(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 765 892**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 60/00 (2009.01)
H04W 76/14 (2008.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 9/08 (2006.01)
H04W 92/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.06.2013 PCT/CN2013/078054**

(87) Fecha y número de publicación internacional: **31.12.2014 WO14205697**

(96) Fecha de presentación y número de la solicitud europea: **26.06.2013 E 13888415 (0)**

(97) Fecha y número de publicación de la concesión europea: **30.10.2019 EP 3014801**

(54) Título: **Métodos y aparatos para generar claves en las comunicaciones de dispositivo a dispositivo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.06.2020

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

LIU, YANG y
ZHANG, DA JIANG

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Métodos y aparatos para generar claves en las comunicaciones de dispositivo a dispositivo

Campo de la invención

La presente invención generalmente se refiere a comunicaciones de dispositivo a dispositivo controladas por la red. De manera más específica, la invención se refiere a métodos mejorados para generar claves de criptografía en comunicaciones de dispositivo a dispositivo (en lo sucesivo, también denominado "D2D") y aparatos relacionados.

Antecedentes

Con el desarrollo del futuro servicio, sistemas de comunicación inalámbrica de próxima generación, como el sistema 3GPP (Proyecto de Asociación de Tercera Generación) LTE (evolución a largo plazo) y más allá, sistema IMT-A (Telecomunicaciones Móviles Internacionales - Avanzado) etc., se introducen para satisfacer la alta velocidad, gran capacidad y una alta calidad de servicio (QoS) para miles de millones de suscriptores. En este sentido, se han realizado esfuerzos para realizar comunicaciones D2D controladas por la red para reducir la carga en la red de comunicación celular. Los ejemplos de tales comunicaciones D2D incluyen comunicaciones directas entre un grupo de dispositivos de proximidad y comunicaciones D2D autónomas en una red celular. En tales comunicaciones D2D controladas por la red, dispositivos como equipos de usuario (UE) o terminales se comunican directamente entre sí, en lugar de transmitir datos de un dispositivo a otro a través de la red celular (en particular a través de un nodo de acceso o estación base del mismo), en el que el control primario y las configuraciones, tales como configuraciones de canal / portadora, puede ser realizado por la red celular.

La protección de seguridad puede ser un problema para las comunicaciones D2D controladas por la red, por ejemplo, porque los usuarios malintencionados pueden espiar la comunicación D2D si no se utiliza una protección de seguridad sólida entre los UE pares que realizan una comunicación D2D directa. Según el mecanismo de seguridad actual, La generación de claves para las comunicaciones D2D controladas por la red son gestionadas y controladas por la red central. La red central, especialmente aparatos para la gestión de claves (como la MME (Entidad de Gestión de Movilidad)), el HSS (Servidor de Abonado Local) y / o similares) deben participar en un establecimiento y negociación clave de cada conexión D2D. Esto puede aumentar considerablemente la carga de señalización de la red central, por ejemplo, en un caso en que el número de UE que realizan comunicaciones D2D es enorme.

En vista de esto, Sería un avance en la técnica proporcionar una manera de disminuir la carga de señalización de una red central en una generación clave de comunicaciones D2D.

El documento WO 2011/117677 describe métodos para la gestión de claves de dispositivo a dispositivo (D2D). En una realización de ejemplo de la figura 4, el eNB distribuye la información utilizada para compartir las claves de seguridad D2D pares. En 400, el eNB 120 determina que los terminales móviles 150 deberían pasar a una conexión D2D, y el eNB 120 envía una petición de claves de seguridad D2D a la MME 110. En respuesta a la petición del eNB 120, la MME 110, en 405, se puede configurar para generar los valores base (por ejemplo, valor base a y valor base b), que pueden ser números aleatorios o pseudoaleatorios. En 410, la MME 110 puede configurarse para generar la clave de seguridad D2D a y la clave de seguridad D2D b utilizando la misma clave secreta que utilizan los terminales móviles (por ejemplo, KAsME, n) vía, por ejemplo, una función de derivación clave. La MME 110 también se puede configurar para combinar la clave de seguridad D2D a con la clave de seguridad D2D b para generar o determinar un valor de combinación de clave de seguridad D2D en 415. En 420, la MME 110 puede configurarse para enviar los valores base (por ejemplo, valor base a y valor base b) y el valor de combinación de clave de seguridad D2D para el eNB 120. En respuesta a la recepción del valor de combinación de clave de seguridad D2D, el eNB 120, en 425a y 425b, puede configurarse para enviar el valor de combinación de clave de seguridad D2D y los valores base respectivos a los terminales móviles 150. En respuesta a la recepción de los mensajes en 425a y 425b, los terminales móviles 150 pueden configurarse para generar sus respectivas claves de seguridad D2D.

El documento WO 2012/137633 describe un método en el que la clave K_x se usa para transmitir y recibir la señal de datos entre la estación móvil UE#1 y la estación móvil UE#2 a través de la interfaz Ud. En una realización, las claves K_eNB no son gestionadas por un nodo de gestión móvil MME (excepto que los M_EKB generan las K_eNB por primera vez durante el establecimiento de la comunicación), pero administrado solo por la estación base de radio eNB y la estación móvil respectiva. K_x es generada por K_AsMEs (entidad de administración de seguridad de acceso). K_x es generada por la K AsME de las estaciones móviles y se transmite a las estaciones móviles.

El documento US 2008/298328 se refiere a la comunicación directa entre dos dispositivos cliente inalámbricos y divulga que dos dispositivos, STA-A y STA-B, pueden comunicar tramas de datos cifrados entre sí, utilizando una clave transitoria por pares (PTK) derivada de la clave maestra por pares (PMK) como clave de cifrado mediante un protocolo de enlace de 4 vías.

ALGUNAS REALIZACIONES DE EJEMPLO

Para superar las limitaciones descritas anteriormente, y para superar otras limitaciones que serán evidentes al leer y comprender la presente memoria, la divulgación proporciona un enfoque para generar claves de criptografía en las comunicaciones D2D sin introducir demasiada carga de señalización en una red central.

La invención se define en las reivindicaciones independientes adjuntas.

De acuerdo con una realización, un método comprende derivar en un primer equipo de usuario, una primera clave basada en un primer parámetro de seguridad y una clave compartida entre un aparato de red central y el primer equipo de usuario. El método comprende además enviar una notificación de servicios de dispositivo a dispositivo a un segundo equipo de usuario. El método comprende además recibir un segundo parámetro de seguridad del segundo equipo de usuario, en el que el segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave por un aparato de red de acceso en el que está registrado el primer equipo de usuario. El método comprende además derivar en el primer equipo de usuario, la segunda clave basada en el segundo parámetro de seguridad y la primera clave, para proteger una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario.

En algunas realizaciones a modo de ejemplo, derivar la primera clave comprende enviar un mensaje de petición al aparato de red central, indicando una capacidad de comunicación de dispositivo a dispositivo del primer equipo de usuario; y recibir los primeros parámetros de seguridad del aparato de red central. El primer equipo de usuario puede volver al modo inactivo después de recibir los primeros parámetros de seguridad.

En algunas realizaciones a modo de ejemplo, el método puede comprender además registrar el primer equipo de usuario en el aparato de red de acceso con una información de ubicación del área de registro de dispositivo a dispositivo del primer equipo de usuario.

De acuerdo con otra realización, un aparato que comprende al menos un procesador y al menos una memoria que incluye código de programa de ordenador, la al menos una memoria y el código del programa de ordenador configurado para, con el al menos un procesador, hacer que, al menos en parte, el aparato para derivar en un primer equipo de usuario, una primera clave basada en un primer parámetro de seguridad y una clave compartida entre un aparato de red central y el primer equipo de usuario. Además, se hace que el aparato envíe una notificación de servicios de dispositivo a dispositivo a un segundo equipo de usuario. Además, se hace que el aparato reciba un segundo parámetro de seguridad del segundo equipo de usuario, en el que el segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave por un aparato de red de acceso en el que está registrado el primer equipo de usuario. El aparato se deriva además en el primer equipo de usuario, la segunda clave basada en el segundo parámetro de seguridad y la primera clave, para proteger una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario.

De acuerdo con otra realización, un medio de almacenamiento legible por ordenador que lleva una o más secuencias de una o más instrucciones que, cuando se ejecutan por uno o varios procesadores, hacer que, al menos en parte, un aparato para derivar en un equipo de primer usuario, una primera clave basada en un primer parámetro de seguridad y una clave compartida entre un aparato de red central y el primer equipo de usuario; enviar una notificación de servicios de dispositivo a dispositivo a un segundo equipo de usuario; recibir un segundo parámetro de seguridad del segundo equipo de usuario, en el que el segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave por un aparato de red de acceso en el que está registrado el primer equipo de usuario; y derivar al primer equipo de usuario, la segunda clave basada en el segundo parámetro de seguridad y la primera clave, para proteger una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario.

De acuerdo con otra realización, un aparato comprende medios para derivar en un primer equipo de usuario, una primera clave basada en un primer parámetro de seguridad y una clave compartida entre un aparato de red central y el primer equipo de usuario. El aparato también comprende medios para enviar una notificación de servicios de dispositivo a dispositivo a un segundo equipo de usuario. El aparato también comprende recibir un segundo parámetro de seguridad del segundo equipo de usuario, en el que el segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave por un aparato de red de acceso en el que está registrado el primer equipo de usuario. El aparato también comprende derivar en el primer equipo de usuario, la segunda clave basada en el segundo parámetro de seguridad y la primera clave, para proteger una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario.

De acuerdo con una realización, un método comprende en un aparato de red de acceso, obtener de un aparato de red central y almacenar una primera clave compartida entre un primer equipo de usuario y el aparato de red central para comunicaciones de dispositivo a dispositivo del primer equipo de usuario. El método comprende además recibir de un segundo equipo de usuario, una petición para generar una segunda clave para una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario. El método comprende además en respuesta a la petición, generar la segunda clave basada en la primera clave y los parámetros de seguridad. El método comprende además enviar la segunda clave al segundo equipo de usuario.

En algunas realizaciones a modo de ejemplo, el método puede comprender además aceptar un registro del primer equipo de usuario; y almacenar la primera clave asociada a una información de ubicación del área de registro de dispositivo a dispositivo del primer equipo de usuario. En algunas realizaciones a modo de ejemplo, el método puede comprender además enviar los parámetros de seguridad al segundo equipo de usuario, para que al menos parte de los parámetros de seguridad se envíen al primer equipo de usuario. En algunas realizaciones a modo de ejemplo, el método puede comprender además eliminar la primera clave del aparato de la red de acceso después de que el primer equipo de usuario se haya movido fuera del área de registro gestionada por el aparato de la red de acceso.

En una realización a modo de ejemplo, la petición para generar la segunda clave puede indicar que la segunda clave se utilizará para una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario, y puede comprender una identidad del primer equipo de usuario. El aparato de red de acceso puede ser un Nodo B mejorado o un servidor de función de servidor de registro de dispositivo a dispositivo.

De acuerdo con una realización, un método comprende recibir en un aparato de red central, una petición para generar una primera clave para comunicaciones de dispositivo a dispositivo de un equipo de usuario. El método comprende además en respuesta a la petición, generar la primera clave basada en una clave compartida entre el aparato de red central y el equipo de usuario y los parámetros de seguridad. El método comprende además enviar los parámetros de seguridad al equipo del usuario. El método comprende además enviar la primera clave a un aparato de red de acceso en el que está registrado el primer equipo de usuario.

En una realización a modo de ejemplo, la petición puede indicar una capacidad de comunicación de dispositivo a dispositivo del equipo de usuario. Los parámetros de seguridad pueden transmitirse desde el aparato de red central al aparato de red de acceso junto con la primera clave y la identidad del equipo de usuario en un mismo mensaje. El aparato de red central puede ser una entidad de gestión de movilidad.

Todavía otros aspectos, características y ventajas de la invención son fácilmente evidentes a partir de la siguiente descripción detallada, simplemente ilustrando una serie de realizaciones e implementaciones particulares, incluyendo el mejor modo contemplado para llevar a cabo la invención. La invención también es capaz de otras y diferentes realizaciones, y sus diversos detalles pueden modificarse en varios aspectos obvios, todo sin apartarse del alcance de la invención. En consecuencia, los dibujos y la descripción deben considerarse de naturaleza ilustrativa y no restrictiva.

Breve descripción de los dibujos

Las realizaciones de la invención se ilustran a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos:

La figura 1 es un sistema de comunicación inalámbrico en el que se puede implementar al menos una realización de la presente invención;

La figura 2 representa un diagrama de temporización de ejemplo que ilustra un procedimiento de generación de claves entre equipos de usuario D2D de acuerdo con una realización de la presente invención;

La figura 3 es un diagrama de flujo de un proceso de generación de claves para una comunicación D2D controlada por red, de acuerdo con una realización;

La figura 4 es un diagrama de flujo de un proceso de generación de claves para una comunicación D2D controlada por red, de acuerdo con una realización;

La figura 5 es un diagrama de flujo de un proceso de generación de claves para una comunicación D2D controlada por red, de acuerdo con una realización; y

La figura 6 es un diagrama de bloques simplificado de varios dispositivos que son adecuados para su uso en la práctica de diversas realizaciones a modo de ejemplo de la presente invención.

Descripción de algunas realizaciones

Ejemplos de un método, Se revelan aparatos y programas informáticos para generar claves de criptografía en comunicaciones D2D sin introducir demasiada carga en una red central. En la siguiente descripción, a efectos de explicación, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión completa de las realizaciones de la invención. Es aparente, sin embargo, para un experto en la materia, las realizaciones de la invención se pueden practicar sin estos detalles específicos o con una disposición equivalente. En otros casos, diversas estructuras y dispositivos se muestran en forma de diagrama de bloques con el fin de evitar complicar innecesariamente las realizaciones de la invención. Los números de referencia similares se refieren a los elementos similares a lo largo de la memoria.

La figura 1 es un sistema de comunicación inalámbrico en el que se puede implementar al menos una realización de la presente invención. Por lo general, un sistema de comunicación inalámbrico incluye una red de acceso por radio y una red central. La red de acceso de radio controla una celda y ciertos UE que operan dentro de esa celda, para proporcionar un acceso inalámbrico a la red central. Como se muestra en la figura 1, una red de acceso por radio 120 puede comprender una estación base 122, que puede soportar un servicio correspondiente o un área de cobertura (también denominada celular). La estación base 120 también es capaz de comunicarse con dispositivos inalámbricos, tales como equipos de usuario 110A, 110B, dentro del área de cobertura. Aunque la figura 1 representa una estación base 122 y dos equipos de usuario 110A, 110B en la red de acceso por radio 120, también se pueden implementar otras cantidades de estaciones base y equipos de usuario.

En algunas implementaciones, la estación base 120 puede implementarse como una estación base de tipo Nodo B (eNB) desarrollada de acuerdo con los estándares, incluidos los estándares de evolución a largo plazo (LTE). Los equipos de usuario 110A, 110B pueden ser móviles y / o estacionarios. Asimismo, los equipos de usuario 110A, 110B pueden ser referidos como, por ejemplo, dispositivos, estaciones móviles, unidades móviles, estaciones de suscriptor, terminales inalámbricos, terminales, o similares. El equipo de usuario puede implementarse como, por ejemplo, un dispositivo inalámbrico de mano, un accesorio de complemento inalámbrico, o similar. Por ejemplo, el equipo del usuario puede tomar la forma de un teléfono inalámbrico, un ordenador con una conexión inalámbrica a una red, o similar. En algunos casos, el equipo del usuario puede incluir uno o más de los siguientes: al menos un procesador, al menos un medio de almacenamiento legible por ordenador (por ejemplo, memoria, almacenamiento y similares), un mecanismo de acceso por radio y una interfaz de usuario.

La red central 130 comprende los elementos de red convencionales y la función de una red de comunicación celular, como la MME 132 (Entidad de Gestión de Movilidad), el HSS (Servidor de Suscriptor Doméstico) 134, Los elementos de red en la red central pueden organizarse en una estructura básica y operar de una manera básica bien conocida por un experto en la materia.

En realizaciones de la presente invención, el sistema de comunicación inalámbrico 100 está configurado para soportar aún más las comunicaciones D2D controladas por la red. En este sentido, una función D2D está integrada en los sistemas móviles terrestres públicos, como el Proyecto de Asociación de 3ra Generación (3GPP), así como las generaciones posteriores de sistemas de comunicación celular. Los sistemas de comunicación celular, como el eNB 122, la MME 132 u otros elementos de red, puede usarse para ayudar en el establecimiento y el control continuo de las comunicaciones D2D, por ejemplo, asignación de recursos de radio de las comunicaciones D2D, control del interruptor, etc. En otras palabras, los UE pueden comunicarse entre sí a través del sistema de comunicación celular (en particular a través de eNB 122) o mediante una comunicación D2D directa. Como se muestra en la figura 1, el UE 110A está bajo el control del eNB 122 y se comunica directamente con el UE 110B.

Para que la gestión de las comunicaciones D2D sea más factible y eficiente, se puede introducir un servidor de DRSF (Función de Servidor de Registro D2D) para el registro, autenticación e identificación de usuarios de D2D. Un usuario D2D en un área de registro D2D puede registrarse en la DRSF del área de registro D2D con una ID de usuario D2D y una ID de UE temporal (por ejemplo, S-TMSI). Un servidor de DRSF puede ubicarse en una entidad de red de acceso de radio (por ejemplo, eNB) o en una entidad de red central (por ejemplo, MME) o en ambos con una estructura jerárquica. En el caso de que un servidor de DRSF esté ubicado en una red de acceso de radio, El DSRF se puede implementar de forma centralizada o distribuida.

Para un DRSF centralizado, un área de registro D2D debe estar limitada dentro del área de control de un elemento RAN. Por ejemplo, si un servidor de DRSF se encuentra en eNB, el área de registro D2D puede limitarse a la celda controlada por un eNB. Tener un DRSF centralizado en una RAN puede acortar el tiempo para la configuración de la conexión D2D ya que hay menos entidades de red y señalización involucradas en los procedimientos de configuración de la conexión D2D, pero requiere un registro D2D más frecuente. Es decir, un registro D2D debe realizarse nuevamente cuando un equipo de usuario se traslada a una nueva área de registro D2D, por ejemplo, una celda controlada por un nuevo eNB. Para DRSF distribuida, un área de registro D2D puede extenderse al área de cobertura controlada por múltiples elementos RAN para evitar registros D2D demasiado frecuentes. En ese caso, el control relacionado con D2D (por ejemplo, paginación D2D, configuración de conexión D2D, etc.) la señalización debe atravesar la interfaz de elementos RAN (por ejemplo, la interfaz X2 en E-UTRAN).

Tradicionalmente, la protección de seguridad de las comunicaciones directas D2D también se proporciona en virtud del sofisticado mecanismo de seguridad del sistema de comunicación celular. Por ejemplo, las derivaciones de claves de seguridad para asegurar las comunicaciones D2D directas pueden ser controladas por la red central que incluye MME 132 y HSS 134. Como se muestra en la figura 1, cuando el UE1 está en modo inactivo RRC (Control de Recursos de Radio), el UE2 solicitará a la red central (por ejemplo, MME 132) que genere una clave de seguridad para un servicio D2D entre el UE1 y el UE2. Por lo general, para un área D2D dada, puede haber muchos UE D2D operando en el servicio D2D. Por lo tanto, molestará a la red central 130 (o MME 132) para generar cada clave de seguridad para el servicio D2D respectivo, lo cual es un desafío potencial desde el punto de vista de la red central. Las realizaciones a modo de ejemplo de la invención abordan cómo soportar eficientemente la seguridad de la comunicación D2D controlada por la red, incluyendo cómo generar, distribuir y actualizar claves de seguridad para servicios D2D con menos impacto de señalización en la red central. Realizaciones a modo de ejemplo conducen tal

generación, distribución y actualización de claves independientemente de si un UE está en estado RRC conectado o en estado inactivo.

En realizaciones a modo de ejemplo de la invención, una MME puede generar una primera clave para el servicio D2D de un UE, y luego compartirla entre el UE, la MME y un elemento (como un eNB o DRSF) de una red de acceso que controla el UE. La primera clave se puede generar en función de un contexto de seguridad válido (por ejemplo, contexto de seguridad NAS (estrato de no acceso)) para el UE mantenido en la red central. Por ejemplo, la MME puede generar la primera clave a partir de una Clave de Entidad de Administración de Seguridad de Acceso Válida (denominada K_{asme}) para el UE. La primera clave se almacena en la red de acceso, de modo que las claves de seguridad para cada servicio D2D iniciado por el UE bajo el control del elemento de red de acceso pueden ser generadas por el elemento de red de acceso basado en la primera clave, sin necesidad de solicitar claves de seguridad de la red central para cada servicio D2D.

La figura 2 representa un diagrama de temporización de ejemplo que ilustra un procedimiento de generación de claves entre equipos de usuario D2D de acuerdo con una realización de la presente invención. Supongamos que hay una explicación de que hay un servidor de DRSF 124 en la red de acceso de radio. Aunque la figura 1 ilustra el servidor de DRSF 124 como una entidad separada y distinta de cualquiera de los elementos de la red de acceso, en la práctica, la función del servidor 124 puede incorporarse en cualquier aparato (por ejemplo, en eNB 122) de la red de acceso 120. Con referencia a la figura 2, UE1 110A se enciende en 210 e inicia un procedimiento de conexión a la red central. A continuación, el UE1 puede solicitar a la MME 132 que genere una primera clave para los servicios D2D iniciados por el UE1. Por ejemplo, el UE1 puede indica su capacidad D2D a la MME 132, en el mensaje de petición de adjunto enviado desde el UE1 110A a la MME 132, en 215. A continuación, en 220, la MME 132 puede generar una primera clave (indicada como $K_{d2d\text{-}UE1}$) para el UE1 basada en una clave NAS compartida entre el UE1 y la MME 132 (por ejemplo, K_{asme} del UE1) junto con otros parámetros de seguridad, como un número aleatorio denotado R_{d2d}. Los parámetros para derivar la clave D2D se pueden proporcionar o generar de acuerdo con la identidad del UE1. Por ejemplo, cuando el UE1 se alojó temporalmente por primera vez en la celda del eNB 122 después del encendido, la red central (es decir, el estrato sin acceso) puede registrar el UE1 y lograr una consistencia de seguridad NAS (por ejemplo, compartir una clave NAS común) entre el UE1 y la red central. En este sentido, habrá un contexto de seguridad NAS válido para el UE1 que comprende la clave NAS común mantenida en la red central, por ejemplo en la MME 132 o el HSS 134. Por ejemplo, la clave NAS compartida entre el UE1 y la MME 132 puede ser una K_{asme} del UE1, que puede recuperarse en función de la identidad del UE1.

La MME 132 puede incluir los parámetros de seguridad (como el número aleatorio R_{d2d}) en un mensaje de aceptación de adjunto que se envía desde la MME 132 al UE1 110A con seguridad de nivel NAS protegida (por ejemplo, cifrado). Paralelamente, en 230, la MME puede enviar el $K_{d2d\text{-}UE1}$ generado para el UE1 junto con la identidad del UE1, por ejemplo, S-TMSI del UE1, al eNB 122 (o DRSF 134) donde se inicia el procedimiento de conexión. A continuación, eNB o DRSF pueden almacenar esta información para su uso posterior, como se muestra en 245. En algunas realizaciones a modo de ejemplo, los dos conjuntos de parámetros enviados desde la MME 132 respectivamente a eNB 122 y el UE1 110A pueden estar contenidos en un mismo mensaje S1AP, es decir, mensaje de PETICIÓN DE CONFIGURACIÓN DE CONTEXTO INICIAL, así que desde el punto de vista de la MME, solo se usa una señalización S1AP para transmitir los parámetros esenciales. En función de la clave NAS compartida K_{asme} y de los parámetros de seguridad recibidos R_{d2d}, el UE1 puede derivar la primera clave, por ejemplo como se muestra en 240. Como tal, la primera clave se puede compartir entre el UE1, el eNB / DRSF y la MME 132.

Aunque como se ilustra en la figura 2, la primera clave se genera y distribuye durante un procedimiento de conexión a la red central, Debe apreciarse que en algunas realizaciones a modo de ejemplo, la generación de la primera clave no se limita a este procedimiento. Por ejemplo, la primera clave se puede actualizar en la MME y proporcionar al UE1 automáticamente, y / o la primera clave se puede generar en un procedimiento dedicado iniciado por el UE1 o la MME.

Paralelamente a la generación y distribución de la primera clave, el UE1 puede registrarse en un aparato de red de acceso (como un eNB o DRSF) que controla el área de registro D2D en la que se encuentra actualmente el UE1, para servicios D2D en esta área de registro D2D. Este registro se puede realizar como registro de área D2D. En esta realización ilustrada en la figura 1, el UE1 110A está conectado a la red central 130 a través de la red de acceso 120, y luego puede registrarse en eNB 122 / DRSF 124 con su identidad y su información de ubicación en un área de registro D2D, en 235. El eNB / DRSF puede almacenar información de registro D2D para asociar la primera clave para el UE1 a la identidad (por ejemplo, S-TMSI del UE1) y la información de ubicación del UE1. Debe apreciarse que el registro del área D2D puede ocurrir en cualquier momento necesario. En algunas realizaciones, el registro del área D2D puede realizarse antes o después de la generación y distribución de la primera clave.

A través del registro D2D, el UE1 110 A puede realizar servicios D2D en el área de registro D2D bajo el control eNB 122 y / o DRSF 124. Después del procedimiento de conexión o el registro del área D2D, el UE1 puede volver al modo inactivo, por ejemplo para el menor consumo de energía. En otras palabras, no hay una conexión RRC establecida entre el UE1 y el eNB 122. Por ejemplo, el UE1 puede permanecer en modo inactivo RRC como se especifica en los protocolos LTE. Como un dispositivo capaz de comunicación D2D, el UE1 puede transmitir notificaciones de servicios D2D a sus UE D2D adyacentes cuando quiere comunicaciones D2D, incluso si permanece en modo inactivo RRC. Por ejemplo en 255, mientras permanece en modo inactivo, el UE1 difunde una notificación para los servicios D2D.

Esa notificación también identifica al UE1 como el creador de los servicios D2D con la identidad del UE1, por ejemplo, una IMEI (Identidad internacional de equipo móvil), una IMSI (Identidad de suscriptor móvil internacional), o una S-IMSI (Identidad de suscriptor móvil a corto plazo) del UE1 u otra identificación de usuario D2D. La identidad del UE1 puede asignarse al UE1 cuando el UE1 acampa en la celda del eNB 122. Aunque como se ilustra en la figura 2, el UE1 está en modo inactivo mientras transmite la notificación de los servicios D2D, la notificación también se puede transmitir mientras el UE1 está en modo RRC conectado.

A continuación, uno o más UE D2D adyacentes (por ejemplo, el UE2 110B) pueden detectar la notificación emitida del servicio D2D desde el UE1 y decidir establecer una conexión D2D con el UE1. Según la información en la notificación detectada, el UE2 puede obtener la información de identidad (por ejemplo, S-TMSI) del UE1 y solicitar al eNB / DRSF que genere una segunda clave para la conexión D2D entre el UE1 y el UE2. En el caso de que no haya conexión RRC entre el UE2 y el eNB 122, el UE2 puede iniciar un procedimiento de configuración de conexión RRC al eNB 122, como se muestra en 260A, 260B y 265. A través de la conexión RRC establecida, la petición de la segunda clave se puede enviar a eNB / DRSF. Por ejemplo, la identidad del UE1 que se puede obtener de la notificación recibida en 255, se puede transmitir al eNB 122 / DRSF 124 en un mensaje de configuración completa de conexión RRC en 265, solicitar al eNB 122 / DRSF 124 para generar las claves de seguridad D2D requeridas. En este ejemplo, el eNB indica que el procedimiento de configuración de la conexión RRC se imita solo para una derivación de claves D2D que es diferente de las conexiones RRC heredadas. En el legado, de acuerdo con las especificaciones relacionadas, el eNB generalmente necesita reenviar el mensaje inicial del UE (por ejemplo, la petición iniciada desde el UE2) a la red central (por ejemplo, la MME) después del procedimiento de configuración de la conexión RRC. En su lugar, el reenvío no es necesario en diversas realizaciones de la presente invención, porque se debe al eNB / DRSF para generar la segunda clave. En este sentido, el UE2 puede incluir un nuevo valor de causa, por ejemplo, "procedimiento de derivación de clave D2D" en el mensaje de configuración de conexión RRC completa, para indicar al eNB que el procedimiento de configuración de la conexión RRC es simplemente para una derivación de claves D2D, para que la red de acceso por radio y la red central (especialmente, el eNB 122 y la MME 132) no necesitan realizar ninguna operación adicional más allá de habilitar la derivación de la segunda clave.

En algunas realizaciones a modo de ejemplo, el UE2 puede tener una conexión RRC activada al eNB 122 en el momento de decidir establecer una conexión D2D con el UE1. En ese caso, no es necesario iniciar el procedimiento de configuración de la conexión RRC. el UE2 puede permanecer en un modo conectado RRC y enviar una petición de derivación de la segunda clave al eNB / DRSF utilizando la conexión RRC activa entre el UE2 y el eNB 122. Como se discutió anteriormente en relación con la petición en el mensaje de configuración completa de la conexión RRC, esta petición también comprende la identidad del UE1 (por ejemplo, S-TMSI del UE1). Además, el UE2 indica este propósito de generación de clave D2D para el eNB / DRSF, de manera similar, el eNB / DRSF puede finalizar el procedimiento al lado de la red de acceso, en lugar de reenviar este procedimiento al lado de la red central.

En respuesta a la recepción de la petición de derivación de clave, el eNB 132 o la DRSF 134 pueden proporcionar al UE2 una segunda clave (denominada K_{d2d_serv}) para la conexión D2D entre el UE1 y el UE2, y los parámetros de seguridad asociados para derivar la segunda clave. En este sentido, el eNB / DRSF puede identificar la primera clave ($K_{d2d\text{-}UE1}$) para el UE1 basándose en la identidad del UE1 (por ejemplo, S-TMSI del UE1) de la petición recibida. Basado en $K_{d2d\text{-}UE1}$ y parámetros de seguridad, el eNB / DRSF puede generar K_{d2d_serv} en 270, para la protección y cifrado de integridad del servicio D2D, por ejemplo. Los parámetros de seguridad asociados para derivar K_{d2d_serv} pueden comprender un número aleatorio (denotado como R_{d2d}*) generado por el eNB / DRSF y / o algunos parámetros asociados al UE2, por ejemplo, una identidad temporal (por ejemplo, S-TMSI) del UE2. A continuación, el eNB / DRSF envía el K_{d2d_serv} al UE2 en 275, junto con los parámetros de seguridad asociados (por ejemplo, R_{d2d}* y / o S-TMSI del UE2), si hay alguna.

En algunas realizaciones, el eNB / DRSF también puede especificar una función de derivación de clave (KDF) utilizada para derivar el K_{d2d_serv} e indicar el KDF al UE1 como parte de los parámetros de seguridad asociados. En este sentido, el eNB / DRSF puede obtener una capacidad de seguridad del UE1 de la MME. Por ejemplo, la capacidad de seguridad del UE1 se puede enviar desde la MME 132 al eNB / DRSF junto con $K_{d2d\text{-}UE1}$, en la etapa 230. Desde la capacidad de seguridad, el eNB / DRSF puede aprender los algoritmos soportados por el UE1 para generar la clave K_{d2d_serv}. El eNB / DRSF puede obtener además una capacidad de seguridad del UE2 que se incluye en la petición de conexión RRC. Desde la capacidad de seguridad del UE2, el eNB / DRSF puede aprender los algoritmos soportados por el UE2 para generar la clave K_{d2d_serv}. A continuación, el eNB / DRSF puede decidir un algoritmo que se utilizará para generar una clave para la comunicación D2D entre el UE1 y el UE2, basado en la capacidad de seguridad del UE1 y el UE2. Por ejemplo, el eNB / DRSF puede seleccionar un algoritmo comúnmente soportado entre el UE1 y el UE2. El eNB / DRSF puede enviar una ID de algoritmo que indica el algoritmo seleccionado al UE2 como parte de los parámetros de seguridad asociados, junto con K_{d2d_serv}, en la etapa 275.

En 280, el UE2 recibe K_{d2d_serv} y los parámetros de seguridad asociados (por ejemplo, R_{d2d}* y / o S-TMSI del UE2) para derivar $K_{d2d\text{-}serv}$ del eNB / DRSF, y luego almacena K_{d2d_serv} como la clave de seguridad para el servicio D2D con el UE1. A continuación, el UE2 reenvía los parámetros de seguridad asociados (por ejemplo, R_{d2d}* y / o S-TMSI del UE2) para derivar la clave K_{d2d_serv} al UE1, como se muestra en 285. En algunas realizaciones, una ID de algoritmo que indica que el algoritmo seleccionado que deriva $K_{d2d\text{-}serv}$ también se puede reenviar desde el UE2 al UE1, junto con R_{d2d}* y / o S-TMSI del UE2.

Con los parámetros de seguridad recibidos (por ejemplo, el R_{d2d}* y / o el S-TMSI del UE2, el ID del algoritmo seleccionado) del UE2, el UE1 puede derivar el K_{d2d_serv} basado en el $K_{d2d\text{-}UE1}$ y los parámetros de seguridad. En este sentido, de acuerdo con la ID del algoritmo recibido, el UE1 puede usar el mismo KDF que el eNB para derivar K_{d2d_serv}. Como tal, una clave de criptografía D2D común, K_{d2d_serv} se puede compartir entre el UE1 y el UE2 sin interrumpir la red central. La clave de criptografía D2D K_{d2d_serv} se puede usar directamente para asegurar las comunicaciones D2D entre el UE1 y el UE2. Como alternativa o adicionalmente, K_{d2d_serv} se puede utilizar para derivar otras claves que se utilizan para asegurar la comunicación D2D entre el UE1 y el UE2.

En algunas realizaciones, si UE1 se está moviendo fuera del área de registro D2D controlada por el eNB o la DRSF, el eNB o la DRSF pueden actualizar la información de ubicación del UE1 y eliminar el contexto de seguridad relacionado del UE1, incluyendo el $K_{d2d\text{-}UE1}$ y el K_{d2d_serv}. A continuación, cuando el UE1 vuelve al área de registro D2D del eNB / DRSF y el eNB / DRSF encuentra que no existe ningún contexto de seguridad para el UE1, puede solicitar a la red central (por ejemplo, MME) que transfiera el contexto, incluida la primera clave $K_{d2d\text{-}UE1}$ del UE1. Dado que la MME siempre mantiene cierta información de contexto (incluidos los contextos de seguridad) para los UE, incluso si los UE están en modo inactivo, la MME siempre puede proporcionar esta información de contexto al eNB / DRSF, por ejemplo a través de un procedimiento de petición / respuesta.

Aunque muchas operaciones se describen en un cierto orden con referencia a la figura 2, debe apreciarse que estas operaciones pueden realizarse en órdenes alternativas, y algunas operaciones pueden ajustarse, combinarse, o incluso omitirse. Por ejemplo, en una realización a modo de ejemplo, la derivación (etapa 240) de la primera clave $K_{d2d\text{-}UE1}$ en el UE1 110A puede ocurrir en cualquier momento antes de la derivación (etapa 290) de la segunda clave K_{d2d_serv}. Además, se puede omitir el regreso al modo inactivo en 250, los medios UE1 110A no está en modo inactivo cuando se difunde la notificación de servicios D2D. En una realización a modo de ejemplo, el UE1 110A puede solicitar la primera clave de la MME 132 después del registro del área D2D. En una realización a modo de ejemplo, el eNB / DRSF puede solicitar a la MME 132 que proporcione la primera clave del UE1 cuando el eNB / DRSF encuentra que no puede identificar la primera clave, por ejemplo, cuando se genera la segunda clave K_{d2d_serv} para el UE1 en 270.

En diversas realizaciones, una vez que la red de acceso obtiene una primera clave para las comunicaciones D2D iniciadas por el UE1, puede generar una segunda clave que finalmente se usa para proteger una conexión D2D entre el UE1 y un UE par (por ejemplo, UE2). Como tal, la derivación de una clave para cada conexión D2D puede procesarse en una red de acceso, sin introducir una carga de señalización en la red central (por ejemplo, MME). El impacto de la señalización en la red central se puede reducir significativamente, especialmente en un caso donde muchos UE D2D están en servicios D2D con el UE1. Además, sin la participación de la red central o la MME, la demora para la generación de claves D2D también se acorta en comparación con los métodos heredados, especialmente para un par D2D, uno de los cuales está en modo inactivo.

Las figuras 3, 4 y 5, son diagramas de flujo de flujo lógico que ilustran las operaciones de los métodos y el resultado de la ejecución de instrucciones de programas de ordenador, de acuerdo con las realizaciones de ejemplo de esta invención para generaciones clave para una comunicación D2D controlada por red. De manera más específica, las figuras 3, 4 y 5 son descriptivas de un flujo de proceso entre un equipo de usuario par D2D, como el UE1 y el UE2, un aparato de red de acceso tal como el eNB 122 o DRSF 124, y un aparato de red central, como la MME 132. En una tal realización, los procesos pueden implementarse en, por ejemplo, un conjunto de chips que incluye un procesador y una memoria como se muestra en la figura 6. Como tal, un equipo de usuario puede proporcionar medios para lograr diversas partes del proceso 300, así como medios para lograr otros procesos en conjunto con otros componentes, un aparato de red de acceso puede proporcionar medios para lograr diversas partes del proceso 400, así como medios para lograr otros procesos en conjunto con otros componentes, y un aparato de red central puede proporcionar medios para lograr diversas partes del proceso 500, así como medios para lograr otros procesos en conjunto con otros componentes.

En la etapa 310, un equipo de usuario (como el UE1 110A) deriva una primera clave basada en un primer parámetro de seguridad y una clave compartida entre un aparato de red central (por ejemplo, la MME 132) y el equipo de usuario, como el K_{asme} del UE1. El UE1 puede enviar un mensaje de petición a la MME 132 para una generación de la primera clave. La petición puede indicar una capacidad de comunicación D2D del UE1. En respuesta a la petición, el UE1 puede recibir de la MME 132 los primeros parámetros de seguridad, como un número aleatorio.

En la etapa 320, el UE1 envía una notificación de servicios D2D a sus equipos de usuarios pares, como el UE2. El UE1 puede permanecer en modo inactivo. La notificación de servicios D2D puede transmitirse en balizas de capa física al UE2, y las balizas pueden identificar el UE1 como un creador de servicios D2D.

A continuación en la etapa 330, el UE1 recibe un segundo parámetro de seguridad de sus equipos de usuario pares (como el UE2), que desean establecer una conexión D2D con el UE1. El segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave por un aparato de red de acceso (tal como el eNB 122 o la DRSF 124) en el que el UE1 está registrado. El segundo parámetro de seguridad puede incluir un número aleatorio proporcionado por el aparato de red de acceso, y / o una identidad temporal del equipo de usuario par UE2. El UE1 puede registrarse en el eNB 122 o la DRSF 124 con su información de ubicación del área de registro D2D.

A continuación en la etapa 340, el UE1 deriva la segunda clave basada en el segundo parámetro de seguridad y la primera clave. La segunda clave se utilizará para proteger una comunicación D2D entre el UE1 y su equipo de usuario par. El UE2 puede obtener la segunda clave directamente del aparato de red de acceso. A continuación, se puede establecer una conexión D2D entre el UE1 y el UE2, y las comunicaciones D2D entre el UE1 y el UE2 se pueden asegurar en función de la segunda clave.

En la etapa 410, un aparato de red de acceso (como el eNB 122 o la DRSF 124) obtiene de un aparato de red central (como la MME 132) una primera clave para un equipo de usuario D2D (como el UE1) y almacena la primera clave. La primera clave se comparte entre el UE1 y la MME 132 para las comunicaciones D2D del UE1. El UE1 puede ser un equipo de usuario D2D dentro de un área de registro D2D administrado por el eNB 122 o la DRSF 124. Al aceptar un registro del UE1, el eNB 122 o la DRSF 124 pueden almacenar la primera clave asociada a una información de ubicación del área de registro D2D del UE1.

En la etapa 420, el aparato de red de acceso (como el eNB 122 o la DRSF 124) recibe de otro equipo de usuario (como el UE2), una petición para generar una segunda clave para una comunicación D2D entre el UE1 y el segundo equipo de usuario. La petición puede indicar al eNB 122 o la DRSF 124 que la segunda clave se utilizará para una comunicación D2D entre el UE1 y el UE2.

De la petición, el eNB 122 o la DRSF 124 pueden identificar la identidad del UE1 y recuperar $K_{d2d\text{-}UE1}$. Basado en el $K_{d2d\text{-}UE1}$ y algunos parámetros de seguridad, tal número aleatorio o identidad temporal del UE2 S-TMSI, el eNB 122 o la DRSF 124 pueden generar la segunda clave en respuesta a la petición, en la etapa 430.

A continuación en la etapa 440, el eNB 122 o la DRSF 124 envían la segunda clave al otro equipo de usuario UE2. Los parámetros de seguridad utilizados para generar la segunda clave también se pueden enviar al UE2, para que los parámetros de seguridad se puedan reenviar al UE1.

En la etapa 510, un aparato de red central (como la MME 132) recibe una petición para generar una primera clave para comunicaciones D2D de un equipo de usuario (como el UE1). La petición puede indicar una capacidad de comunicación D2D del UE1. A continuación en la etapa 520, en respuesta a la petición, la MME 132 puede generar la primera clave basada en una clave (como K_{asme} del UE1) compartida entre la MME 132 y el UE1 y algunos parámetros de seguridad, como un número aleatorio proporcionado por la MME 132.

A continuación en la etapa 530, la MME 132 envía los parámetros de seguridad al UE1, para que el UE1 pueda derivar la primera clave. En la etapa 540, la MME 132 envía además la primera clave a un aparato de red de acceso, como el eNB 122 y la DRSF 124, en el que el UE1 está registrado. Con el intercambio de la primera clave entre el UE1 y el aparato de red de acceso, la generación de claves (es decir, la segunda clave) para los servicios D2D del UE1 puede ser terminada en la red de acceso por el aparato de la red de acceso, sin interrumpir la red central.

Ahora se hace referencia a la figura 6 que ilustra un diagrama de bloques simplificado de varios dispositivos electrónicos que son adecuados para su uso en la práctica de las realizaciones a modo de ejemplo de la presente invención. En la figura 6, una red de comunicación inalámbrica 600 se puede adaptar para la comunicación con los equipos de usuario 610 (como los UE 110A y 110B) a través de una estación base (como un eNB 122). La red 600 puede incluir además un aparato de red de acceso 620 (tal como el eNB 122 o servidor de la DRSF 124) para generaciones clave de un servicio D2D, y un aparato de red central 640 (tal como la MME 132) para proporcionar una seguridad NAS para los equipos de usuario. Los UE 110A y 110B pueden realizar una comunicación celular bajo el control de la MME 132 y el eNB 122. Además, el UE1 110A y el UE2 110B pueden realizar una comunicación D2D directamente entre sí bajo el control de la MME 132 y el eNB 122, y opcionalmente un servidor DSRF 124. Las claves para los servicios D2D se pueden generar para los UE sin introducir demasiada carga en una red central de acuerdo con las realizaciones a modo de ejemplo de la presente invención como se discutió anteriormente.

El UE 610 incluye un procesador de datos (DP) 610A, una memoria (MEM) 610B que almacena un programa (PROG) 610C y un transceptor de radiofrecuencia (RF) adecuado 610D para comunicaciones inalámbricas con el eNB a través de una o más antenas. En una realización a modo de ejemplo, el transceptor 610D en el UE1 110A puede usarse para comunicaciones D2D tanto en banda con licencia (por ejemplo, banda celular) como en banda sin licencia (por ejemplo, banda WLAN). Alternativamente, el transceptor 610D puede comprender componentes separados para soportar comunicaciones D2D en banda con licencia (por ejemplo, banda celular) y banda sin licencia (por ejemplo, banda WLAN) respectivamente.

El aparato de red de acceso 620 incluye un DP 620A, una MEM 620B que almacena un PROG 620C y una interfaz de comunicación adecuada 620E. La interfaz de comunicación 620E puede comunicarse con la red central, como la MME 132. En algunas implementaciones que el aparato de red de acceso 620 se implementa como un servidor de DRSF, la interfaz de comunicación 620E puede adaptarse además para comunicarse con los UE a través del eNB. En algunos ejemplos, la interfaz de comunicación 620E puede usarse para transmitir y recibir información usando protocolos y métodos asociados a la comunicación D2D controlada por la red. En algunas realizaciones donde el aparato de red de acceso 620 se implementa como un eNB, o en otras palabras, que se incorpora un DRSF en el

eNB, el aparato de acceso de red 620 puede incluir además un transceptor 620D de radiofrecuencia (RF) adecuado para comunicaciones inalámbricas con los UE a través de una o más antenas.

El aparato de red central también incluye un DP 640A, una MEM 640B que almacena un PROG 640C y una interfaz de comunicación adecuada 640E. La interfaz de comunicación 640E puede ser capaz de comunicarse con eNB y con el UE1 y el UE2 a través del eNB. En algunas realizaciones, la interfaz de comunicación 640E está adaptada para comunicarse con un servidor de DRSF. En algunos ejemplos, la interfaz de comunicación 640E puede usarse para transmitir y recibir información usando protocolos y métodos asociados a la comunicación D2D controlada por la red.

Al menos uno de los PROG 610C, 620C, Se supone que 640C incluye instrucciones de programa que, cuando es ejecutado por el DP asociado, permitir que el dispositivo electrónico funcione de acuerdo con las realizaciones a modo de ejemplo de esta invención, como se explicó anteriormente. Es decir, las realizaciones a modo de ejemplo de esta invención pueden implementarse al menos en parte mediante un software informático ejecutable por el DP 610A del UE 610A, por el DP 620A del aparato de red de acceso 620, y por el DP 640A del aparato de red central 640, o por hardware, o por una combinación de software y hardware. La estructura básica y el funcionamiento del UE 610, el aparato de red de acceso 620 (por ejemplo, el eNB 122 o la DRSF 124) y el aparato de red central 640 (por ejemplo, la MME 132) son conocidos por un experto en la materia.

En general, las diversas realizaciones del UE 610 pueden incluir, pero no se limitan a, teléfonos celulares, asistentes digitales personales (PDA) con capacidades de comunicación inalámbrica celular, ordenadores portátiles con capacidad de comunicación inalámbrica celular, dispositivos de captura de imágenes, como cámaras digitales con capacidad de comunicación inalámbrica, dispositivos de juego con capacidades de comunicación inalámbrica celular, dispositivos de almacenamiento y reproducción de música con capacidad de comunicación inalámbrica celular, aparatos de Internet que permiten el acceso inalámbrico a Internet móvil y la navegación, así como unidades portátiles o terminales que incorporan combinaciones de tales funciones.

Las MEM 610B, 620B, 640B pueden ser de cualquier tipo adecuadas para el entorno técnico local y pueden implementarse utilizando cualquier tecnología de almacenamiento de datos adecuada, tales como dispositivos de memoria basados en semiconductores, memoria flash, dispositivos y sistemas de memoria magnética, dispositivos y sistemas de memoria óptica, memoria fija y memoria extraíble. Los DP 620A, 620A, 640A pueden ser de cualquier tipo adecuado para el entorno técnico local y pueden incluir uno o más de los ordenadores de uso general, ordenadores especiales, microprocesadores, procesadores de señales digitales (DSP) y procesadores basados en arquitecturas de procesadores multinúcleo, como ejemplos no limitantes.

En general, las diversas realizaciones a modo de ejemplo pueden implementarse en hardware o circuitos de uso especial, software, lógica o cualquier combinación de las mismas. Por ejemplo, algunos aspectos pueden implementarse en hardware, mientras que otros aspectos pueden implementarse en el firmware o software que puede ejecutar un controlador, microprocesador u otro dispositivo informático, aunque la invención no se limita a los mismos. Si bien varios aspectos de las realizaciones a modo de ejemplo de esta invención pueden ilustrarse y describirse como diagramas de bloques, diagramas de flujo, o usando alguna otra representación pictórica, se entiende bien que estos bloques, aparatos, sistemas, técnicas o métodos descritos en este documento pueden implementarse en, como ejemplos no limitantes, hardware, software, firmware, circuitos de propósito especial o lógica, hardware o controlador de uso general u otros dispositivos informáticos, o alguna combinación de los mismos.

Como tal, se debería apreciar que al menos algunos aspectos de las realizaciones ilustrativas de la invención se pueden poner en práctica en diversos componentes tales como módulos y chips de circuito integrado. Por lo tanto, debe apreciarse que las realizaciones a modo de ejemplo de esta invención pueden realizarse en un aparato que se realiza como un circuito integrado, donde el circuito integrado puede comprender circuitos (así como posiblemente firmware) para incorporar al menos uno o más procesadores de datos, un procesador de señal digital, circuitería de banda base y circuitería de radiofrecuencia que son configurables para funcionar de acuerdo con las realizaciones a modo de ejemplo de esta invención.

Debería apreciarse que al menos algunos aspectos de las realizaciones a modo de ejemplo de las invenciones pueden incorporarse en instrucciones ejecutables por ordenador, como en uno o más módulos de programa, ejecutadas por uno o más ordenadores u otros dispositivos. Por lo general, los módulos del programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc.que realizan tareas particulares o implementan tipos de datos abstractos particulares cuando los ejecuta un procesador en un ordenador u otro dispositivo. Las instrucciones ejecutables del ordenador pueden almacenarse en un medio legible por ordenador, como un disco duro, disco óptico, medios de almacenamiento extraíbles, memoria de estado sólido, RAM, etc. Como apreciará un experto en la materia, la función de los módulos de programa puede combinarse o distribuirse según se desee en diversas realizaciones. Además, la función puede incorporarse total o parcialmente en firmware o equivalentes de hardware, como circuitos integrados, matrices de puertas programables de campo (FPGA) y similares.

La presente invención incluye cualquier característica novedosa o combinación de características descritas aquí, ya sea explícitamente o cualquier generalización de la misma. Varias modificaciones y adaptaciones a las realizaciones a modo de ejemplo anteriores de esta invención pueden resultar evidentes para los expertos en las técnicas relevantes

en vista de la descripción anterior, cuando se lee junto con los dibujos adjuntos. Sin embargo, cualquiera y cada una de las modificaciones seguirán cayendo dentro del ámbito de las realizaciones no limitantes e ilustrativas de esta invención.

REIVINDICACIONES

1. Un método, que comprende:

derivar (310) en un equipo de primer usuario, una primera clave basada en un primer parámetro de seguridad y una clave compartida entre un aparato de red central y el primer equipo de usuario;
enviar (320) una notificación de servicios de dispositivo a dispositivo a un segundo equipo de usuario;
recibir (330) un segundo parámetro de seguridad del segundo equipo de usuario, en donde el segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave por un aparato de red de acceso en el que está registrado el primer equipo de usuario; y
derivar (340) en el primer equipo de usuario, la segunda clave basada en el segundo parámetro de seguridad y la primera clave, para proteger una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario.

2. Un método de la reivindicación 1, en el que derivar la primera clave comprende,
enviar un mensaje de petición (215) al aparato de red central, indicar una capacidad de comunicación de dispositivo a dispositivo del primer equipo de usuario; y
recibir (225) los primeros parámetros de seguridad desde el aparato de red central.

3. Un método de la reivindicación 2, en el que el primer equipo de usuario vuelve al modo inactivo (250) después de recibir los primeros parámetros de seguridad.

4. Un método de la reivindicación 1, comprende adicionalmente:
registrar (235) el primer equipo de usuario al aparato de red de acceso con una información de ubicación del área de registro de dispositivo a dispositivo del primer equipo de usuario.

5. Un método, que comprende:

en un aparato de red de acceso, obtener de un aparato de red central y almacenar (410) una primera clave basada en un primer parámetro de seguridad y una clave compartida entre el aparato de red central y un primer equipo de usuario, siendo compartida la primera clave entre un primer equipo de usuario y el aparato de red central para comunicaciones de dispositivo a dispositivo del primer equipo de usuario;
recibir (420) de un segundo equipo de usuario, una petición para generar una segunda clave para una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario; en respuesta a la petición, generar (430) la segunda clave basada en la primera clave y los segundos parámetros de seguridad, en donde los segundos parámetros de seguridad son para generar una segunda clave basada en la primera clave por el aparato de red de acceso en el que está registrado el primer equipo de usuario; y
enviar (440) la segunda clave y los segundos parámetros de seguridad al segundo equipo de usuario, para que al menos parte de los segundos parámetros de seguridad se envíen al primer equipo de usuario.

6. Un método de la reivindicación 5, comprende además,
aceptar un registro del primer equipo de usuario; y
almacenar (245) la primera clave asociada a una información de ubicación del área de registro de dispositivo a dispositivo del primer equipo de usuario.

7. Un método de la reivindicación 5, comprende adicionalmente:
retirar la primera clave del aparato de red de acceso después de que el primer equipo de usuario se haya movido fuera del área de registro gestionada por el aparato de red de acceso.

8. Un método de la reivindicación 5, en el que la petición para generar la segunda clave indica que la segunda clave se debe usar para una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario, y comprende una identidad del primer equipo de usuario.

9. Un método de la reivindicación 5, en el que el aparato de red de acceso es un Nodo B mejorado (122) o un servidor de función de servidor de registro de dispositivo a dispositivo (124).

10. Un método, que comprende:

recibir (510) en un aparato de red central, una petición para generar una primera clave para comunicaciones de dispositivo a dispositivo de un equipo de usuario;
en respuesta a la petición, generar (520) la primera clave basada en una clave compartida entre el aparato de red central y el equipo de usuario y primeros parámetros de seguridad; enviar (530) los primeros parámetros de seguridad al equipo del usuario; y
enviar (540) la primera clave a un aparato de red de acceso en el cual el primer equipo de usuario está registrado para generar una segunda clave por el aparato de red de acceso basado en la primera clave y uno o más segundos parámetros de seguridad.

11. Un método de la reivindicación 10, en el que la petición indica una capacidad de comunicación de dispositivo a dispositivo del equipo de usuario.

12. Un método de la reivindicación 10, en el que los primeros parámetros de seguridad se transmiten desde el aparato de red central al aparato de red de acceso junto con la primera clave y la identidad del equipo de usuario en un mismo mensaje.

13. Un método de la reivindicación 10, en el que el aparato de red central es una entidad de gestión de movilidad (132).

14. Un aparato (610, 620, 640) que comprende medios para realizar el método de acuerdo con una cualquiera de las reivindicaciones 1-13.

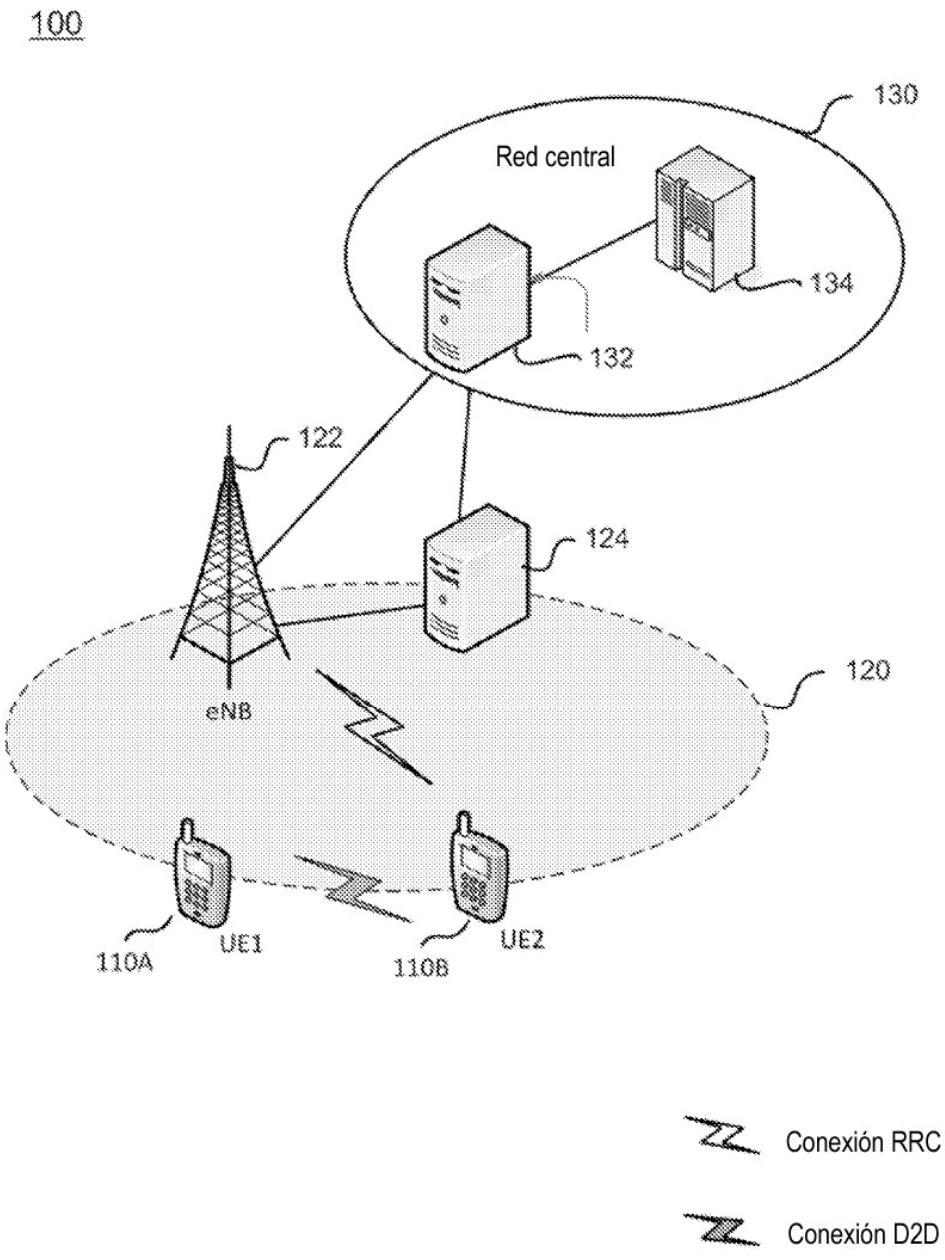
100
130
Red central
134
132
122
124
120
eNB
110A
UE1
110B
UE2
Conexión RRC
Conexión D2D

FIG.1

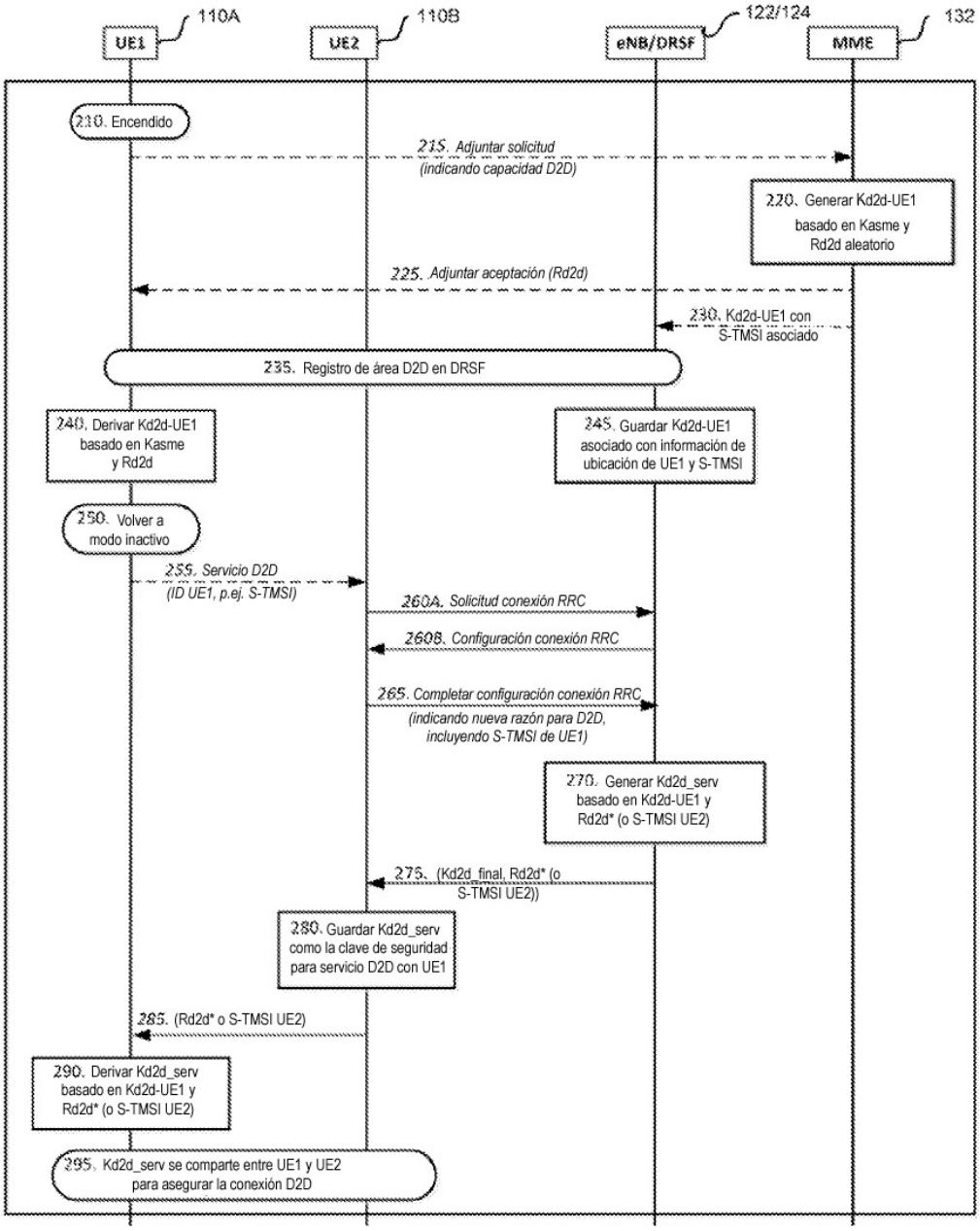
UE1
110A
UE2
110B
eNB/DRSF
122/124
MME
132
210. Encendido
215. Adjuntar solicitud
(indicando capacidad D2D)
220. Generar Kd2d-UE1
basado en Kasme y
Rd2d aleatorio
225. Adjuntar aceptación (Rd2d)
230. Kd2d-UE1 con
S-TMSI asociado
235. Registro de área D2D en DRSF
240. Derivar Kd2d-UE1
basado en Kasme
y Rd2d
245. Guardar Kd2d-UE1
asociado con información de
ubicación de UE1 y S-TMSI
250. Volver a
modo inactivo
255. Servicio D2D
(ID UE1, p.ej. S-TMSI)
260A. Solicitud conexión RRC
260B. Configuración conexión RRC
265. Completar configuración conexión RRC
(indicando nueva razón para D2D,
incluyendo S-TMSI de UE1)
270. Generar Kd2d_serv
basado en Kd2d-UE1 y
Rd2d* (o S-TMSI UE2)
275. (Kd2d_final, Rd2d* (o
S-TMSI UE2))
280. Guardar Kd2d_serv
como la clave de seguridad
para servicio D2D con UE1
285. (Rd2d* o S-TMSI UE2)
290. Derivar Kd2d_serv
basado en Kd2d-UE1 y
Rd2d* (o S-TMSI UE2)
295. Kd2d_serv se comparte entre UE1 y UE2
para asegurar la conexión D2D

FIG.2

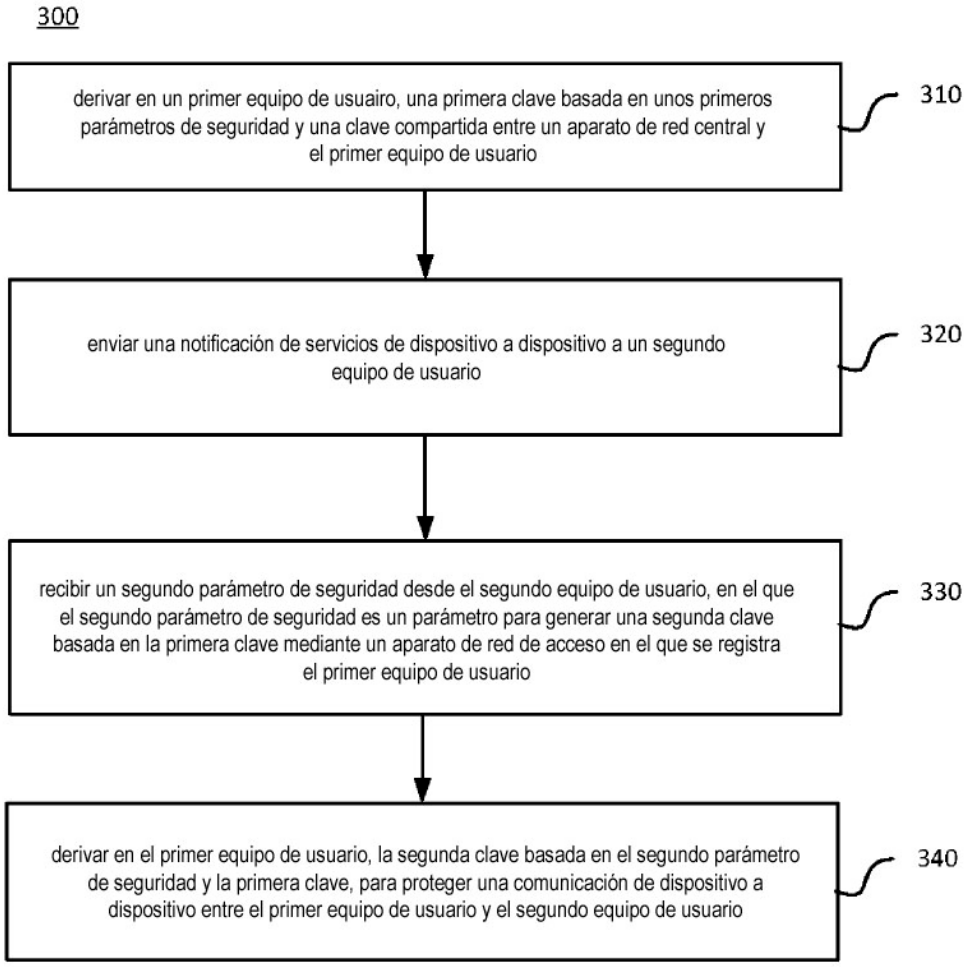
300
derivar en un primer equipo de usuairo, una primera clave basada en unos primeros parámetros de seguridad y una clave compartida entre un aparato de red central y el primer equipo de usuario
310
enviar una notificación de servicios de dispositivo a dispositivo a un segundo equipo de usuario
320
recibir un segundo parámetro de seguridad desde el segundo equipo de usuario, en el que el segundo parámetro de seguridad es un parámetro para generar una segunda clave basada en la primera clave mediante un aparato de red de acceso en el que se registra el primer equipo de usuario
330
derivar en el primer equipo de usuario, la segunda clave basada en el segundo parámetro de seguridad y la primera clave, para proteger una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario
340

FIG. 3

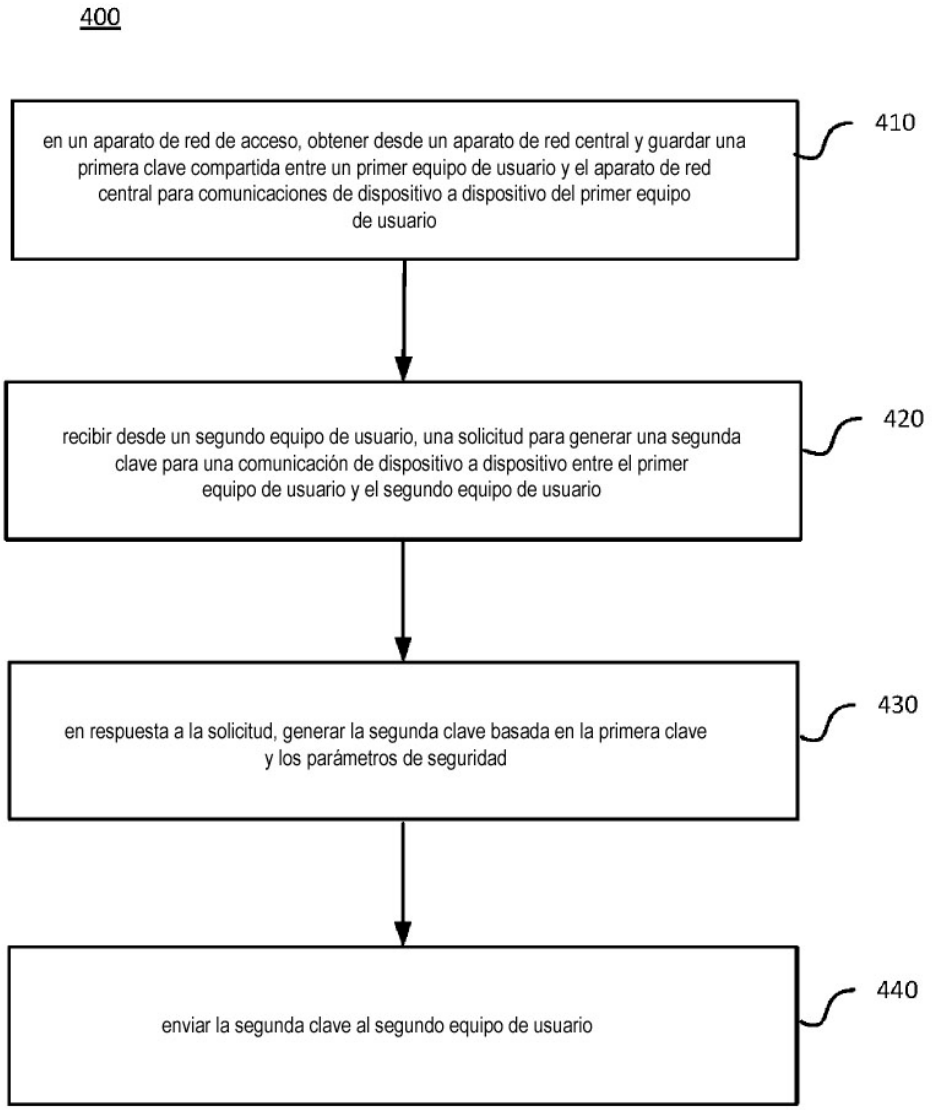
400
en un aparato de red de acceso, obtener desde un aparato de red central y guardar una primera clave compartida entre un primer equipo de usuario y el aparato de red central para comunicaciones de dispositivo a dispositivo del primer equipo de usuario
410
recibir desde un segundo equipo de usuario, una solicitud para generar una segunda clave para una comunicación de dispositivo a dispositivo entre el primer equipo de usuario y el segundo equipo de usuario
420
en respuesta a la solicitud, generar la segunda clave basada en la primera clave y los parámetros de seguridad
430
enviar la segunda clave al segundo equipo de usuario
440

FIG. 4

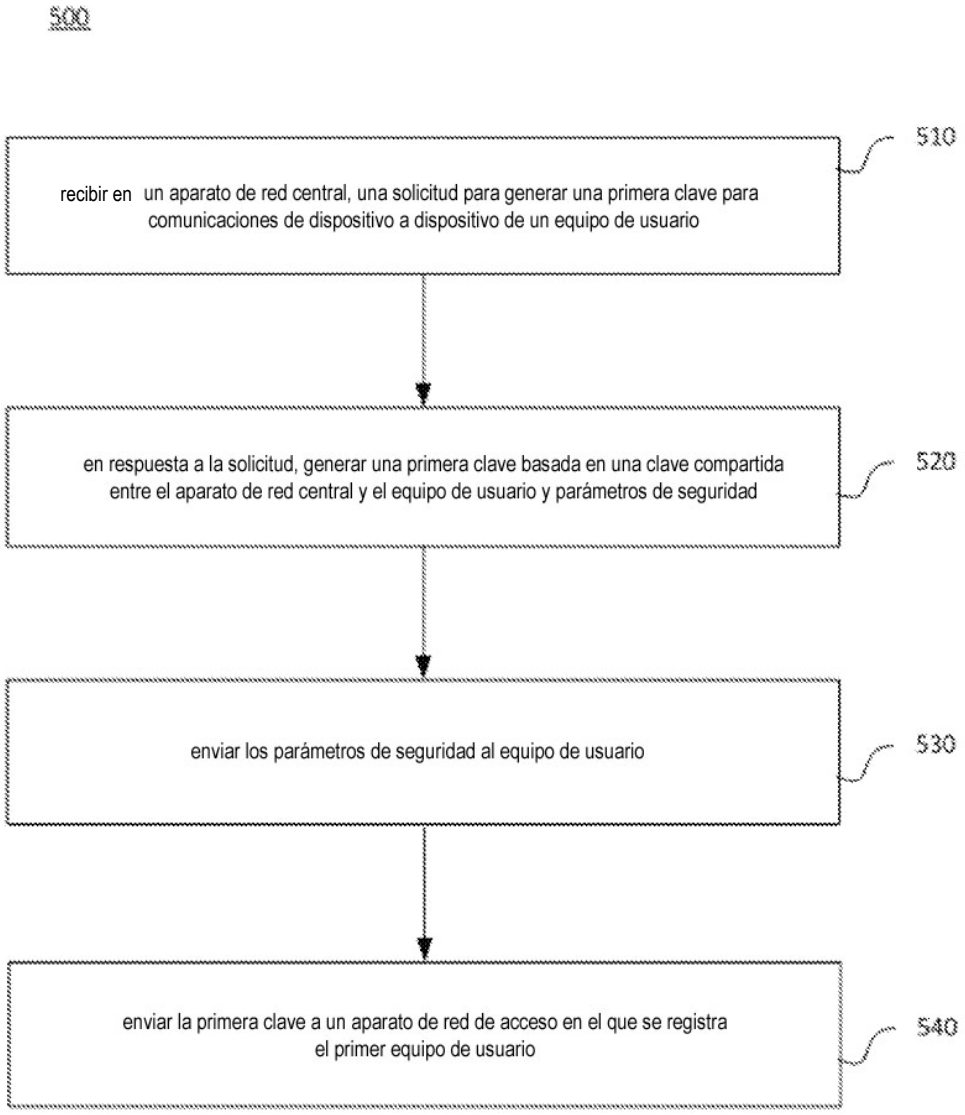
500
recibir en un aparato de red central, una solicitud para generar una primera clave para comunicaciones de dispositivo a dispositivo de un equipo de usuario
510
en respuesta a la solicitud, generar una primera clave basada en una clave compartida entre el aparato de red central y el equipo de usuario y parámetros de seguridad
520
enviar los parámetros de seguridad al equipo de usuario
530
enviar la primera clave a un aparato de red de acceso en el que se registra el primer equipo de usuario
540

FIG.5

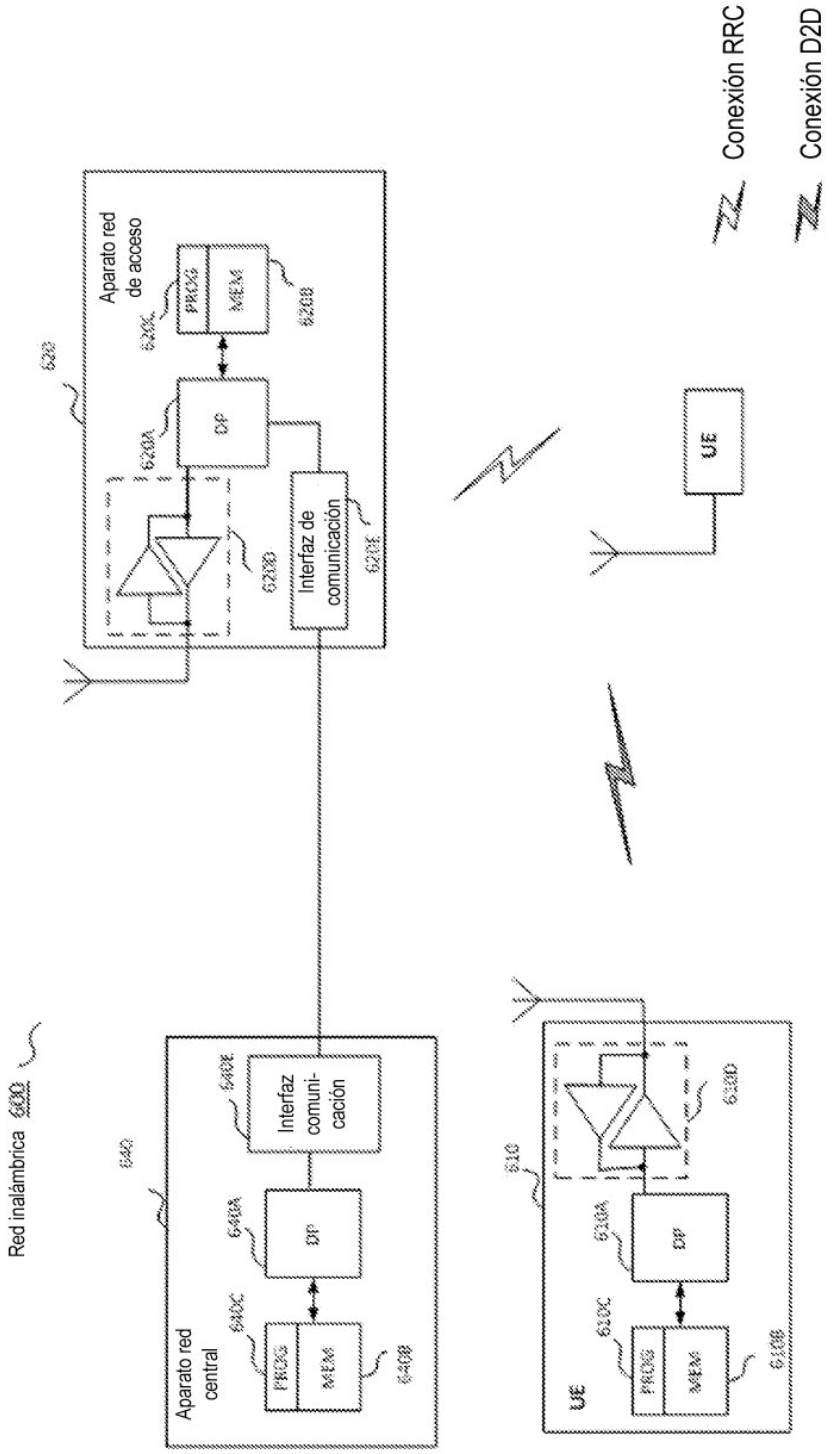
Red inalámbrica 600
Aparato red central
640
640C
PROG
MEM
640B
640A
DP
640E
Interfaz comuni-cación
UE
610
610C
PROG
MEM
610B
610A
DP
610D
Aparato red de acceso
620
620C
PROG
MEM
620B
620A
DP
620D
Interfaz de comunicación
620E
UE
Conexión RRC
Conexión D2D

FIG.6