7.

En el bloque 1520, el método 1500 puede bifurcarse al bloque 1525 o 1540, dependiendo de si el tipo de red determinado incluye un tipo de red celular o un tipo de red no celular. Cuando el tipo de red determinado incluye un tipo de red celular, el método 1500 puede bifurcarse al bloque 1525. Cuando el tipo de red determinado incluye un tipo de red no celular, el método 1500 puede bifurcarse al bloque 1540. En ciertos ejemplos, las operaciones de bloque 1520 pueden realizarse usando el identificador de tipo de red 640 descrito por referencia a las Figuras 6 y 7. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas.

Si el UE determina que el tipo de red incluye un tipo de red celular, en los bloques 1525 y 1530, el UE puede realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador. El al menos un procedimiento de autenticación puede basarse en una asociación de la MSK o EMSK al tipo de red determinado. En el bloque 1525, el UE puede derivar una primera clave de seguridad para una red celular, como se ha descrito anteriormente por referencia a la Figura 5. La primera clave de seguridad puede basarse al menos en parte en la EMSK y un segundo conjunto de parámetros. En algunos ejemplos, el segundo conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos. En ciertos ejemplos, las operaciones del bloque 1525 pueden realizarse usando el autenticador de red 645 descrito por referencia a las Figuras 6 y 7, o el derivador de claves de red 705 descrito por referencia a la Figura 7.

En el bloque 1530, el UE puede derivar una segunda clave de seguridad para un nodo de red de la red celular, como se ha descrito anteriormente por referencia a la Figura 5. La segunda clave de seguridad puede basarse al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros. En algunos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE y el nodo de red, o una combinación de los mismos. En ciertos ejemplos, las operaciones del bloque 1530 pueden realizarse usando el autenticador de red 645 descrito por referencia a las Figuras 6 y 7, o el derivador de claves de nodo de red 710 descrito por referencia a la Figura 7.

En el bloque 1535, el UE puede comunicarse con la red celular a través del nodo de red basándose al menos en parte en la segunda clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5. En ciertos ejemplos, las operaciones del bloque 1530 pueden realizarse usando el gestor de comunicación de red celular 715 descrito por referencia a la Figura 7.

Si el UE determina que el tipo de red incluye un tipo de red no celular, en el bloque 1540, el UE puede derivar una primera clave de seguridad para una red no celular. La primera clave de seguridad puede basarse al menos en parte en la MSK y en un cuarto conjunto de parámetros. En ciertos ejemplos, las operaciones del bloque 1540 pueden realizarse usando el autenticador de red 645 descrito por referencia a las Figuras 6 y 7, o el derivador de claves de red 705 descrito por referencia a la Figura 7.

La Figura 16 muestra un diagrama de flujo que ilustra un método 1600 para comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación. Las operaciones del método 1600 pueden realizarse por un servidor de autenticación o sus componentes, como se describe por referencia a las Figuras 1-5, 9 y 10. En algunos ejemplos, las operaciones del método 1600 pueden realizarse por el gestor de autenticación descrito por referencia a las Figuras 9 y 10. En algunos ejemplos, un servidor de autenticación puede ejecutar un conjunto de códigos para controlar los elementos funcionales del servidor de autenticación para realizar las funciones descritas posteriormente. Además, o alternativamente, un servidor de autenticación puede realizar aspectos de las funciones descritas posteriormente utilizando *hardware* para usos especiales.

En el bloque 1605, un servidor de autenticación puede realizar un procedimiento de EAP con un UE a través de un autenticador, como se ha descrito anteriormente por referencia a la Figura 5. El procedimiento de EAP puede basarse al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE. En ciertos ejemplos, las operaciones del bloque 1605 pueden realizarse usando el gestor de EAP 935 descrito por referencia a la Figura 9.

En el bloque 1610, el servidor de autenticación puede derivar, como parte de la realización del procedimiento de EAP, una MSK y una EMSK que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el primer conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos. En ciertos ejemplos, las operaciones del bloque 1610 pueden realizarse usando el gestor de EAP 935 descrito por referencia a la Figura 9.

En el bloque 1615, el servidor de autenticación puede determinar un tipo de red asociado al autenticador, como se ha descrito anteriormente por referencia a la Figura 5. En algunos ejemplos, el tipo de red determinado puede incluir un tipo de red celular o un tipo de red no celular (por ejemplo, un tipo de WLAN). En ciertos ejemplos, las operaciones del bloque 1615 pueden realizarse usando el identificador de tipo de red 940 descrito por referencia a la Figura 9.

En el bloque 1620, el servidor de autenticación puede derivar una clave de seguridad para el tipo de red determinado basándose al menos en parte en una asociación de la MSK o EMSK al tipo de red, y basándose al menos en parte en un segundo conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. Cuando el tipo de red determinado incluye un tipo de red celular, y en algunos ejemplos, el segundo conjunto de parámetros puede incluir un identificador de una red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el servidor de autenticación y la red celular, o una combinación de los mismos. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas. En ciertos ejemplos, las operaciones del bloque 1620 pueden realizarse usando el derivador de claves de red 945 descrito por referencia a la Figura 9.

En el bloque 1625, el servidor de autenticación puede transmitir la clave de seguridad al autenticador a través de un canal seguro, como se ha descrito anteriormente por referencia a la Figura 5. En ciertos ejemplos, las operaciones del bloque 1625 pueden realizarse usando el instalador de claves de red 950 descrito por referencia a la Figura 9.

La Figura 17 muestra un diagrama de flujo que ilustra un método 1700 para comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación. Las operaciones del método 1700 pueden realizarse por una red celular o sus componentes, como se describe por referencia a las Figuras 1-5 y 11-13. En algunos ejemplos, las operaciones del método 1700 pueden realizarse por el gestor de comunicación descrito por referencia a las Figuras 11-13. En algunos ejemplos, una red celular (o uno o más nodos de la misma) puede ejecutar un conjunto de códigos para controlar los elementos funcionales de la red celular para realizar las funciones descritas posteriormente. Además, o alternativamente, una red celular (o uno o más nodos de la misma) puede realizar aspectos de las funciones descritas posteriormente usando *hardware* para usos especiales.

En el bloque 1705, una red celular puede recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. En algunos ejemplos, el primer conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos. En algunos ejemplos, el segundo conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas. En ciertos ejemplos, las operaciones del bloque 1705 pueden realizarse usando el gestor de claves de red 1135 descrito por referencia a la Figura 11.

En el bloque 1710, la red celular puede realizar al menos un procedimiento de autenticación con el UE basándose al menos en parte en la primera clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5. En ciertos ejemplos, las operaciones del bloque 1710 pueden realizarse usando el autenticador de UE 1140 descrito por referencia a la Figura 11.

La Figura 18 muestra un diagrama de flujo que ilustra un método 1800 para comunicación inalámbrica, de acuerdo con diversos aspectos de la presente divulgación. Las operaciones del método 1800 pueden realizarse por una red celular o sus componentes, como se describe por referencia a las Figuras 1-5 y 11-13. En algunos ejemplos, las operaciones del método 1800 pueden realizarse por el gestor de comunicación descrito por referencia a las Figuras 11-13. En algunos ejemplos, una red celular (o uno o más nodos de la misma) puede ejecutar un conjunto de códigos para controlar los elementos funcionales de la red celular para realizar las funciones descritas posteriormente. Además, o alternativamente, una red celular (o uno o más nodos de la misma) puede realizar aspectos de las funciones descritas posteriormente usando *hardware* para usos especiales.

En el bloque 1805, una red celular puede recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una EMSK y un primer conjunto de parámetros, como se ha descrito anteriormente por referencia a la Figura 5. La EMSK puede basarse al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros. Las credenciales de autenticación pueden intercambiarse entre un UE y el servidor de autenticación durante un procedimiento de EAP. En algunos ejemplos, el primer conjunto de parámetros puede incluir un identificador de la red celular, al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE y la red celular, o una combinación de los mismos. En algunos ejemplos, el segundo conjunto de parámetros puede incluir al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE o una combinación de los mismos. En algunos ejemplos, la red celular puede incluir al menos una de una red 5G, una red 4G, una red LTE, una red LTE-A, una red 3G, o una combinación de las mismas. En ciertos ejemplos, las operaciones del bloque 1805 pueden realizarse usando el gestor de claves de red 1135 descrito por referencia a la Figura 11.

En el bloque 1810, la red celular puede realizar al menos un procedimiento de autenticación con el UE basándose al menos en parte en la primera clave de seguridad. La realización del al menos un procedimiento de autenticación con el UE puede incluir derivar una segunda clave de seguridad para un nodo de red de la red celular, como se ha descrito

anteriormente por referencia a la Figura 5. La segunda clave de seguridad puede basarse al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros. En algunos ejemplos, el tercer conjunto de parámetros puede incluir un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE y el nodo de red, o una combinación de los mismos. En ciertos ejemplos, las operaciones del bloque 1810 pueden realizarse usando el autenticador de UE 1140 descrito por referencia a la Figura 11, o el derivador de claves de nodo de red 1205 descrito por referencia a la Figura 12.

En el bloque 1815, la red celular puede comunicarse con el UE a través del nodo de red basándose al menos en parte en la segunda clave de seguridad, como se ha descrito anteriormente por referencia a la Figura 5. En ciertos ejemplos, las operaciones del bloque 1815 pueden realizarse usando el gestor de comunicación de UE 1210 descrito por referencia a la Figura 12.

Se ha de indicar que los métodos descritos anteriormente ilustran posibles implementaciones de las técnicas descritas en la presente divulgación. En algunos ejemplos, las operaciones de los métodos pueden realizarse en diferentes órdenes o incluir diferentes operaciones.

Las técnicas descritas en el presente documento pueden usarse para diversos sistemas de comunicación inalámbrica tales como CDMA, TDMA, FDMA, OFDMA, SC-FDMA y otros sistemas. Los términos "sistema" y "red" se utilizan a menudo de forma intercambiable. Un sistema CDMA puede implementar una tecnología de radio como CDMA2000, acceso por radio terrestre universal (UTRA), etc. CDMA2000 cubre los estándares IS-2000, IS-95 e IS-856. Las versiones 0 y A de IS-2000 pueden denominarse CDMA2000 IX, IX, etc. IS-856 (TIA-856) puede denominarse CDMA2000 1xEV-DO, paquetes de datos de alta velocidad (HRPD), etc. UTRA incluye banda ancha CDMA (WCDMA) y otras variantes de CDMA. Un sistema TDMA puede implementar una tecnología de radio tal como el sistema global para las comunicaciones móviles (GSM). Un sistema OFDMA puede implementar una tecnología de radio tal como banda ancha ultra móvil (UMB), UTRA evolucionado (E-UTRA), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM™, etc. UTRA y E-UTRA forman parte del sistema universal de telecomunicaciones móviles (UMTS). 3GPP LTE y LTE-A son nuevas versiones de UMTS que usan E-UTRA. UTRA, E-UTRA, UMTS, LTE, LTE-A y GSM se describen en documentos de una organización denominada 3GPP. CDMA2000 y UMB se describen en documentos de una organización denominada "Proyecto asociación de tercera generación 2" (3GPP2). Las técnicas descritas en el presente documento pueden usarse para los sistemas y tecnologías de radio mencionados anteriormente, así como para otros sistemas y tecnologías de radio, incluyendo comunicaciones celulares (por ejemplo, LTE) en un ancho de banda compartido o sin licencia. Sin embargo, la descripción anterior describe un sistema LTE/LTE-A a modo de ejemplo, y la terminología LTE se usa en gran parte de la descripción anterior, aunque las técnicas son aplicables más allá de las aplicaciones LTE/LTE-A.

La descripción detallada expuesta anteriormente en relación con los dibujos adjuntos describe ejemplos y no representa todos los ejemplos que pueden implementarse o que están dentro del alcance de las reivindicaciones. Los términos "ejemplo" y la expresión "a modo de ejemplo", cuando se usan en la presente descripción, significan "que sirve como ejemplo, caso o ilustración" y no "preferente" o "ventajoso sobre otros ejemplos". La descripción detallada incluye detalles específicos con el fin de proporcionar una comprensión de las técnicas descritas. Sin embargo, estas técnicas pueden ponerse en práctica sin estos detalles específicos. En algunos casos, se muestran estructuras y aparatos bien conocidos en forma de diagrama de bloques para evitar complicar los conceptos de los ejemplos descritos.

La información y señales pueden representarse usando cualquiera de una diversidad de tecnologías y técnicas diferentes. Por ejemplo, los datos, instrucciones, comandos, información, señales, bits, símbolos y chips a los que se puede hacer referencia en la descripción anterior pueden estar representados por tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos, o cualquier combinación de los mismos.

Los diversos bloques y componentes ilustrativos descritos en relación con la divulgación en el presente documento pueden implementarse o realizarse con un procesador de uso general, un procesador de señal digital (DSP), un ASIC, un FPGA u otro dispositivo lógico, puerta discreta o lógica de transistor programable, 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, alternativamente, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estado convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, microprocesadores múltiples, uno o más microprocesadores junto con un núcleo DSP, o cualquier otra de tales configuraciones.

Las funciones descritas en el presente documento pueden implementarse en *hardware*, *software* ejecutado por un procesador, *firmware*, o cualquier combinación de los mismos. Si se implementa en *software* ejecutado por un procesador, las funciones pueden almacenarse o transmitirse como una o más instrucciones o código en un medio legible por computadora. Otros ejemplos e implementaciones están dentro del alcance de la divulgación y las reivindicaciones adjuntas. Por ejemplo, debido a la naturaleza del *software*, las funciones descritas anteriormente pueden implementarse usando *software* ejecutado por un procesador, *hardware*, *firmware*, cableado, o combinaciones

de cualquiera de estos. Los componentes que implementan funciones también pueden estar ubicados físicamente en diversas posiciones, incluyendo distribuidos de modo que partes de las funciones se implementen en diferentes ubicaciones físicas. Como se usa en el presente documento, incluyendo en las reivindicaciones, el término "o", cuando se usa en una lista de dos o más elementos, significa que cualquiera de los elementos enumerados puede emplearse por sí mismo, o puede emplearse cualquier combinación de dos o más de los elementos enumerados. Por ejemplo, si se describe que una composición contiene los componentes A, B o C, la composición puede contener solo A; solo B; solo C; A y B en combinación; A y C en combinación; B y C en combinación; o A, B y C en combinación. Además, como se usa en el presente documento, incluyendo en las reivindicaciones, "o" usado en una lista de elementos (por ejemplo, una lista de elementos precedida por una expresión tal como "al menos uno de" o "uno o más de") indica una lista disyuntiva tal que, por ejemplo, una lista de "al menos uno de A, B o C" significa A o B o C o AB o AC o BC o ABC (es decir, A y B y C).

Los medios legibles por computadora incluyen tanto medios de almacenamiento como medios de comunicación informáticos, incluyendo cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que se pueda acceder mediante una computadora de uso general o de uso especial. A modo de ejemplo, y no de limitación, los medios legibles por computadora pueden comprender RAM, ROM, EEPROM, memoria *flash*, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para transportar o almacenar medios deseados de código informático en forma de instrucciones o estructuras de datos y al que se pueda acceder mediante una computadora de uso general o de uso especial, o un procesador de uso general o de uso especial. Además, cualquier conexión se denomina adecuadamente medio legible por computadora. Por ejemplo, si el *software* se transmite desde un sitio *web*, servidor u otra fuente remota usando un cable coaxial, cable de fibra óptica, par trenzado, línea de suscriptor digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, cable de fibra óptica, par trenzado, DSL o tecnologías inalámbricas tales como infrarrojos, radio y microondas se incluyen en la definición de medio. Disco (incluyendo los términos *disk* y *disc* del inglés), como se usa en el presente documento, incluye disco compacto (CD), disco láser, disco óptico, disco versátil digital (DVD), disquete y disco Blu-ray, donde los discos (*disks*) generalmente reproducen datos magnéticamente, mientras que los discos (*discs*) reproducen datos ópticamente con láseres. Las combinaciones de los anteriores también están incluidas dentro del alcance de los medios legibles por computadora.

La descripción anterior de la divulgación se proporciona para permitir que un experto en la materia realice o use la divulgación. Diversas modificaciones de la divulgación resultarán muy evidentes para los expertos en la materia, y los principios genéricos definidos en el presente documento pueden aplicarse a otras variaciones sin desviarse del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para comunicación inalámbrica en un equipo de usuario, UE, (115) que comprende:

realizar un procedimiento de protocolo de autenticación extensible, EAP, con un servidor de autenticación (245) a través de un autenticador (235), el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE (115) y el servidor de autenticación (245);
derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra, MSK, y una clave de sesión maestra extendida, EMSK, que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros;
determinar un tipo de red asociado al autenticador (235); y
realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador (235), el al menos un procedimiento de autenticación basado en una asociación de la MSK o la EMSK al tipo de red determinado.

2. El método de la reivindicación 1, en donde el tipo de red determinado comprende un tipo de red celular y realizar el al menos un procedimiento de autenticación con el autenticador (235) comprende:

derivar una primera clave de seguridad para una red celular (205), la primera clave de seguridad basada al menos en parte en la EMSK y un segundo conjunto de parámetros;

en particular, en donde el segundo conjunto de parámetros comprende: un identificador de la red celular (205), al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE (115) y la red celular (205), o una combinación de los mismos; o
en particular, en donde realizar el al menos un procedimiento de autenticación con el autenticador (235) comprende:

derivar una segunda clave de seguridad para un nodo de red de la red celular (205), la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros; y comunicar con la red celular (205) a través del nodo de red basándose al menos en parte en la segunda clave de seguridad;
además, en particular, en donde el tercer conjunto de parámetros comprende: un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE (115) y el nodo de red, o una combinación de los mismos.

3. El método de la reivindicación 1, en donde el primer conjunto de parámetros comprende: al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos; o

en donde una red celular (205) asociada al autenticador (235) comprende al menos una de: una red de quinta generación, 5G, una red de cuarta generación, 4G, una red de Evolución a Largo Plazo, LTE, una red LTE Avanzada, LTE-A, una red de tercera generación, 3G, o una combinación de las mismas; o
en donde el tipo de red determinado es un tipo de red no celular y realizar el al menos un procedimiento de autenticación con el autenticador (235) comprende:
derivar una primera clave de seguridad para una red no celular, la primera clave de seguridad basada al menos en parte en la MSK y un segundo conjunto de parámetros.

4. Un aparato para comunicación inalámbrica en un equipo de usuario, UE, (115), que comprende:

medios para realizar un procedimiento de protocolo de autenticación extensible, EAP, con un servidor de autenticación (245) a través de un autenticador (235), el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE (115) y el servidor de autenticación (245);
medios para derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra, MSK, y una clave de sesión maestra extendida, EMSK, que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros;
medios para determinar un tipo de red asociado al autenticador (235); y
medios para realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador (235), el al menos un procedimiento de autenticación basado en una asociación de la MSK o la EMSK al tipo de red determinado.

5. El aparato de la reivindicación 4, en donde el tipo de red determinado comprende un tipo de red celular y los medios para realizar el al menos un procedimiento de autenticación comprenden:

medios para derivar una primera clave de seguridad para una red celular (205), la primera clave de seguridad basada al menos en parte en la EMSK y un segundo conjunto de parámetros;

en particular, en donde el segundo conjunto de parámetros comprende: un identificador de la red celular (205), al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE (115) y la red celular (205), o una combinación de los mismos; o
en particular, en donde los medios para realizar el al menos un procedimiento de autenticación comprenden:

medios para derivar una segunda clave de seguridad para un nodo de red de la red celular (205), la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros; y
medios para comunicar con la red celular (205) a través del nodo de red basándose al menos en parte en la segunda clave de seguridad;
además, en particular, en donde el tercer conjunto de parámetros comprende: un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE (115) y el nodo de red, o una combinación de los mismos.

6. El aparato de la reivindicación 4, en donde el primer conjunto de parámetros comprende: al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos; o

en donde una red celular (205) asociada al autenticador (235) comprende al menos una de: una red de quinta generación, 5G, una red de cuarta generación, 4G, una red de Evolución a Largo Plazo, LTE, una red LTE Avanzada, LTE-A, una red de tercera generación, 3G, o una combinación de las mismas; o
en donde el tipo de red determinado es un tipo de red no celular y los medios para realizar el al menos un procedimiento de autenticación comprenden:
medios para derivar una primera clave de seguridad para una red no celular, la primera clave de seguridad basada al menos en parte en la MSK y un segundo conjunto de parámetros.

7. Un método para comunicación inalámbrica en un servidor de autenticación (245), que comprende:

realizar un procedimiento de protocolo de autenticación extensible, EAP, con un equipo de usuario, UE, (115) a través de un autenticador (235), el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación (245) y el UE (115);
derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra, MSK, y una clave de sesión maestra extendida, EMSK, que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros;
determinar un tipo de red asociado al autenticador (235);
derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red, y basada al menos en parte en un segundo conjunto de parámetros; y
transmitir la clave de seguridad al autenticador (235) a través de un canal seguro.

8. El método de la reivindicación 7, en donde el primer conjunto de parámetros comprende: al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos; o

en donde el tipo de red determinado comprende un tipo de red celular y el segundo conjunto de parámetros comprende: un identificador de una red celular (205), al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el servidor de autenticación (245) y la red celular (205), o una combinación de los mismos;
en particular, en donde la red celular (205) comprende al menos una de: una red de quinta generación, 5G, una red de cuarta generación, 4G, una red de Evolución a Largo Plazo, LTE, una red LTE Avanzada, LTE-A, una red de tercera generación, 3G, o una combinación de las mismas.

9. Un aparato para comunicación inalámbrica en un servidor de autenticación (245), que comprende:

medios para realizar un procedimiento de protocolo de autenticación extensible, EAP, con un equipo de usuario, UE, (115) a través de un autenticador (235), el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación (245) y el UE (115);
medios para derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra, MSK, y una clave de sesión maestra extendida, EMSK, que se basan al menos en parte en las credenciales de autenticación y un primer conjunto de parámetros;
medios para determinar un tipo de red asociado al autenticador (235);
medios para derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red determinado, y basada al menos en parte en un segundo conjunto de parámetros; y
medios para transmitir la clave de seguridad al autenticador (235) a través de un canal seguro.

10. El aparato de la reivindicación 9, en donde el primer conjunto de parámetros comprende: al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos; o

en donde el tipo de red determinado comprende un tipo de red celular y el segundo conjunto de parámetros comprende: un identificador de una red celular (205), al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el servidor de autenticación (245) y la red celular (205), o una combinación de los mismos; o
en donde la red celular (205) comprende al menos una de: una red de quinta generación, 5G, una red de cuarta generación, 4G, una red de Evolución a Largo Plazo, LTE, una red LTE Avanzada, LTE-A, una red de tercera generación, 3G, o una combinación de las mismas.

11. Un método para comunicación inalámbrica en una red celular (205), que comprende:

determinar, en un servidor de autenticación (245), un tipo de red asociado a un autenticador (235);
derivando el servidor de autenticación (245) una primera clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de una clave de sesión maestra, MSK, o una clave de sesión maestra extendida, EMSK, al tipo de red y basada en un primer conjunto de parámetros, en donde la MSK y la EMSK se basan al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros, y transmitir dicha clave de seguridad al autenticador (235) a través de un canal seguro;
recibir, en el autenticador (235) asociado a la red celular (205) y desde el servidor de autenticación (245), dicha primera clave de seguridad, las credenciales de autenticación intercambiadas entre un equipo de usuario, UE, (115) y el servidor de autenticación (245) durante un procedimiento de protocolo de autenticación extensible, EAP; y
realizar, mediante el autenticador (235), al menos un procedimiento de autenticación con el UE (115) basado al menos en parte en la primera clave de seguridad.

12. El método de la reivindicación 11, en donde realizar el al menos un procedimiento de autenticación con el UE (115) comprende:

derivar una segunda clave de seguridad para un nodo de red de la red celular (205), la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros; y comunicar con el UE (115) a través del nodo de red basándose al menos en parte en la segunda clave de seguridad;

en particular, en donde el tercer conjunto de parámetros comprende: un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE (115) y el nodo de red, o una combinación de los mismos; o
el método de la reivindicación 11, en donde el primer conjunto de parámetros comprende: un identificador de la red celular (205), al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE (115) y la red celular (205), o una combinación de los mismos; o
en donde el segundo conjunto de parámetros comprende: al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos; o
en donde la red celular (205) comprende al menos una de: una red de quinta generación, 5G, una red de cuarta generación, 4G, una red de Evolución a Largo Plazo, LTE, una red LTE Avanzada, LTE-A, una red de tercera generación, 3G, o una combinación de las mismas.

13. Un sistema para comunicación inalámbrica en una red celular (205), que comprende:

medios para determinar, en un servidor de autenticación (245), un tipo de red asociado a un autenticador (235);
medios para derivar, en el servidor de autenticación (245), una primera clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de una clave de sesión maestra, MSK, o una clave de sesión maestra extendida, EMSK, al tipo de red y basada en un primer conjunto de parámetros, en donde la MSK y la EMSK se basan al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros, y transmitir dicha clave de seguridad al autenticador (235) a través de un canal seguro
medios para recibir, en el autenticador (235) asociado a la red celular (205) y desde el servidor de autenticación (245), dicha primera clave de seguridad, las credenciales de autenticación intercambiadas entre un equipo de usuario, UE, (115) y el servidor de autenticación (245) durante un procedimiento de protocolo de autenticación extensible, EAP; y
medios para realizar, en el autenticador (235), al menos un procedimiento de autenticación con el UE (115) basado al menos en parte en la primera clave de seguridad.

14. El sistema de la reivindicación 13, en donde los medios para realizar el al menos un procedimiento de autenticación con el UE (115) comprenden:

medios para derivar una segunda clave de seguridad para un nodo de red de la red celular (205), la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros; y
medios para comunicar con el UE (115) a través del nodo de red basándose al menos en parte en la segunda clave de seguridad;

en particular, en donde el tercer conjunto de parámetros comprende: un identificador del nodo de red, al menos un parámetro específico de nodo de red, al menos un parámetro intercambiado entre el UE (115) y el nodo de red, o una combinación de los mismos; o

el sistema de la reivindicación 13, en donde el primer conjunto de parámetros comprende: un identificador de la red celular (205), al menos un parámetro específico de red celular, al menos un parámetro intercambiado entre el UE (115) y la red celular (205), o una combinación de los mismos; o
en donde el segundo conjunto de parámetros comprende: al menos un identificador, al menos un número aleatorio, al menos un parámetro de red, al menos un parámetro de UE, o una combinación de los mismos; o
en donde la red celular (205) comprende al menos una de: una red de quinta generación, 5G, una red de cuarta generación, 4G, una red de Evolución a Largo Plazo, LTE, una red LTE Avanzada, LTE-A, una red de tercera generación, 3G, o una combinación de las mismas.

15. Programas informáticos que comprenden código ejecutable por computadora para realizar, respectivamente, el método de acuerdo con cualquiera de las reivindicaciones 1 a 3 cuando se ejecuta en un equipo de usuario, UE, o el método de acuerdo con las reivindicaciones 7 u 8 cuando se ejecuta en un servidor de autenticación o el método de acuerdo con las reivindicaciones 11 o 12 cuando se ejecuta en una red celular.

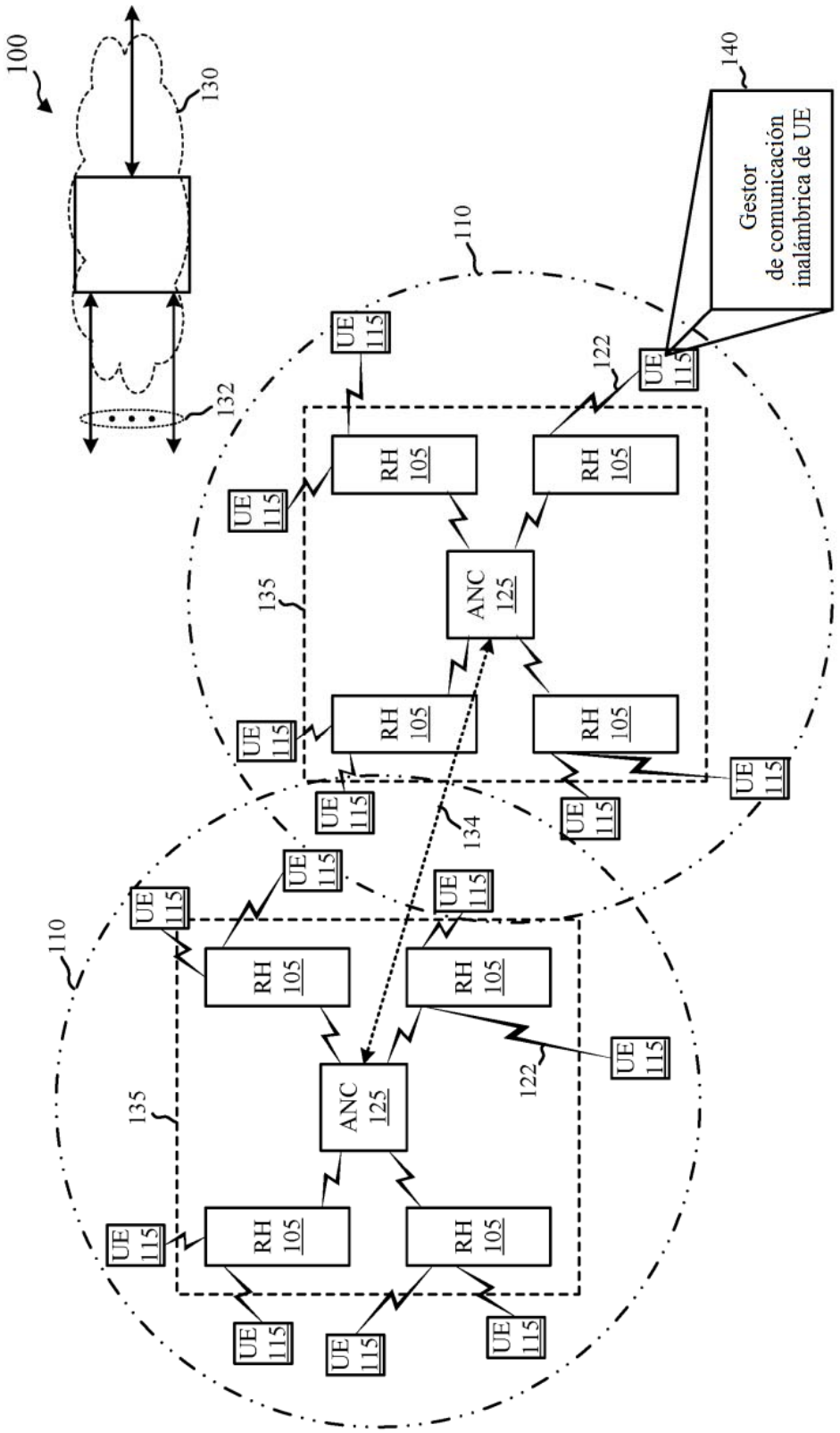
100
130
132
140
Gestor de comunicación inalámbrica de UE
110
122
135
134
ANC 125
RH 105
UE 115

FIG. 1

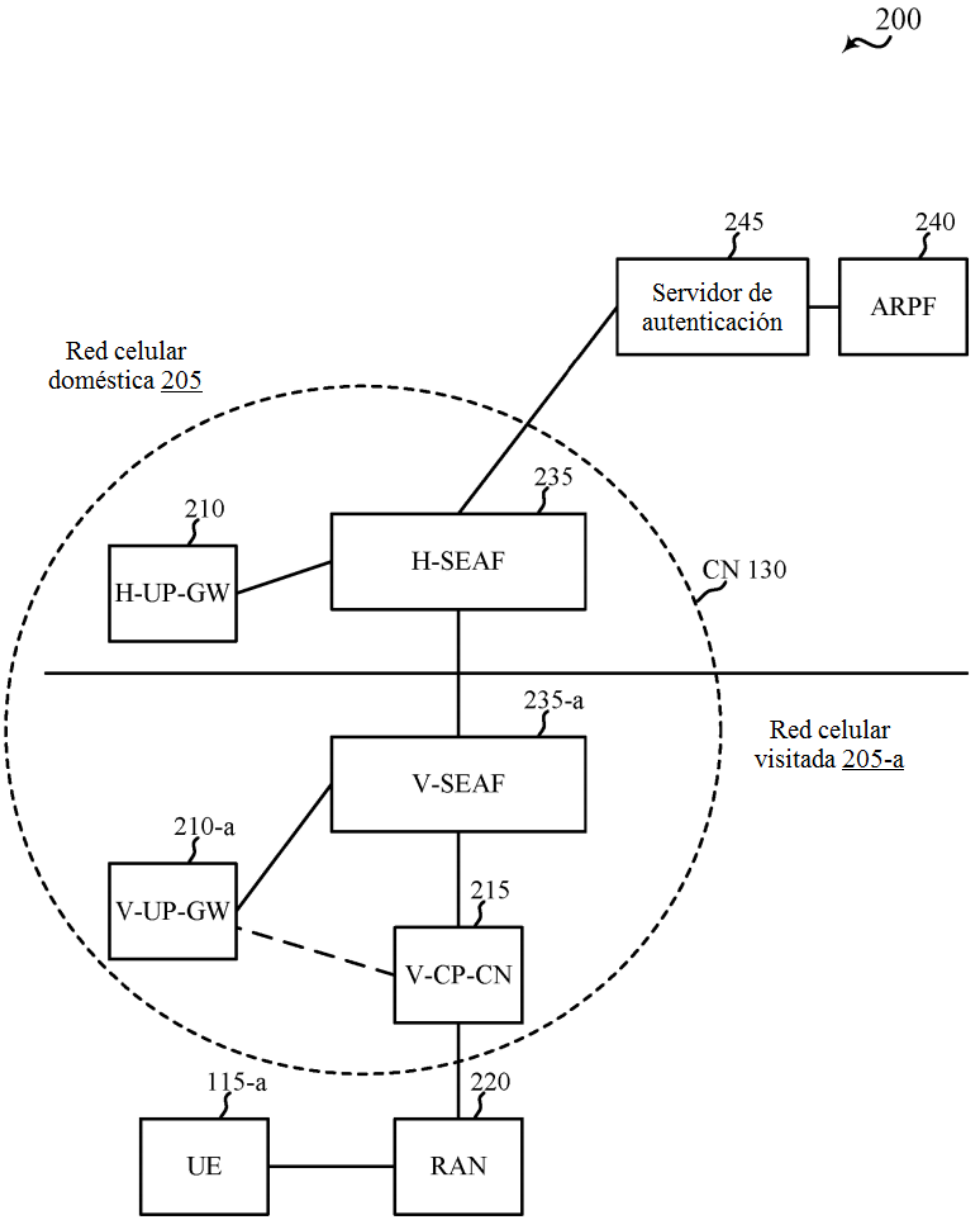
200
245
240
Servidor de autenticación
ARPF
Red celular doméstica 205
235
210
H-SEAF
H-UP-GW
CN 130
235-a
Red celular visitada 205-a
V-SEAF
210-a
215
V-UP-GW
V-CP-CN
115-a
220
UE
RAN

FIG. 2

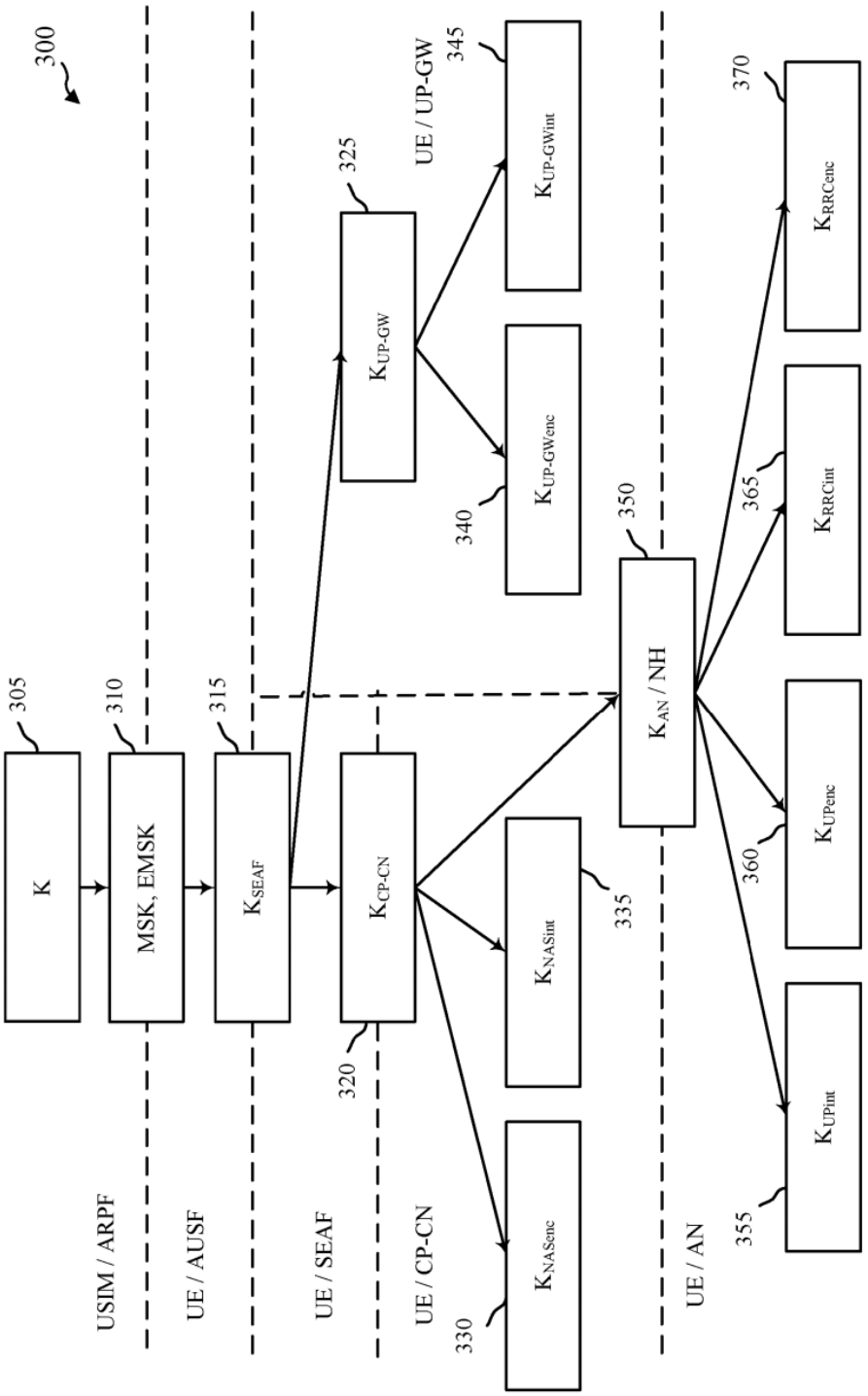
300
305
K
310
MSK, EMSK
315
K_{SEAF}
320
K_{CP-CN}
325
K_{UP-GW}
330
K_{NASenc}
335
K_{NASint}
340
$K_{UP-GWenc}$
345
$K_{UP-GWint}$
350
K_{AN} / NH
355
K_{UPint}
360
K_{UPenc}
365
K_{RRCint}
370
K_{RRCenc}
USIM / ARPF
UE / AUSF
UE / SEAF
UE / CP-CN
UE / UP-GW
UE / AN

FIG. 3

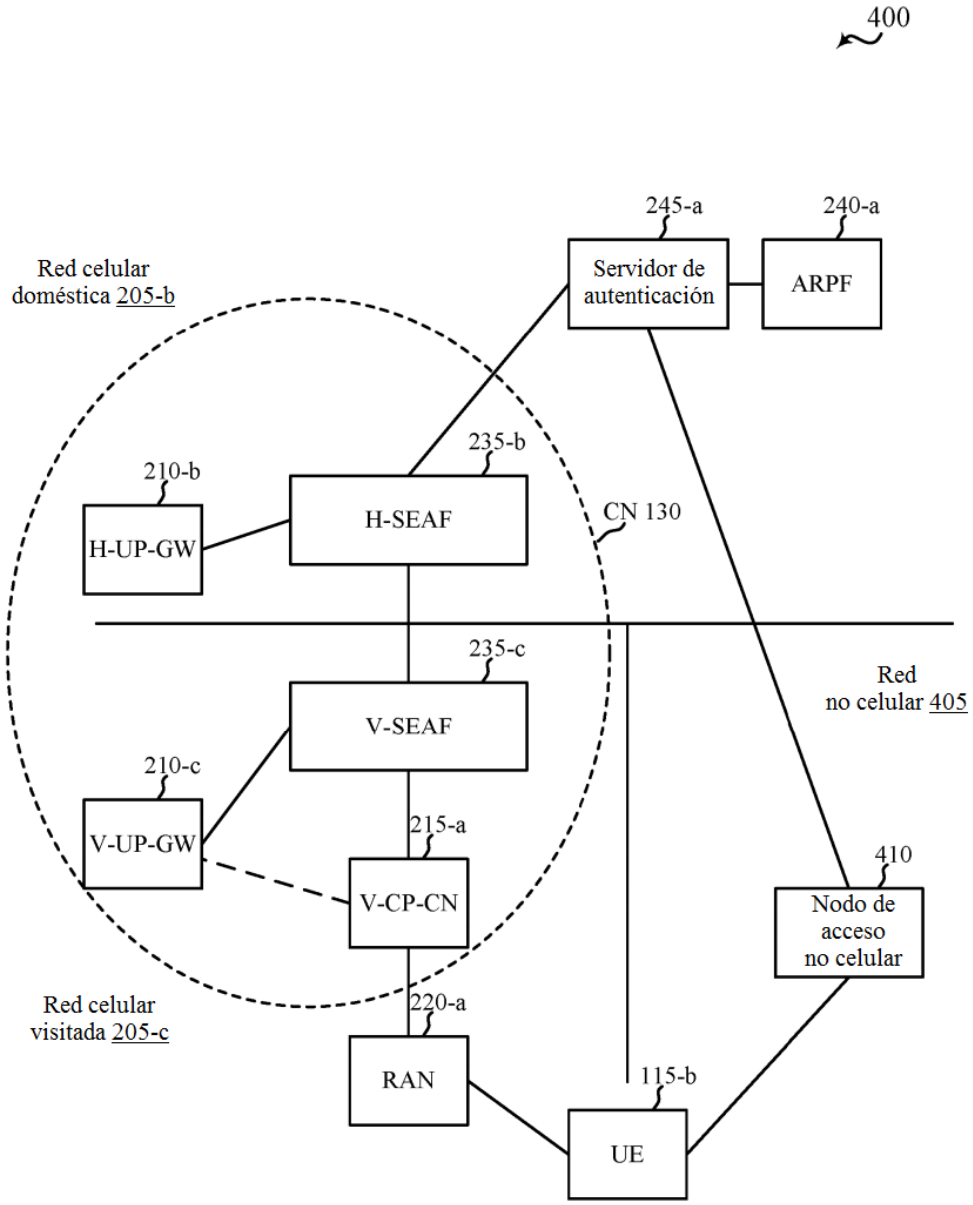
400
245-a
240-a
Servidor de autenticación
ARPF
Red celular doméstica 205-b
235-b
210-b
H-SEAF
H-UP-GW
CN 130
235-c
Red no celular 405
V-SEAF
210-c
V-UP-GW
215-a
410
V-CP-CN
Nodo de acceso no celular
Red celular visitada 205-c
220-a
RAN
115-b
UE

FIG. 4

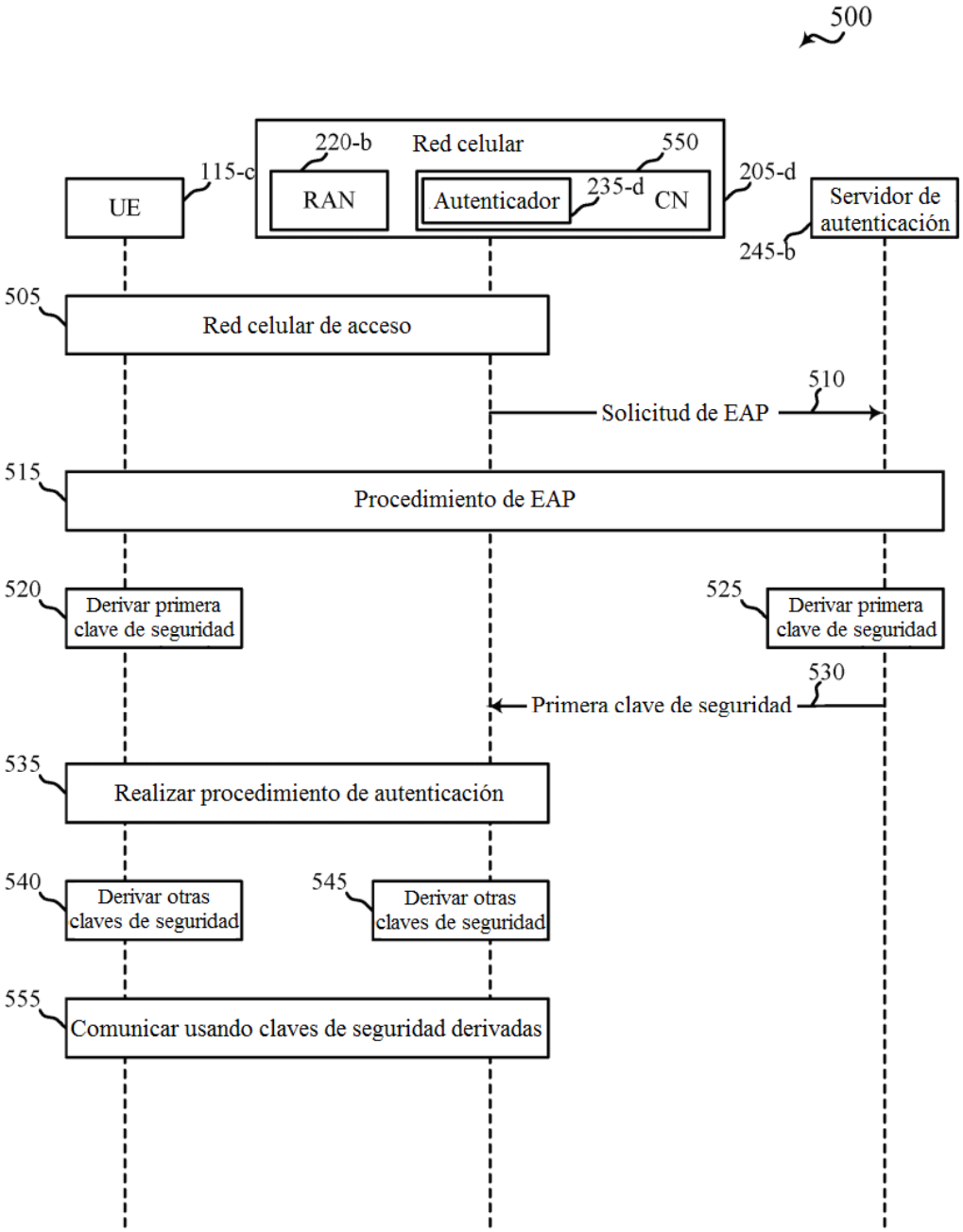
500
220-b
Red celular
550
115-c
205-d
UE
RAN
Autenticador
235-d
CN
Servidor de autenticación
245-b
505
Red celular de acceso
510
Solicitud de EAP
515
Procedimiento de EAP
520
Derivar primera clave de seguridad
525
Derivar primera clave de seguridad
530
Primera clave de seguridad
535
Realizar procedimiento de autenticación
540
Derivar otras claves de seguridad
545
Derivar otras claves de seguridad
555
Comunicar usando claves de seguridad derivadas

FIG. 5

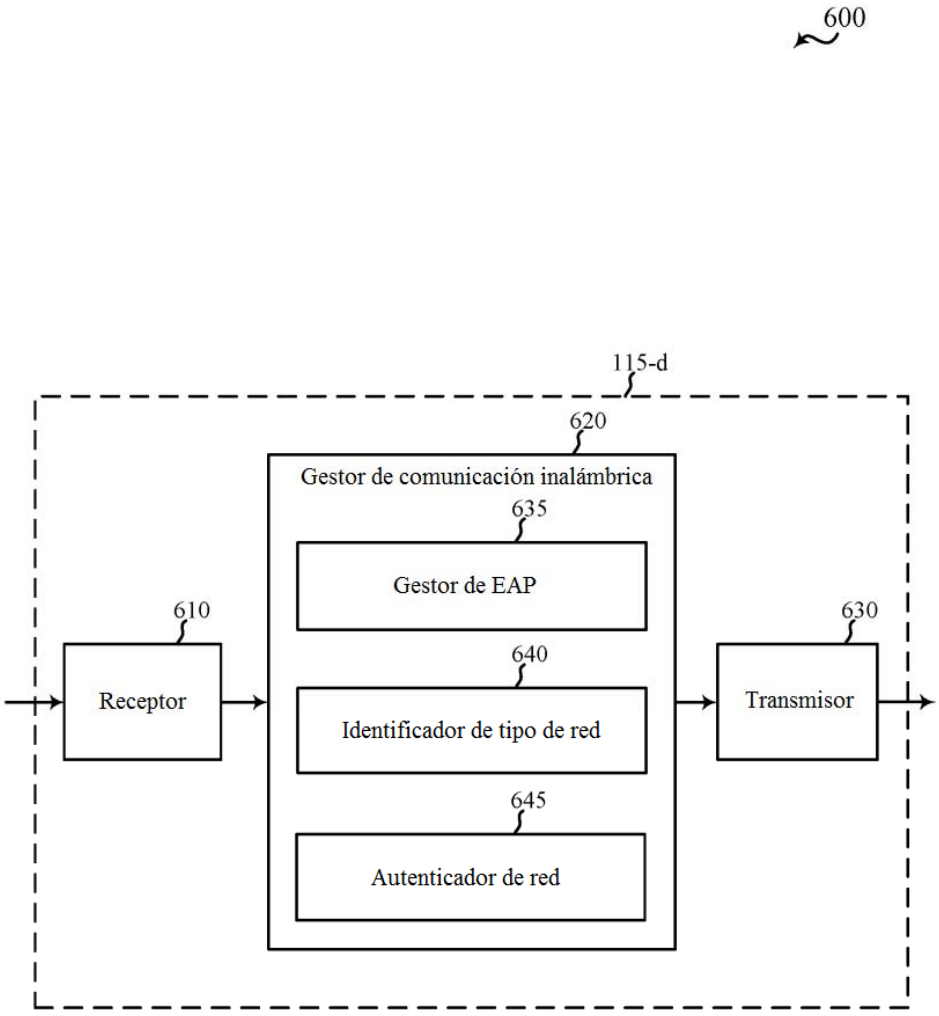
600
115-d
620
Gestor de comunicación inalámbrica
635
Gestor de EAP
610
Receptor
640
Identificador de tipo de red
630
Transmisor
645
Autenticador de red

FIG. 6

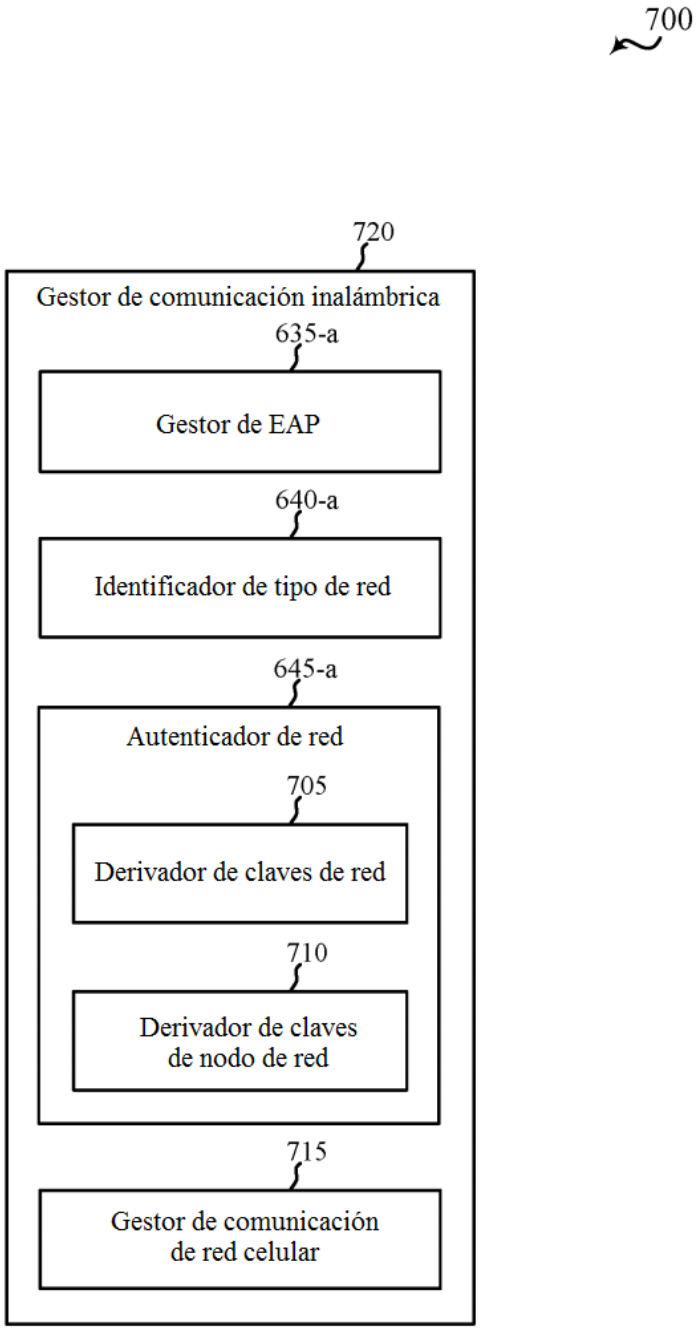
700
720
Gestor de comunicación inalámbrica
635-a
Gestor de EAP
640-a
Identificador de tipo de red
645-a
Autenticador de red
705
Derivador de claves de red
710
Derivador de claves de nodo de red
715
Gestor de comunicación de red celular

FIG. 7

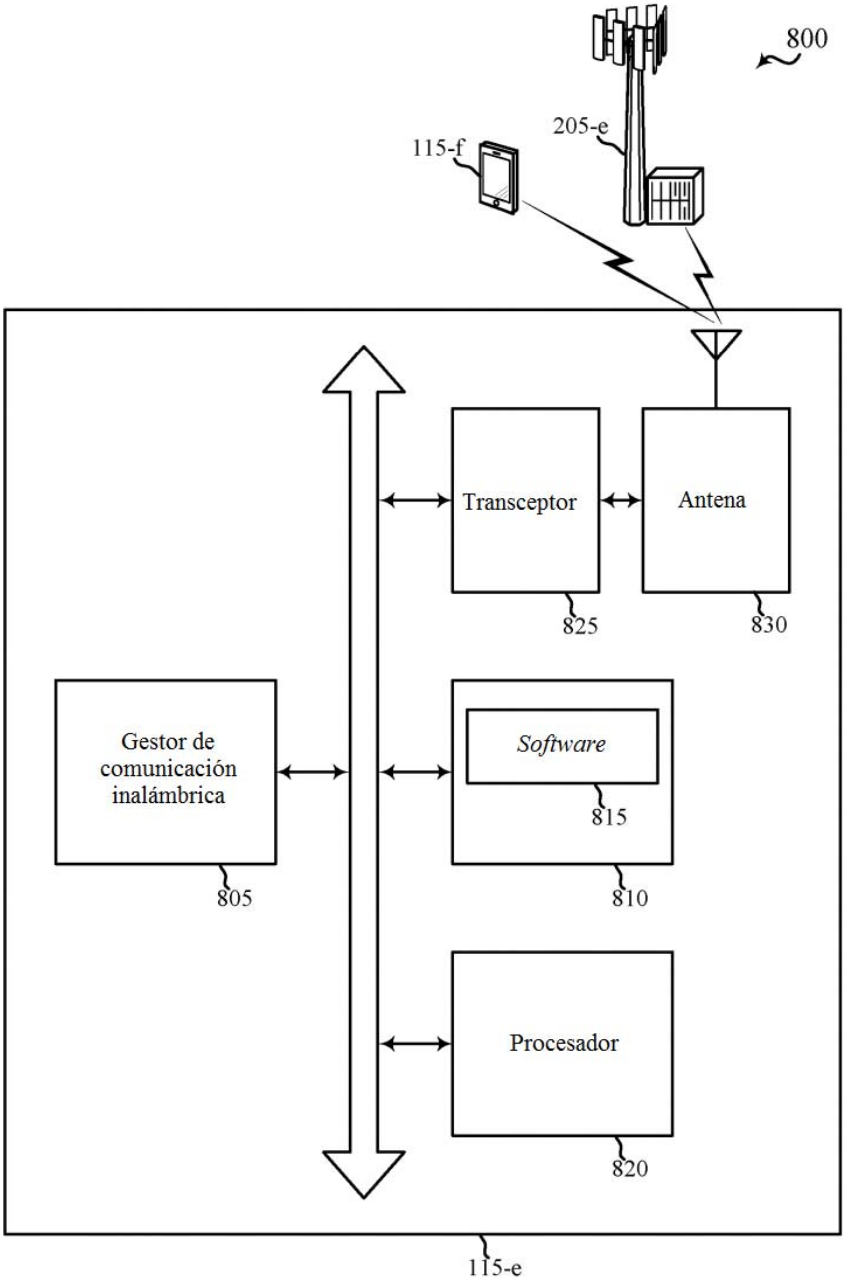
800
205-e
115-f
Transceptor
Antena
825
830
Gestor de comunicación inalámbrica
Software
815
805
810
Procesador
820
115-e

FIG. 8

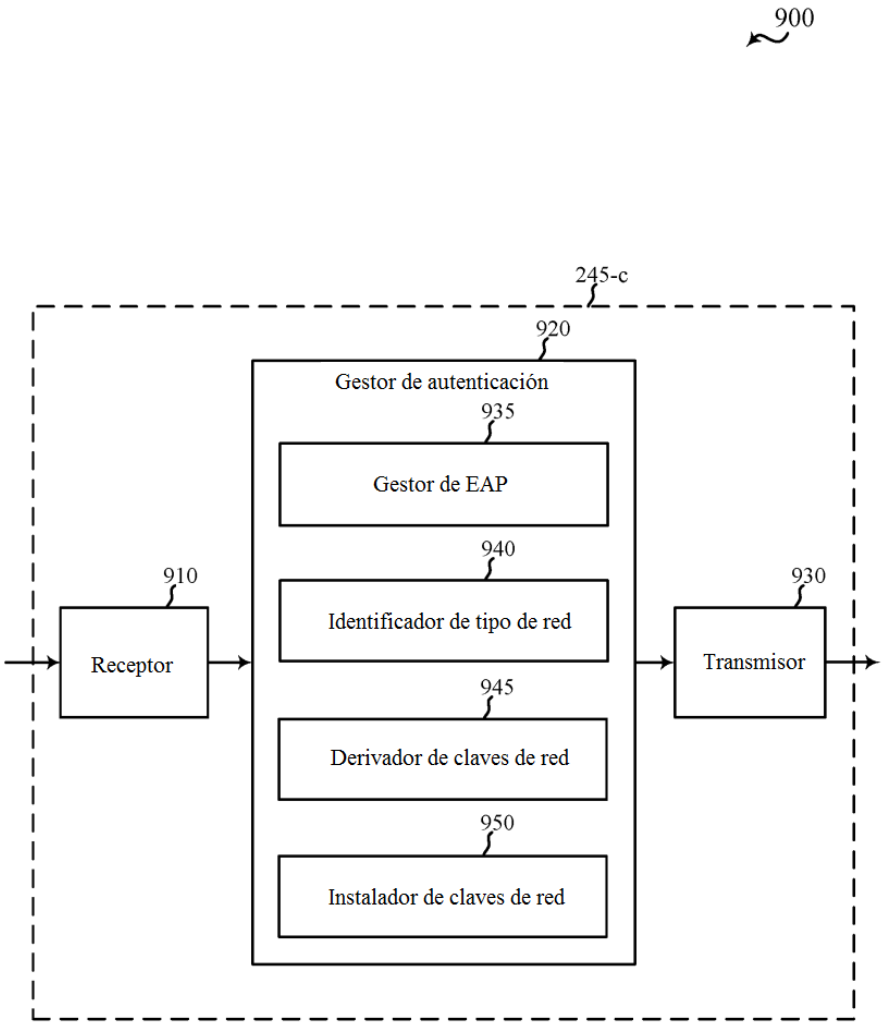
900
245-c
920
Gestor de autenticación
935
Gestor de EAP
940
Identificador de tipo de red
945
Derivador de claves de red
950
Instalador de claves de red
910
Receptor
930
Transmisor

FIG. 9

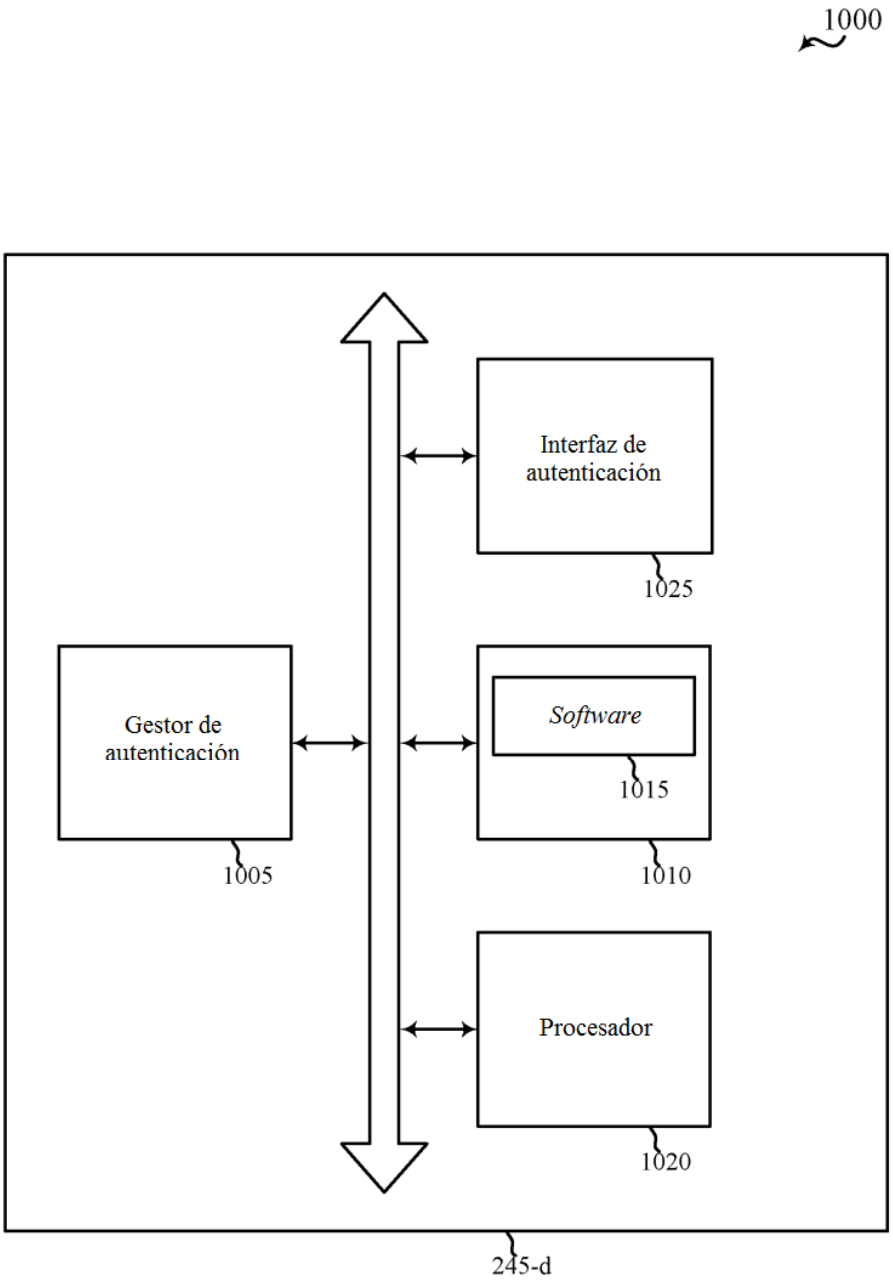
1000
Interfaz de autenticación
1025
Gestor de autenticación
1005
Software
1015
1010
Procesador
1020
245-d

FIG. 10

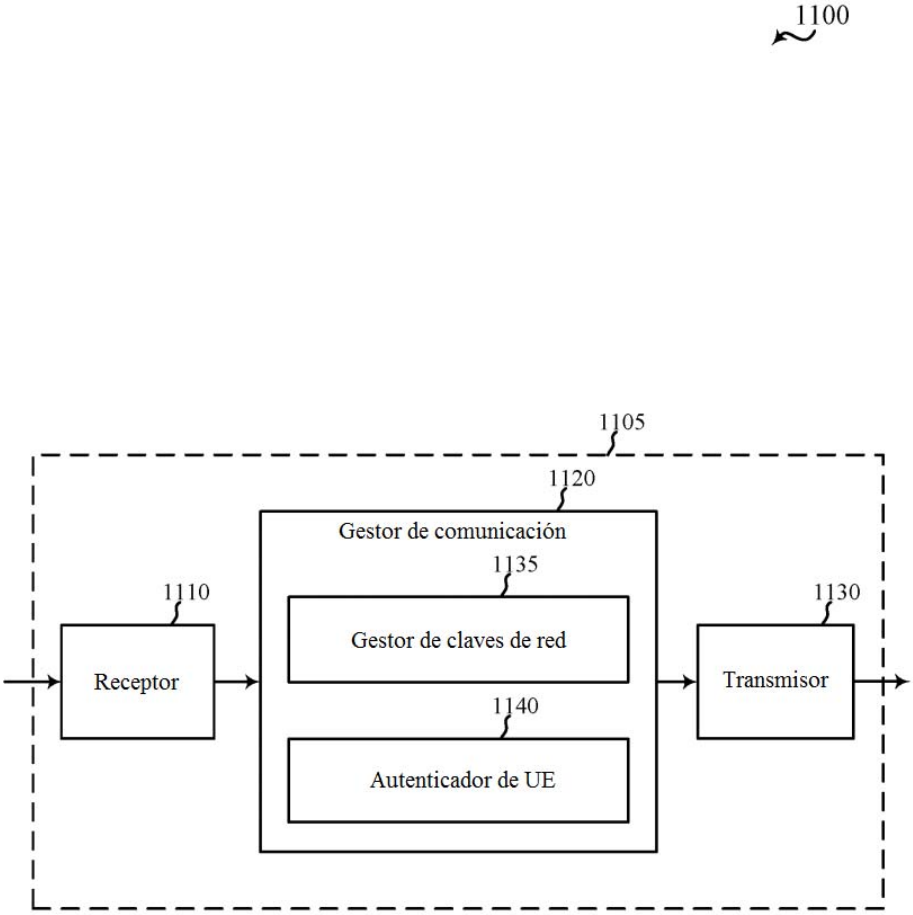
1100
1105
1120
Gestor de comunicación
1135
Gestor de claves de red
1110
Receptor
1130
Transmisor
1140
Autenticador de UE

FIG. 11

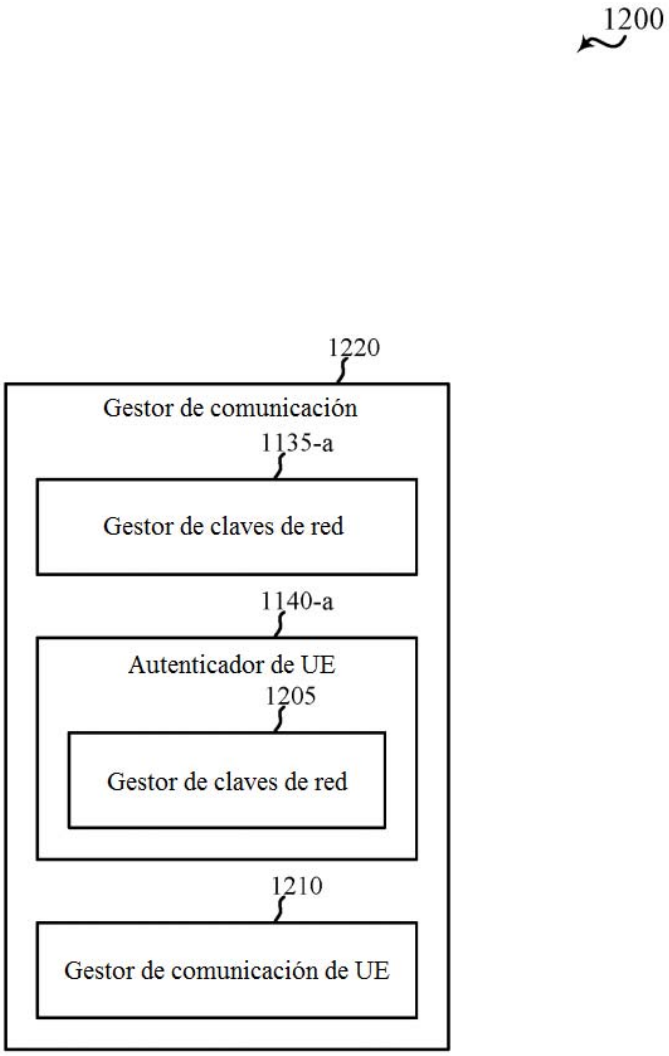
1200
1220
Gestor de comunicación
1135-a
Gestor de claves de red
1140-a
Autenticador de UE
1205
Gestor de claves de red
1210
Gestor de comunicación de UE

FIG. 12

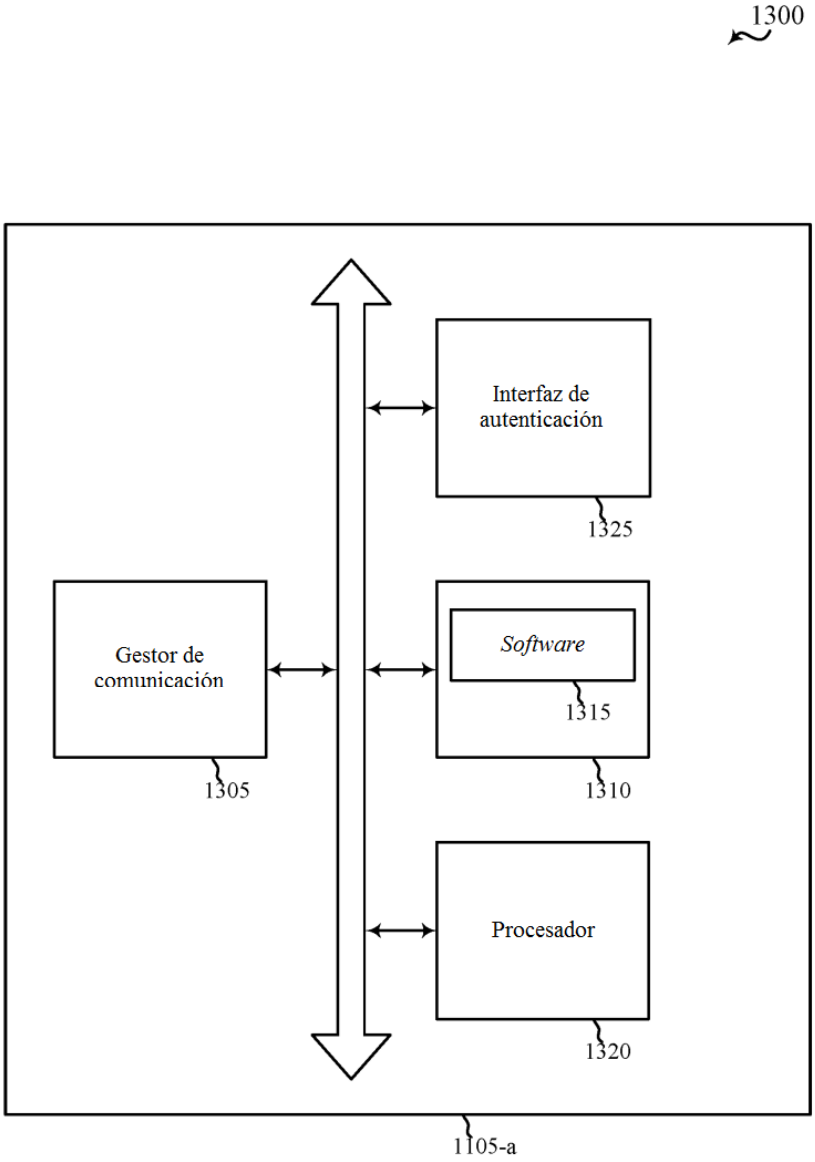
1300
Interfaz de autenticación
1325
Gestor de comunicación
Software
1315
1305
1310
Procesador
1320
1105-a

FIG. 13

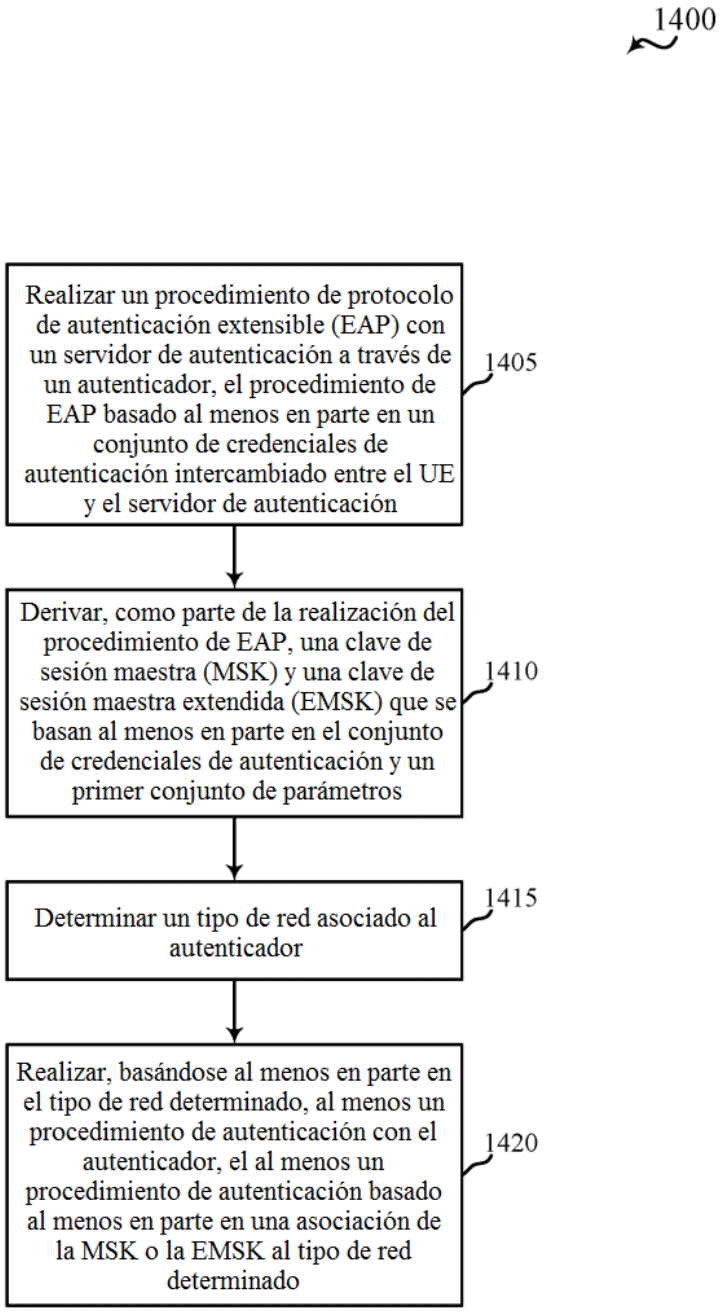
1400
Realizar un procedimiento de protocolo de autenticación extensible (EAP) con un servidor de autenticación a través de un autenticador, el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación
1405
Derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra (MSK) y una clave de sesión maestra extendida (EMSK) que se basan al menos en parte en el conjunto de credenciales de autenticación y un primer conjunto de parámetros
1410
Determinar un tipo de red asociado al autenticador
1415
Realizar, basándose al menos en parte en el tipo de red determinado, al menos un procedimiento de autenticación con el autenticador, el al menos un procedimiento de autenticación basado al menos en parte en una asociación de la MSK o la EMSK al tipo de red determinado
1420

FIG. 14

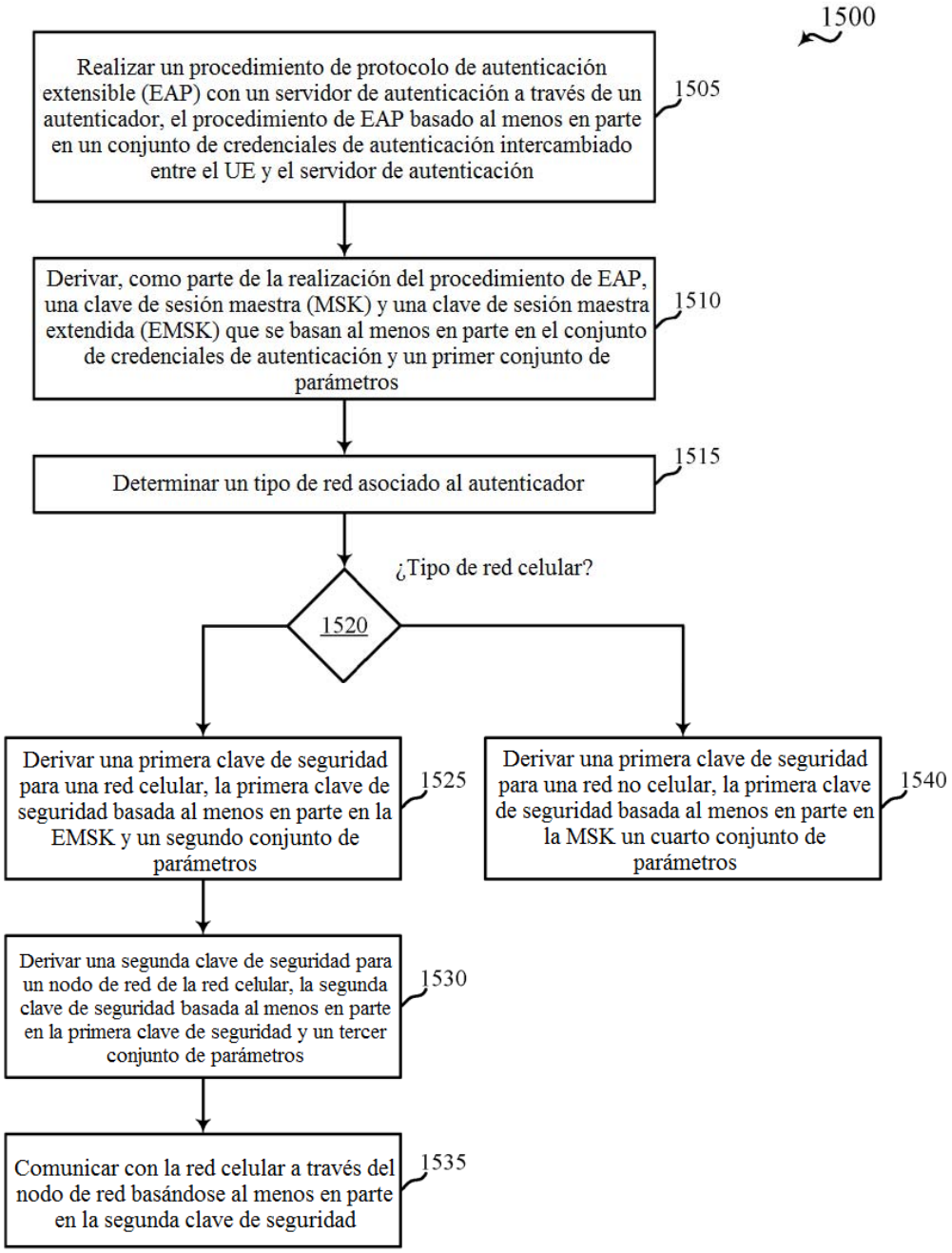
1500
Realizar un procedimiento de protocolo de autenticación extensible (EAP) con un servidor de autenticación a través de un autenticador, el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el UE y el servidor de autenticación
1505
Derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra (MSK) y una clave de sesión maestra extendida (EMSK) que se basan al menos en parte en el conjunto de credenciales de autenticación y un primer conjunto de parámetros
1510
Determinar un tipo de red asociado al autenticador
1515
¿Tipo de red celular?
1520
Derivar una primera clave de seguridad para una red celular, la primera clave de seguridad basada al menos en parte en la EMSK y un segundo conjunto de parámetros
1525
Derivar una primera clave de seguridad para una red no celular, la primera clave de seguridad basada al menos en parte en la MSK un cuarto conjunto de parámetros
1540
Derivar una segunda clave de seguridad para un nodo de red de la red celular, la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros
1530
Comunicar con la red celular a través del nodo de red basándose al menos en parte en la segunda clave de seguridad
1535

FIG. 15

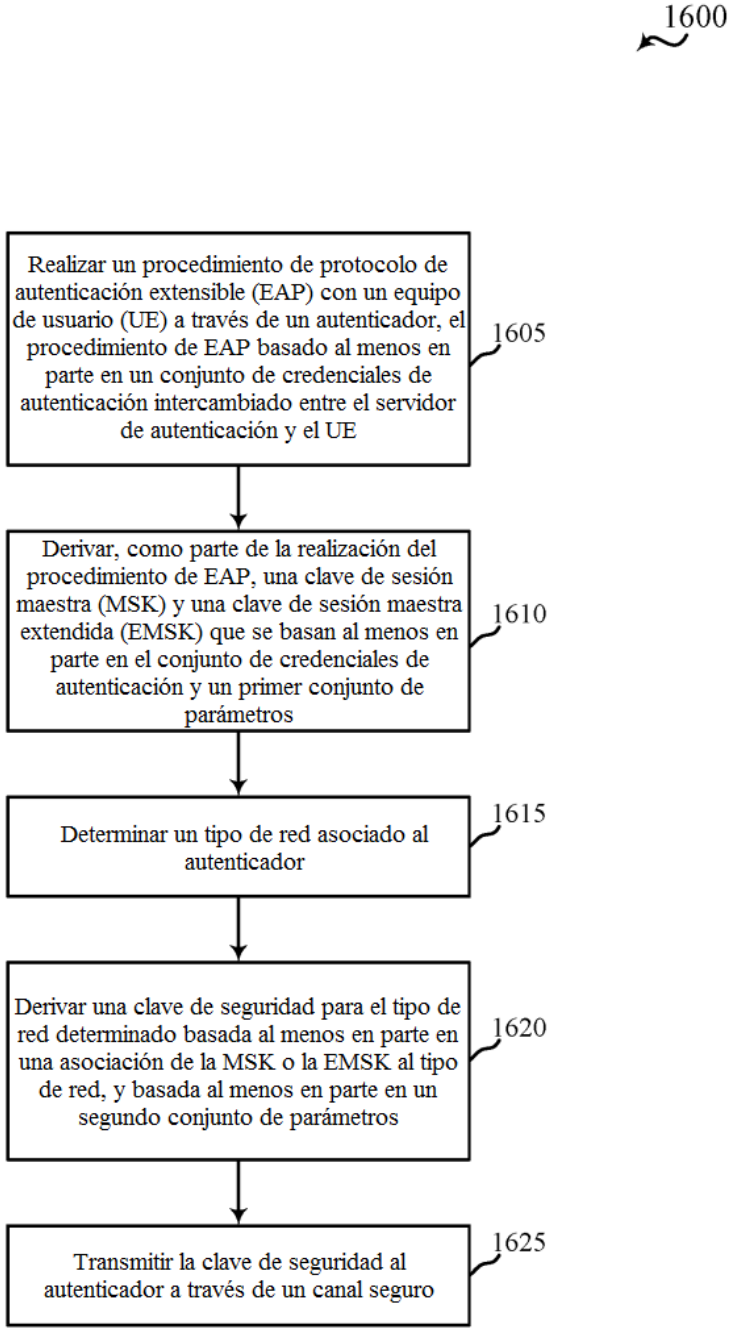
1600
Realizar un procedimiento de protocolo de autenticación extensible (EAP) con un equipo de usuario (UE) a través de un autenticador, el procedimiento de EAP basado al menos en parte en un conjunto de credenciales de autenticación intercambiado entre el servidor de autenticación y el UE
1605
Derivar, como parte de la realización del procedimiento de EAP, una clave de sesión maestra (MSK) y una clave de sesión maestra extendida (EMSK) que se basan al menos en parte en el conjunto de credenciales de autenticación y un primer conjunto de parámetros
1610
Determinar un tipo de red asociado al autenticador
1615
Derivar una clave de seguridad para el tipo de red determinado basada al menos en parte en una asociación de la MSK o la EMSK al tipo de red, y basada al menos en parte en un segundo conjunto de parámetros
1620
Transmitir la clave de seguridad al autenticador a través de un canal seguro
1625

FIG. 16

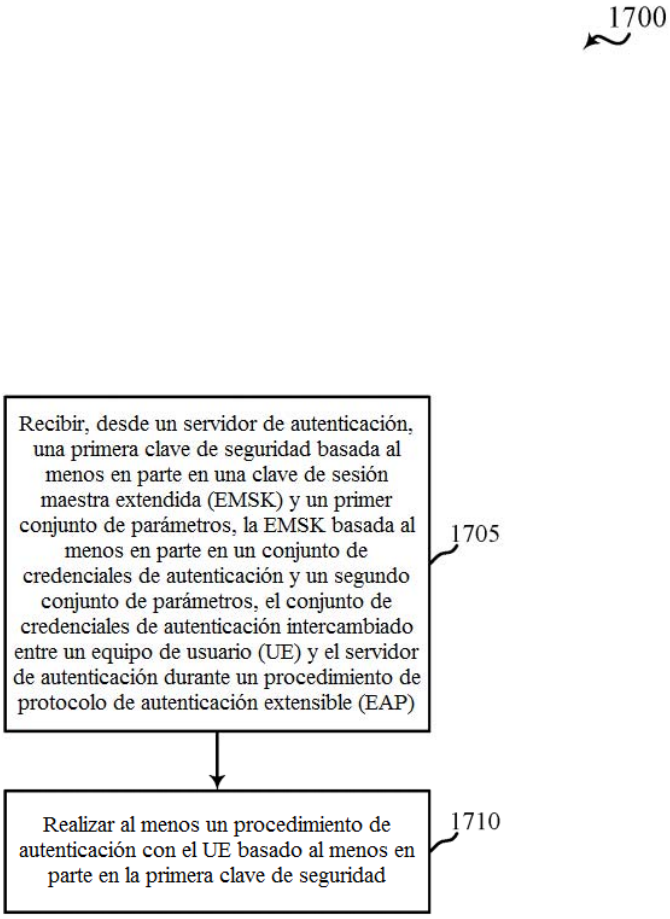
1700
Recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una clave de sesión maestra extendida (EMSK) y un primer conjunto de parámetros, la EMSK basada al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros, el conjunto de credenciales de autenticación intercambiado entre un equipo de usuario (UE) y el servidor de autenticación durante un procedimiento de protocolo de autenticación extensible (EAP)
1705
Realizar al menos un procedimiento de autenticación con el UE basado al menos en parte en la primera clave de seguridad
1710

FIG. 17

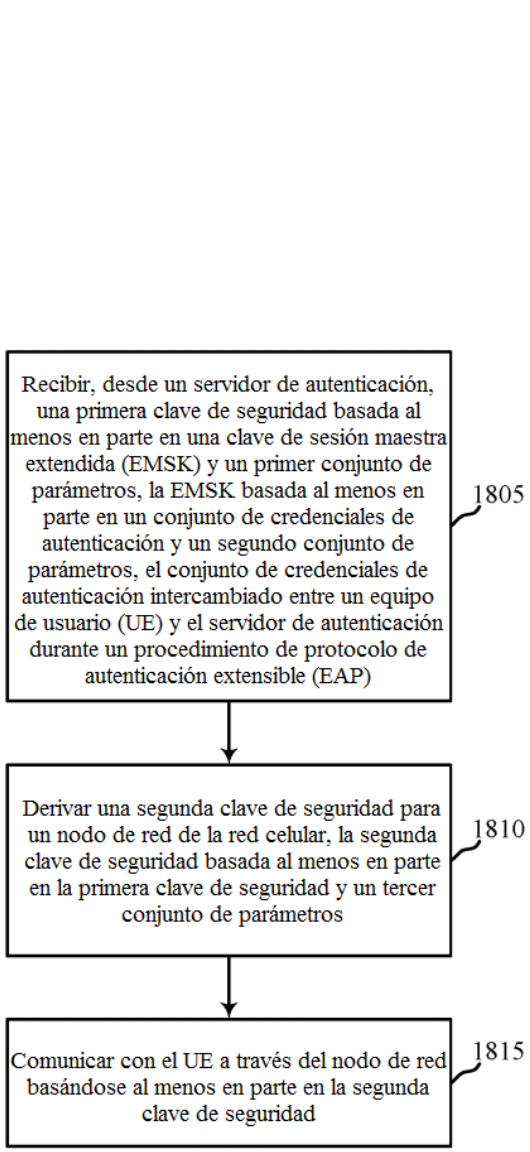
1800
Recibir, desde un servidor de autenticación, una primera clave de seguridad basada al menos en parte en una clave de sesión maestra extendida (EMSK) y un primer conjunto de parámetros, la EMSK basada al menos en parte en un conjunto de credenciales de autenticación y un segundo conjunto de parámetros, el conjunto de credenciales de autenticación intercambiado entre un equipo de usuario (UE) y el servidor de autenticación durante un procedimiento de protocolo de autenticación extensible (EAP)
1805
Derivar una segunda clave de seguridad para un nodo de red de la red celular, la segunda clave de seguridad basada al menos en parte en la primera clave de seguridad y un tercer conjunto de parámetros
1810
Comunicar con el UE a través del nodo de red basándose al menos en parte en la segunda clave de seguridad
1815

FIG. 18