

CONMUTACIÓN DE TRAYECTORIA ENTRE RETRANSMISORES Y

PROCEDIMIENTOS DE SEGURIDAD

CAMPO TÉCNICO

- 5 Diversas realizaciones de ejemplo se refieren al campo de la comunicación y, en particular, a dispositivos, métodos, aparatos y medios de almacenamiento legibles por ordenador para conmutación de trayectoria entre retransmisores y procedimientos de seguridad.

ANTECEDENTES

- 10 La retransmisión de equipo de usuario (UE) a red se puede referir a uno o más retransmisores, tal como un retransmisor de UE a red (U2N) de capa 3 y un retransmisor de UE a red de capa 2. La conmutación de trayectoria entre dos trayectorias de comunicación de red indirecta para retransmisión de UE a red puede implicar escenarios de conmutación de trayectoria de servicio. Durante la
- 15 conmutación de trayectoria, se podría tener en cuenta la continuidad de servicio y el retardo o las interrupciones del servicio.

SUMARIO

- En general, las realizaciones de ejemplo de la presente divulgación proporcionan dispositivos, métodos, aparatos y medios de almacenamiento
- 20 legibles por ordenador para conmutación de trayectoria entre procedimientos de seguridad de retransmisores.

- En un primer aspecto, se proporciona un dispositivo terminal remoto. El dispositivo terminal remoto comprende al menos un procesador, y al menos una memoria que almacena instrucciones. Las instrucciones, cuando son ejecutadas
- 25 por el al menos un procesador, hacen que el dispositivo terminal remoto al

menos: obtenga una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un procedimiento de seguridad de plano de usuario (UP); basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de origen con un RSC de origen, seleccione un RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen, y una pluralidad de indicadores asociados con la pluralidad de RSC; y seleccione, para la conmutación de trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

En un segundo aspecto, se proporciona un dispositivo terminal remoto. El dispositivo terminal remoto comprende al menos un procesador, y al menos una memoria que almacena instrucciones. Las instrucciones, cuando son ejecutadas por el al menos un procesador, hacen que el dispositivo terminal remoto al menos: obtenga una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y determine desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

En un tercer aspecto, se proporciona un dispositivo de función de servidor de autenticación (AUSF). El dispositivo de AUSF comprende al menos un procesador y al menos una memoria que almacena instrucciones. Las instrucciones, cuando son ejecutadas por el al menos un procesador, hacen que el dispositivo AUSF al menos: genere una clave raíz independiente de un código

de selección de retransmisión (RSC), usándose la clave raíz para generar al menos una clave de servicios basados en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y transmita, a un dispositivo de
5 función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

En un cuarto aspecto, se proporciona un método. El método comprende: obtener, en un dispositivo terminal remoto, una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de
10 RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un procedimiento de seguridad de plano de usuario (UP); basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de origen con un RSC de origen, seleccionar un
15 RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen, y una pluralidad de indicadores asociados con la pluralidad de RSC; y seleccionar, para la conmutación de trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

En un quinto aspecto, se proporciona un método. El método comprende:
20 obtener, en un dispositivo terminal remoto, una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y determinar desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

25 En un sexto aspecto, se proporciona un método. El método comprende:

generar, en un dispositivo de función de servidor de autenticación (AUSF), una clave raíz independiente de un código de selección de retransmisión (RSC), usándose la clave raíz para generar al menos una clave de servicios basados en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y transmitir, a un dispositivo de función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

En un séptimo aspecto, se proporciona un aparato. El aparato comprende medios para realizar el método de acuerdo con el tercer, cuarto o quinto aspecto.

10 En un octavo aspecto, se proporciona un medio legible por ordenador que comprende instrucciones de programa. Las instrucciones, cuando son ejecutadas por un aparato, hacen que el aparato realice el método de acuerdo con el tercer, cuarto o el quinto aspectos.

En un noveno aspecto, se proporciona un programa informático que comprende instrucciones que, cuando son ejecutadas por un aparato, hacen que el aparato al menos realice el método de acuerdo con el tercer, cuarto o quinto aspecto.

En un décimo aspecto, se proporciona un dispositivo. El dispositivo comprende circuiterías para realizar: obtener, en un dispositivo terminal remoto, una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un procedimiento de seguridad de plano de usuario (UP); basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal

20

25

retransmisor de origen con un RSC de origen, seleccionar un RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen, y una pluralidad de indicadores asociados con la pluralidad de RSC; y seleccionar, para la conmutación de trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

En un undécimo aspecto, se proporciona un dispositivo. El dispositivo comprende circuiterías para realizar: obtener, en un dispositivo terminal remoto, una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y determinar desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

En un duodécimo aspecto, se proporciona un dispositivo. El dispositivo comprende circuiterías para realizar: generar, en un dispositivo de función de servidor de autenticación (AUSF), una clave raíz independiente de un código de selección de retransmisión (RSC), usándose la clave raíz para generar al menos una clave de servicios basados en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y transmitir, a un dispositivo de función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

Otras características y ventajas de las realizaciones de la presente divulgación también serán evidentes a partir de la siguiente descripción de realizaciones específicas cuando se leen junto con los dibujos adjuntos, que ilustran, a modo de ejemplo, los principios de las realizaciones de la divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se presentan realizaciones de la divulgación en el sentido de ejemplos y

sus ventajas se explican con mayor detalle a continuación, con referencia a los dibujos adjuntos, en los que:

la figura 1A ilustra un entorno de comunicación de ejemplo en el que se pueden implementar realizaciones de la presente divulgación;

5 la figura 1B ilustra un procedimiento de establecimiento de seguridad de PC5 para comunicación de retransmisión de UE a red de ProSe de 5G a través de plano de usuario;

10 la figura 1C ilustra un procedimiento de establecimiento de seguridad de PC5 para comunicación de retransmisión de UE a red de ProSe de 5G a través de plano de control;

la figura 2 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo de selecciones de RSC de acuerdo con algunas realizaciones de la presente divulgación;

15 la figura 3 ilustra un diagrama de señalización de ejemplo que muestra un proceso de ejemplo de selecciones de RSC de acuerdo con algunas realizaciones de la presente divulgación;

20 la figura 4 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo de selección de un RSC y un retransmisor basado en un indicador de seguridad de CP de acuerdo con algunas realizaciones de la presente divulgación;

la figura 5 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo para optimizar procedimientos de seguridad de acuerdo con algunas realizaciones de la presente divulgación;

25 la figura 6 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo para optimizar un procedimiento de seguridad de CP de acuerdo con

algunas realizaciones de la presente divulgación;

la figura 7 ilustra un diagrama de señalización de ejemplo que muestra un procedimiento de seguridad de UP optimizado de acuerdo con algunas realizaciones de la presente divulgación;

5 la figura 8 ilustra un diagrama de señalización de ejemplo que muestra un procedimiento de seguridad de CP de acuerdo con algunas realizaciones de la presente divulgación;

la figura 9 muestra un diagrama de bloques simplificado de un dispositivo que es adecuado para implementar realizaciones de ejemplo de la presente
10 divulgación; y

la figura 10 muestra un diagrama de bloques de un medio legible por ordenador de ejemplo de acuerdo con algunas realizaciones de la presente divulgación.

En todos los dibujos, los mismos números de referencia, o unos similares,
15 representan el mismo elemento, o uno similar.

DESCRIPCIÓN DETALLADA

El principio de la presente divulgación se describirá a continuación con referencia a algunas realizaciones de ejemplo. Se ha de entender que estas realizaciones se describen solo para facilidad de entendimiento y para ayudar a
20 los expertos en la materia a entender e implementar la presente divulgación, sin sugerir ninguna limitación en cuanto al alcance de la divulgación. La divulgación descrita en el presente documento se puede implementar de diversas formas que no sean las descritas a continuación.

En la descripción y reivindicaciones siguientes, a menos que se defina lo
25 contrario, todos los términos técnicos y científicos usados en el presente

documento tienen el mismo significado que entendería comúnmente un experto en la materia a la que pertenece esta divulgación.

Referencias en la presente divulgación a "una realización", "una realización de ejemplo" y similares indican que la realización descrita puede
5 incluir un rasgo, estructura o característica particular, pero no es necesario que cada realización incluya el rasgo, estructura o característica particular. Además, tales expresiones no están haciendo referencia necesariamente a la misma realización. Además, cuando un rasgo, estructura o característica particular se describe en conexión con una realización de ejemplo, se afirma que está dentro
10 del conocimiento de un experto en la materia afectar a tal rasgo, estructura o característica en conexión con otras realizaciones, ya se describa explícitamente o no.

Se deberá entender que, aunque los términos "primero" y "segundo" etc., se pueden usar en el presente documento para describir diversos elementos,
15 estos elementos no deberían estar limitados por estos términos. Estos términos se usan solo para distinguir funcionalidades de diversos elementos. Como se usa en el presente documento, la expresión "y/o" incluye todas y cada una de las combinaciones de uno o más de los términos enumerados.

La terminología usada en el presente documento es solo para el fin de
20 describir realizaciones particulares y no pretende ser limitante de realizaciones de ejemplo. Como se usan en el presente documento, se pretende que las formas singulares "un", "una", "el" y "la" incluyan asimismo las formas plurales, a menos que el contexto indique claramente lo contrario. Se entenderá adicionalmente que las expresiones "comprende", "comprendiendo/que
25 comprende", "tiene", "teniendo/que tiene", "incluye" y/o "incluyendo/que incluye",

cuando se usan en el presente documento, especifican la presencia de rasgos, elementos y/o componentes etc., expuestos, pero no excluyen la presencia o adición de otros uno o más rasgos, elementos o componentes diferentes, y/o combinaciones de los mismos. Como se usa en el presente documento, "al menos uno de los siguientes: <una lista de dos o más elementos>" y "al menos uno de <una lista de dos o más elementos>" y enunciados similares, en donde la lista de dos o más elementos se une mediante "y" u "o", significan al menos uno cualquiera de los elementos, o al menos dos cualesquiera o más de los elementos, o al menos todos los elementos.

10 Como se usa en esta solicitud, el término "circuitería" se puede referir a uno o más o a la totalidad de los siguientes:

(a) implementaciones de circuito solo de hardware (tales como implementaciones en circuitería solo analógica y/o digital) y

(b) combinaciones de circuitos de hardware y software, tales como (según sea aplicable):

(i) una combinación de circuito(s) de hardware analógico(s) y/o digital(es) con software/firmware y

(ii) cualquier porción de procesador(es) de hardware con software (incluyendo procesador(es) de señales digitales), software y memoria(s) que trabajan conjuntamente para hacer que un aparato, tal como un teléfono móvil o servidor, realice diversas funciones) y

(c) circuito(s) de hardware y/o procesador(es), tales como un(os) microprocesador(es) o una porción de un(os) microprocesador(es), que requieren software (por ejemplo, firmware) para el funcionamiento, pero el software puede no estar presente cuando no es necesario para el

funcionamiento.

Esta definición de circuitería es aplicable a todos los usos de este término en esta solicitud, incluyendo en cualquier reivindicación. Como un ejemplo adicional, como se usa en esta solicitud, el término circuitería también cubre una
5 implementación de meramente un circuito de hardware o procesador (o múltiples procesadores) o una porción de un circuito de hardware o procesador y su software y/o firmware adjunto. El término circuitería también cubre, por ejemplo, y si es aplicable al elemento de reivindicación particular, un circuito integrado de banda base o circuito integrado de procesador para un dispositivo móvil o un
10 circuito integrado similar en servidor, un dispositivo de red celular u otro dispositivo informático o de red.

Como se usa en el presente documento, la expresión "red de comunicación" se refiere a una red que sigue cualquier norma de comunicación adecuada, tales como sistemas de la quinta generación (5G) Evolución a Largo
15 Plazo (LTE), LTE Avanzada (LTE-A), Acceso Múltiple por División de Código de Banda Ancha (WCDMA), Acceso por Paquetes de Alta Velocidad (HSPA), Internet de las Cosas de Banda Estrecha (NB-IoT) y así sucesivamente. Además, la comunicación entre un dispositivo terminal y un dispositivo de red en la red de comunicación se puede realizar de acuerdo con cualquier protocolo de
20 comunicación de generación adecuado, incluyendo, pero sin limitación, los protocolos de comunicación de la cuarta generación (4G), 4.5G, de nueva radio (NR) de la quinta generación (5G) futura, y/o cualquier otro protocolo o bien conocido en la actualidad o bien que se vaya a desarrollar en el futuro. Las realizaciones de la presente divulgación se pueden aplicar en diversos sistemas
25 de comunicación. Dado el rápido desarrollo en la comunicación, también

existirán, por supuesto, tecnologías y sistemas de comunicación de tipo futuro con los que se pueda materializar la presente divulgación. No se debería ver como que limita el alcance de la presente divulgación a solo el sistema mencionado anteriormente.

5 Como se usa en el presente documento, la expresión "dispositivo de red" hace referencia a un nodo en una red de comunicación a través del cual un dispositivo terminal accede a la red y recibe servicios de la misma. El dispositivo de red se puede referir a una estación base (BS) o un punto de acceso (AP), por ejemplo, un nodo B (Nodo B o NB), un Nodo B evolucionado (eNodo B o eNB),
10 un Nodo B de próxima generación de NR (gNB), una unidad de radio remota (RRU), una unidad de entrada de radio (RH), una unidad de entrada de radio remota (RRH), un retransmisor, un nodo de baja potencia tal como uno de tipo femto, pico, y así sucesivamente, dependiendo de la terminología y la tecnología aplicadas. Una arquitectura dividida de RAN comprende una gNB-CU (unidad
15 centralizada, que aloja RRC, SDAP y PDCP) que controla una pluralidad de gNB-DU (unidad distribuida, que aloja RLC, MAC y PHY). Un nodo de retransmisión puede corresponder a la parte de DU del nodo de IAB.

 La expresión "dispositivo terminal" se refiere a cualquier dispositivo de extremo que pueda ser capaz de una comunicación inalámbrica. A modo de
20 ejemplo, en lugar de limitación, un dispositivo terminal también se puede denominar dispositivo de comunicación, UE, estación de abonado (SS), estación de abonado portátil, estación móvil (MS) o terminal de acceso (AT). El dispositivo terminal puede incluir, pero sin limitación, un teléfono móvil, un teléfono celular, un teléfono inteligente, teléfonos de voz sobre IP (VoIP), teléfonos de bucle local
25 inalámbrico, una tableta, un dispositivo terminal ponible, un asistente digital

personal (PDA), ordenadores portátiles, ordenador de sobremesa, dispositivos terminales de captura de imágenes tales como cámaras digitales, dispositivos terminales de juegos, aparatos de almacenamiento y reproducción de música, dispositivos terminales inalámbricos montados en vehículo, puntos de extremo
5 inalámbricos, estaciones móviles, equipo embebido en ordenador portátil (LEE), equipo montado en ordenador portátil (LME), llaves USB, dispositivos inteligentes, equipo inalámbrico en las instalaciones del cliente (CPE), un dispositivo de Internet de las Cosas (IoT), un reloj u otro dispositivo ponible, un visualizador montado en la cabeza (HMD), un vehículo, un dron, un dispositivo y
10 aplicaciones de tipo médico (por ejemplo, cirugía remota), un dispositivo y aplicaciones de tipo industrial (por ejemplo, un robot y/u otros dispositivos inalámbricos que operan en un contexto industrial y/o contexto de cadena de procesamiento automatizado), un dispositivo de electrónica de consumo, un dispositivo que opera en redes inalámbricas comerciales y/o industriales y
15 similares. El dispositivo terminal también puede corresponder a una parte de terminación móvil (MT) del nodo de acceso y red de retroceso integrado (IAB) (también conocido como nodo de retransmisión). En la siguiente descripción, se pueden usar de forma intercambiable las expresiones "dispositivo terminal", "dispositivo de comunicación", "terminal", "equipo de usuario" y "UE".

20 Aunque las funcionalidades descritas en el presente documento se pueden realizar, en diversas realizaciones de ejemplo, en un nodo de red fijo y/o inalámbrico, en otras realizaciones de ejemplo, las funcionalidades se pueden implementar en un aparato de equipo de usuario (tal como un teléfono celular u ordenador de tipo tableta u ordenador portátil u ordenador de sobremesa o
25 dispositivo de IoT móvil o dispositivo de IoT fijo). Este aparato de equipo de

usuario, por ejemplo, puede estar equipado con capacidades correspondientes como se describe en conexión con el nodo o nodos de red fijos y/o inalámbricos, según sea apropiado. El aparato de equipo de usuario puede ser un dispositivo de control de equipo de usuario, tal como un conjunto de chips o procesador, configurado para controlar el equipo de usuario cuando se instala en el mismo. Los ejemplos de tales funcionalidades incluyen la función de servidor de arranque y/o el servidor de abonado doméstico, que se puede implementar en el aparato de equipo de usuario proporcionando, al aparato de equipo de usuario, de software configurado para hacer que el aparato de equipo de usuario funcione desde el punto de vista de estas funciones/nodos.

Como se describe, la conmutación de trayectoria entre dos trayectorias de comunicación de red indirecta para retransmisión de UE a red puede implicar escenarios de conmutación de trayectoria de servicio, por ejemplo, retransmisión de UE a red de capa 3 con función de interfuncionamiento no de 3GPP (N3IWF) conmutando desde/a retransmisión de UE a red de capa 3 con N3IWF, retransmisión de UE a red de capa 3 sin conmutación de N3IWF desde/a retransmisión de UE a red de capa 3 sin N3IWF, retransmisión de UE a red de capa 3 sin conmutación de N3IWF desde/a retransmisión de UE a red de capa 3 con N3IWF, conmutación de retransmisión de UE a red de capa 2 desde/a retransmisión de UE a red de capa 2, conmutación de retransmisión de UE a red de capa 2 desde/a retransmisión de UE a red de capa 3 sin N3IWF, y conmutación de retransmisión de UE a red de capa 2 desde/a retransmisión de UE a red de capa 3 con N3IWF.

Se entiende que la continuidad de servicio en diferentes casos de conmutación de trayectoria se puede conseguir a través de capa de aplicación o

continuidad de sesión. Para la continuidad de servicio durante la conmutación de trayectoria, se pueden considerar algunos aspectos, por ejemplo, cuáles son los desencadenantes y criterios para la conmutación de trayectoria, cómo seleccionar un retransmisor de UE a red para conmutación de trayectoria, 5 identificar el procedimiento de conmutación de trayectoria con consideración de continuidad de servicio, identificar cómo se logra la continuidad de servicio para la solución en la conmutación de trayectoria.

Para los desencadenantes y criterios para conmutación de trayectoria, el UE remoto puede conmutar trayectoria cuando los umbrales de medición 10 configurados de NG-RAN y los criterios se satisfacen o se basan en reglas de reelección de la capa de aplicación, si las hay. Además, si múltiples UE de retransmisión de UE a red satisfacen los criterios de reelección de retransmisión, el UE remoto selecciona la retransmisión de UE a red objetivo para la conmutación de trayectoria basándose en las reglas de política de ProSe 15 de 5G o política de selección de ruta de UE (URSP) y el manejo de tráfico de UE remoto con la consideración: el UE remoto selecciona en primer lugar un UE de retransmisión objetivo que tiene el mismo tipo que el UE de retransmisión original, si esto falla, entonces el UE remoto reevalúa la URSP o sigue evaluando el siguiente descriptor de selección de ruta (RSD) de la URSP seleccionada para 20 la selección de retransmisor objetivo. Además, el UE remoto puede usar reglas de reelección desde la capa de aplicación (por ejemplo, proporcionadas por un servidor de aplicaciones), el UE remoto puede descubrir que hay múltiples UE de retransmisión de UE a red que satisfacen las reglas de reelección y, a continuación, selecciona el UE de retransmisión de UE a red objetivo basándose 25 en prioridad en las reglas de reelección desde la capa de aplicación.

Para el caso de conmutación de trayectoria entre dos trayectorias de retransmisión de UE a red de capa 3 indirectas usando N3IWF, se puede seleccionar el uso de protocolo de movilidad y multiubicación (MOBIKE) para trabajo normativo.

- 5 Sin embargo, cuando un UE remoto conmuta a otro UE de retransmisión, puede desencadenar una nueva autenticación y generación de clave de usuario remoto de ProSe (PRUK), que puede costar tiempo y recursos, por lo tanto, impacta en la continuidad del servicio y provoca una interrupción en el servicio.

En algunas realizaciones, la presente divulgación propone soluciones
10 para optimizar el procedimiento de selección de retransmisor basándose en el indicador de seguridad de CP asociado con RSC, optimizar además el procedimiento de autenticación de seguridad y, a continuación, mejorar la continuidad de servicio después de la conmutación de trayectoria entre retransmisiones de ProSe L3.

- 15 Un principio e implementaciones de la presente divulgación se describirán con detalle a continuación con referencia a las figuras 1A a 10. La figura 1A ilustra un diagrama esquemático de un entorno de comunicación 100 de ejemplo en el que se pueden implementar realizaciones de la presente divulgación. Como se muestra en la figura 1A, el entorno de comunicación 100 puede implicar
20 un UE remoto 110, retransmisores de UE a red 121 y 122, NG-RAN 131 y 132, un núcleo de 5G (5GC) 140 y una red de datos 145. Además, se ha de entender que el número de dispositivos es únicamente para facilitar el entendimiento sin sugerir ninguna limitación. El entorno de comunicación 100 puede incluir cualquier número o tipo adecuado de los dispositivos adaptados para
25 implementar realizaciones de la presente divulgación.

Como se muestra en la figura 1A, el UE remoto 110 se puede conectar al retransmisor de UE a red 121 a través de una interfaz PC5 y comunicarse con la red de datos 145 a través del retransmisor de UE a red o el retransmisor de UE a red con acceso de N3IWF. Además, el entorno de comunicación 100 puede

5 soportar continuidad de servicio para el UE remoto 110 conectado a la red de datos 145 a través del conmutador de retransmisor de UE a red de ProSe de 5G 121 (es decir, trayectoria de comunicación de red indirecta) a otra trayectoria de comunicación de red indirecta, por ejemplo, a través del retransmisor de UE a red de ProSe de 5G 122.

10 En el contexto de la presente divulgación, la expresión "retransmisor de UE a red" se puede usare indistintamente con "retransmisor de UE a red de capa 3 de ProSe de 5G", "retransmisor de UE a red de ProSe de 5G", "retransmisor de U2N", "retransmisor de UE" o "dispositivo terminal retransmisor". La expresión "UE remoto" se puede usar indistintamente con "UE remoto de ProSe 5G" o

15 "dispositivo terminal retransmisor".

Como se conoce, ProSe pueden ser servicios que se pueden proporcionar por el sistema de proyecto de asociación de tercera generación (3GPP) basándose en que los UE están en proximidad entre sí. La característica se introdujo en LTE y evolucionó en el sistema 5G (5GS). Los habilitadores de

20 5GS para ProSe incluyen las siguientes funciones: descubrimiento directo de ProSe de 5G; comunicación directa de ProSe de 5G; y retransmisión de U2N de ProSe de 5G.

PC5 es un punto de referencia entre los UE habilitados para ProSe usados para los planos de control y de usuario para descubrimiento directo de

25 ProSe de 5G, comunicación directa de ProSe de 5G y retransmisión de U2N de

ProSe de 5G.

Las comunicaciones en el entorno de comunicación 100 se pueden implementar de acuerdo con cualquier protocolo o protocolos de comunicación apropiados, comprendiendo, pero sin limitación, protocolos de comunicación celulares de la primera generación (1G), de la segunda generación (2G), de la tercera generación (3G), de la cuarta generación (4G), de la quinta generación (5G), o de la futura sexta generación (6G), protocolos de comunicación de red local inalámbrica tales como 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y similares, y/o cualquier otro protocolo conocido en la actualidad o que se desarrolle en el futuro. Además, la comunicación puede utilizar cualquier tecnología de comunicación inalámbrica apropiada, comprendiendo, pero sin limitación: Acceso Múltiple por División de Código (CDMA), Acceso Múltiple por División de Frecuencia (FDMA), Acceso Múltiple por División de Tiempo (TDMA), Dúplex por División de Frecuencia (FDD), Dúplex por División de Tiempo (TDD), Múltiples Entradas - Múltiples Salidas (MIMO), Multiplexación por División de Frecuencia Ortogonal (OFDM), OFDM de ensanchamiento de Transformada Discreta de Fourier (DFT-s-OFDM) y/o cualquier otra tecnología conocida en la actualidad o que se vaya a desarrollar en el futuro.

La figura 1B ilustra un procedimiento de establecimiento de seguridad de PC5 150 para comunicación de retransmisión de UE a red de ProSe de 5G a través de plano de usuario (UP). El procedimiento 150 puede implicar el UE remoto 110, el retransmisor de UE a red 121, una función de gestión de nombre de descubrimiento directo de 5G (DDNMF) 151 del UE remoto 110, una función de gestión de clave de ProSe (PKMF) 152 del UE remoto 110, una DDNMF de

5G 153 del retransmisor 121, una PKMF 154 del retransmisor 121 y una gestión de datos unificados (UDM) (o una función de soporte de enlace (BSF) o un servidor de abonado doméstico (HSS)) 155 del UE remoto 110.

El UE remoto de ProSe de 5G se puede aprovisionar con los materiales
5 de seguridad de descubrimiento y la clave de usuario remoto de Prose (es decir, UP-PRUK) cuando está en cobertura. Estos materiales de seguridad pueden estar asociados con un tiempo de expiración, después del cual se vuelven no válidos. Si el UE no tiene materiales de seguridad de descubrimiento válidos, el UE remoto de ProSe de 5G se puede necesitar conectar a la función de gestión
10 de clave de ProSe de 5G (PKMF) y obtener unos nuevos para usar los servicios de retransmisión de UE a red de ProSe de 5G.

El procedimiento se describe para el escenario en el que la PKMF de 5G del UE remoto de ProSe de 5G es diferente de la PKMF de 5G del retransmisor de UE a red de ProSe de 5G. Si tanto el UE remoto de ProSe de 5G como el
15 retransmisor de UE a red de ProSe de 5G son atendidos por una única PKMF de 5G, la PKMF de 5G puede asumir el papel de la PKMF de 5G del UE remoto de ProSe de 5G y la PKMF de 5G del retransmisor de UE a red de ProSe de 5G y los intercambios de mensajes de PKMF inter 5G pueden no ser necesarios.

Como se muestra en la figura 1b, en 160a, el UE remoto de ProSe de 5G
20 puede obtener la dirección de PKMF de 5G desde la DDNMF de 5G de su HPLMN. Como alternativa, el UE remoto de ProSe de 5G se puede aprovisionar con la dirección de PKMF de 5G por una función de control de política (PCF). Si el UE remoto de ProSe de 5G se aprovisiona con la dirección de PKMF de 5G, el UE remoto de ProSe de 5G puede acceder a la PKMF de 5G directamente sin
25 solicitar la misma desde la DDNMF de 5G. En caso de que el UE remoto de

ProSe de 5G no pueda acceder a la PKMF de 5G usando la dirección de PKMF de 5G aprovisionada, el UE remoto de ProSe de 5G puede solicitar la dirección de PMKF de 5G a la DDNMF de 5G.

En 160b, el UE remoto de ProSe de 5G puede establecer una conexión
5 segura con la PKMF de 5G a través de punto de referencia de PC8. La seguridad para la interfaz de PC8 se basa en la seguridad de Ua si se usa una arquitectura de arranque genérica (GBA) o una seguridad de Ua* si se usa una autenticación y gestión de claves para aplicaciones (AKMA). La PKMF de 5G del UE remoto de ProSe de 5G puede comprobar si el UE remoto de ProSe de 5G está autorizado
10 a recibir el servicio de retransmisión de UE a red, y si el UE está autorizado, la PKMF de 5G del UE remoto de ProSe de 5G proporciona los materiales de seguridad de descubrimiento al UE remoto de ProSe de 5G. Si el UE remoto de ProSe de 5G proporciona una lista de redes visitadas, la PKMF de 5G del UE remoto de ProSe de 5G puede solicitar los materiales de seguridad de
15 descubrimiento de las PKMF de 5G de los retransmisores de UE a red de ProSe de 5G potenciales desde los que el UE remoto de ProSe de 5G contiene los servicios de retransmisión. La PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede incluir las políticas de seguridad de PC5 para el UE remoto de ProSe de 5G.

20 Se hace notar que la PKMF de 5G se puede configurar localmente con la información de autorización del UE. De lo contrario, la PKMF de 5G puede interactuar con la UDM del UE para recuperar la información de autorización del UE. Además, el UE remoto de ProSe de 5G se aprovisiona por PCF con una lista de las redes visitadas potenciales para el servicio de retransmisión de UE a
25 red de ProSe de 5G (que se identifica por RSC).

En 160c, el retransmisor de UE a red de ProSe de 5G puede obtener la dirección de PKMF de 5G desde su red móvil pública terrestre (HPLMN) de la misma forma que se describe en la etapa 160a.

En 160d, el retransmisor de UE a red de ProSe de 5G puede establecer
5 una conexión segura con la PKMF de 5G a través del punto de referencia de PC8 como en la etapa 160b. La PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede comprobar si el retransmisor de UE a red de ProSe de 5G está autorizado a proporcionar el servicio de retransmisión de UE a red de ProSe de 5G, y si el UE está autorizado, la PKMF de 5G del retransmisor de UE a red de
10 ProSe de 5G puede proporcionar los materiales de seguridad de descubrimiento al retransmisor de UE a red de ProSe de 5G. La PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede incluir las políticas de seguridad de PC5 para el retransmisor de UE a red de ProSe de 5G.

En 161a, el UE remoto de ProSe de 5G puede enviar un mensaje de
15 solicitud de PRUK a su PKMF de 5G. El mensaje puede indicar que el UE remoto de ProSe de 5G está solicitando una UP-PRUK desde la PKMF de 5G. Si el UE remoto de ProSe de 5G ya tiene una UP-PRUK desde esta PKMF de 5G, el mensaje puede contener también el ID de UP-PRUK de la UP-PRUK.

Un identificador (ID) de UP-PRUK puede tomar la forma de cualquiera del
20 formato de identificador de acceso de red (NAI) o la cadena de 64 bits. Si el ID de UP-PRUK está en formato de NAI, es decir, nombre de usuario@dominio, la parte de dominio puede incluir un ID de HPLMN. La parte de nombre de usuario puede incluir la cadena de 64 bits.

En 161b, la PKMF de 5G puede comprobar si el UE remoto de ProSe de
25 5G está autorizado a recibir servicios de retransmisión de UE a red. Esto se

puede hacer usando la identidad del UE remoto de ProSe de 5G asociada con la clave usada para establecer la conexión segura entre el UE Remoto de ProSe de 5G y la PKMF de 5G en la etapa 160b. Si el UE remoto de ProSe de 5G está autorizado a recibir el servicio, la PKMF de 5G puede enviar una UP-PRUK y un ID de UP-PRUK al UE remoto de ProSe de 5G. Si se incluye una UP-PRUK e ID de UP-PRUK, el UE remoto de ProSe de 5G puede almacenar estos y borrar cualquiera previamente almacenado para esta PKMF de 5G.

Se hace notar que las etapas 160a, 160b, 161a, 161b se realizan cuando el UE remoto de ProSe de 5G está en cobertura.

10 En 162, el procedimiento de descubrimiento se puede realizar entre el UE remoto de ProSe de 5G y el retransmisor de UE a red de ProSe de 5G usando los parámetros de descubrimiento y el material de seguridad de descubrimiento.

15 En 163, el UE remoto de ProSe de 5G puede enviar una solicitud de comunicación directa (DCR) que contiene el ID de UP-PRUK o un identificador oculto de suscripción (SUCI) si el UE remoto no tiene un UP-PRUK válido, RSC del servicio de retransmisión de UE a red de ProSe de 5G y una clave para el parámetro de actualización 1 de PC5 de NR (KNRP) al retransmisor de UE a red de ProSe de 5G. Si el ID de UP-PRUK no está en formato de NAI, el mensaje de DCR puede incluir el ID de HPLMN del UE remoto de ProSe de 5G. El
20 procedimiento de establecimiento de seguridad de PC5 entre el UE remoto ProSe de 5G y el retransmisor de UE a red de ProSe de 5G que incluye parámetros de seguridad y negociación de política de seguridad y protección de mensajes en lo sucesivo en el presente documento puede seguir el establecimiento de seguridad uno a uno.

25 En 164a, el retransmisor de UE a red de ProSe de 5G puede enviar un

mensaje de solicitud de clave que contiene el ID de UP-PRUK o el parámetro de actualización de SUCI, RSC y KNRP 1 a su PKMF de 5G. El mensaje de solicitud de clave también puede incluir el ID de HPLMN del UE remoto de ProSe de 5G si se incluye en la DCR.

5 En 164b, al recibir el mensaje de solicitud de clave, la PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede comprobar si el retransmisor de UE a red de ProSe de 5G está autorizado para proporcionar servicio de retransmisión al UE remoto de ProSe de 5G basándose en la identidad del retransmisor de UE a red de ProSe de 5G asociada con la clave usada para
10 establecer la conexión de PC8 segura y el RSC recibido.

 Se observa que la PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede necesitar hacer la autorización de RSC basándose en su implementación. Además, si la información de autorización del retransmisor de UE a red de ProSe de 5G no está disponible localmente, la PKMF de 5G puede
15 solicitar la información de autorización de la UDM del retransmisor de UE a red de ProSe de 5G (no mostrada) usando el servicio Nudm_SDM_Get. Si el retransmisor de UE a red de ProSe de 5G está autorizado a proporcionar el servicio de retransmisión basándose en datos de suscripción de ProSe, la PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede enviar la solicitud de
20 clave con el ID de UP-PRUK o el SUCI a la PKMF de 5G del UE remoto de ProSe de 5G. La PKMF de 5G del retransmisor de UE a red de ProSe de 5G identifica la dirección de PKMF de 5G del UE remoto de ProSe de 5G basándose en el ID de UP-PRUK o el ID de HPLMN o SUCI del UE remoto de ProSe de 5G si está incluido en el mensaje de solicitud de clave.

25 Se observa que la PKMF de 5G del UE remoto de ProSe de 5G puede

necesitar hacer la autorización de RSC basándose en su implementación.

En 164c, al recibir el mensaje de solicitud de clave de la PKMF de 5G del retransmisor de UE a red de ProSe de 5G, la PKMF de 5G del UE remoto de ProSe de 5G puede comprobar si el UE remoto de ProSe de 5G está autorizado para usar el servicio de retransmisión. La comprobación de autorización de servicio de retransmisión se puede basar en el ID de UP-PRUK y el RSC incluidos en el mensaje de solicitud de clave o el SUPI del UE remoto y el RSC incluido en el mensaje de solicitud de clave. Si se incluye una SUCI en el mensaje de solicitud de clave, la PKMF de 5G del UE remoto de ProSe de 5G puede solicitar a la UDM del UE remoto de ProSe de 5G que desconecte la SUCI para obtener el SUPI usando el servicio Nudm_UEIdentifier_Decode, y la UDM invoca una suscripción función de desocultación de identificador (SIDF) para desocultar SUCI para obtener un identificador permanente de suscripción (SUPI). Si la información de autorización del UE remoto de ProSe de 5G no está disponible localmente, la PKMF de 5G puede solicitar la información de autorización de la UDM del UE remoto de ProSe de 5G (no mostrado).

Se observa que puede ser necesario considerar cuestiones de privacidad mientras se determina si el SUPI se ha de enviar a la PKMF. Para un control de privacidad, la UDM puede autorizar la PKMF basándose en su tipo de NF o el dominio de proveedor de servicio.

Si se requiere una nueva UP-PRUK, la PKMF de 5G puede realizar uno de los siguientes procedimientos (como se muestra en la etapa 164c):

Si la PKMF de 5G del UE remoto de ProSe de 5G soporta la interfaz Zpn a la BSF del UE remoto de ProSe de 5G, la PKMF de 5G del UE remoto de ProSe de 5G puede solicitar una información de inserción de GBA (GPI) para el UE

remoto de ProSe de 5G desde la BSF. Cuando se solicita el GPI, la PKMF de 5G puede incluir un ID de UP-PRUK en el campo de P-TID. Al recibir la GPI, la PKMF de 5G puede usar Ks_ext_NAF como la UP-PRUK.

Si la PKMF de 5G del UE remoto de ProSe de 5G soporta la interfaz de SBI (interfaz basada en servicio) a la BSF del UE remoto de ProSe de 5G, la PKMF de 5G puede solicitar la GPI a través de la interfaz de SBI. Al recibir la GPI, la PKMF de 5G puede usar Ks_ext_NAF como la UP-PRUK.

Si la 5G PKMF del UE remoto de ProSe de 5G soporta la interfaz PC4a al HSS del UE, entonces la PKMF de 5G del UE remoto de ProSe de 5G puede solicitar un vector de autenticación (AV) de GBA para el UE remoto de ProSe de 5G desde el HSS. Al recibir el AV, la PKMF de 5G forma localmente el GPI que incluye un ID de UP-PRUK en el campo de P-TID. La PKMF de 5G puede usar Ks_ext_NAF como la UP-PRUK.

Si la PKMF de 5G del UE remoto de ProSe de 5G se cubica o integra con la funcionalidad de BSF y soporta la interfaz de SBI a la UDM/HSS del UE remoto de ProSe de 5G, la PKMF de 5G puede solicitar el AV de GBA a través de una interfaz de SBI. Al recibir el AV, la PKMF de 5G forma localmente el GPI que incluye un ID de UP-PRUK en el campo de P-TID. La PKMF de 5G puede usar Ks_ext_NAF como la UP-PRUK.

Se observa que la GPI se soporta únicamente cuando se usa GBA.

En 164d, la PKMF de 5G del UE remoto de ProSe de 5G puede generar el parámetro de actualización de KNRP 2 y derivar el KNRP usando la UP-PRUK identificada por el ID de UP-PRUK, el RSC, el parámetro de actualización de KNRP 1 y el parámetro de actualización de KNRP 2. A continuación, la PKMF de 5G del UE remoto de ProSe de 5G puede enviar un mensaje de respuesta de

clave que contiene el KNRP y el parámetro de actualización de KNRP 2 a la PKMF de 5G del retransmisor de UE a red de ProSe de 5G. Este mensaje puede incluir GPI si se genera. La PKMF de 5G del UE remoto de ProSe de 5G puede incluir también el ID de usuario remoto del UE remoto de ProSe de 5G en el
5 mensaje de respuesta de clave al retransmisor de UE a red de ProSe de 5G. El ID de UP-PRUK se puede usar como un ID de usuario remoto en el presente documento.

En 164e, la PKMF de 5G del retransmisor de UE a red de ProSe de 5G puede enviar el mensaje de respuesta de clave al retransmisor de UE a red de
10 ProSe de 5G, que incluye ID de usuario remoto, KNRP, parámetro de actualización de KNRP 2, el GPI si se usa para calcular un UP-PRUK nuevo al retransmisor de UE a red.

En 165a, el retransmisor de UE a red de ProSe de 5G puede derivar la clave de sesión (KNRP-SESS) de KNRP y a continuación derivar la clave de
15 confidencialidad (NRPEK) (si es aplicable) y la clave de integridad (NRPIK) basándose en las políticas de seguridad de PC5. El retransmisor de UE a red de ProSe de 5G puede almacenar el ID de usuario remoto recibido en la etapa 4d. El retransmisor de UE a red de ProSe de 5G puede enviar un mensaje de orden de modo de seguridad directo al UE remoto de ProSe de 5G. Este mensaje
20 también puede incluir el parámetro de actualización de KNRP 2.

En 165b, si el UE remoto de ProSe de 5G recibe el mensaje que contiene el GPI, procesa el GPI. El UE remoto de ProSe de 5G puede derivar la UP-PRUK y obtener el ID de UP-PRUK del GPI.

El UE remoto de ProSe de 5G puede derivar KNRP a partir de su
25 UP-PRUK, RSC, parámetro de actualización de KNRP 1 y el parámetro de

actualización de KNRP 2 recibido. A continuación, puede derivar la clave de sesión (KNRP-SESS) y la clave de confidencialidad (NRPEK) (si es aplicable) y la clave de integridad (NRPIK) basándose en las políticas de seguridad de PC5 de la misma manera que el retransmisor de UE a red de ProSe de 5G y procesar la orden de modo de seguridad directo. La verificación satisfactoria de la orden de modo de seguridad directo garantiza al UE remoto de ProSe de 5G que el retransmisor de UE a red de ProSe de 5G está autorizado para proporcionar el servicio de retransmisión.

Se realiza el manejo de fallo de sincronización (para detalles de fallos de sincronización) cuando el UE procesa el desafío de autenticación en el GPI. El UE remoto de ProSe de 5G puede enviar un mensaje de fallo de modo de seguridad directo e incluir RAND y AUTS en el mensaje. El retransmisor de UE a red de ProSe de 5G puede enviar el mensaje de solicitud de clave a la PKMF de 5G del UE remoto de ProSe de 5G a través de la PKMF de 5G del retransmisor de UE a red de ProSe de 5G tras recibir el mensaje de fallo de modo de seguridad directo del UE remoto de ProSe de 5G. El mensaje de solicitud de clave puede incluir el ID de HPLMN del UE remoto de ProSe de 5G, el código de servicio de retransmisión y el parámetro de actualización de KNRP 1 junto con el RAND y el AUTS recibidos desde el UE remoto de ProSe de 5G. Si la PKMF de 5G del UE remoto de ProSe de 5G decide reintentar el procedimiento de inserción de GBA, la PKMF de 5G del UE remoto de ProSe de 5G puede solicitar GPI como se describe en la etapa 164c.

En 165c, el UE remoto de ProSe de 5G puede responder con un mensaje de modo de seguridad directo completo al retransmisor de UE a Red de ProSe de 5G.

En 165d, al recibir el mensaje de modo de seguridad directo completo, el retransmisor de UE a red de ProSe de 5G puede verificar el mensaje de modo de seguridad directo completo. La verificación satisfactoria del mensaje de modo de seguridad directo completo garantiza al retransmisor de UE a red de ProSe de 5G que el UE remoto de ProSe de 5G está autorizado para obtener el servicio de retransmisión.

En 165e, después de verificación satisfactoria, el retransmisor de UE a red de ProSe de 5G responde un mensaje de aceptación de comunicación directa al UE remoto de ProSe de 5G para completar el procedimiento de establecimiento de conexión de PC5.

En 166, el UE remoto de ProSe de 5G y el retransmisor de UE a red de ProSe de 5G continúan el resto del procedimiento para el servicio de retransmisión a través del enlace de PC5 seguro, tal como establecer una nueva sesión de unidad de datos de protocolo (PDU) o modificar una sesión de PDU existente para retransmisión, si es necesario, etc.

Cuando el retransmisor de UE a red de capa 3 de ProSe de 5G envía un informe de UE remoto a la función de gestión de sesión (SMF), el retransmisor de UE a red de capa 3 de ProSe de 5G puede incluir ID de usuario remoto recibido en la etapa 164d. Si el ID de PRUK usado como ID de usuario remoto no está en formato de NAI, el retransmisor de UE a red de capa 3 de ProSe de 5G puede incluir el ID de HPLMN del UE remoto de ProSe de 5G en el informe de UE remoto.

La figura 1C ilustra un procedimiento de establecimiento de seguridad de PC5 170 para comunicación de retransmisión de UE a red de ProSe de 5G a través de plano de control (CP). El procedimiento 170 puede implicar el UE

remoto 110, el retransmisor de UE a red 121, una función de gestión de acceso y movilidad (AMF) 171 del UE remoto 110, una AMF 172 del retransmisor 121, una función de servidor de autenticación (AUSF) 173 del UE remoto 110, la UDM 155 del UE remoto 110 y una función de anclaje de ProSe (PAnF) 174 del UE remoto
5 110.

El procedimiento 170 describe el procedimiento para establecer un enlace de PC5 entre el UE remoto de ProSe de 5G y el retransmisor de UE a red de ProSe de 5G. El procedimiento incluye cómo se autentica el UE remoto de ProSe de 5G por la AUSF del UE remoto de ProSe de 5G a través del retransmisor de
10 UE a red de ProSe de 5G y la AMF del retransmisor de UE a red de ProSe de 5G durante el establecimiento de PC5 de ProSe de 5G. Este mecanismo se puede usar cuando el UE remoto de ProSe de 5G está fuera de cobertura.

En 180, el UE remoto de ProSe de 5G y el retransmisor de UE a red de ProSe de 5G se pueden registrar con la red. El retransmisor de UE a red de ProSe de 5G se autentica y autoriza por la red para proporcionar el servicio de retransmisión de UE a red. El UE remoto de ProSe de 5G se autentica y autoriza
15 por la red para recibir el servicio de retransmisión de UE a red. Las políticas de seguridad de PC5 se aprovisionan al UE remoto de ProSe de 5G y al retransmisor de UE a red de ProSe de 5G respectivamente durante este
20 procedimiento de autorización y de aprovisionamiento de información.

En 181, el UE remoto de ProSe de 5G o UE de retransmisión puede iniciar un procedimiento de descubrimiento usando cualquiera del método del modelo A o del modelo B.

En 182, después del descubrimiento del retransmisor de UE a red de ProSe de 5G, el UE remoto de ProSe de 5G puede enviar una solicitud de
25 ProSe de 5G, el UE remoto de ProSe de 5G puede enviar una solicitud de

comunicación directa al retransmisor de UE a red de ProSe de 5G para establecer un enlace de unidifusión de PC5 seguro. El UE remoto de ProSe de 5G puede incluir sus capacidades de seguridad y política de seguridad de señalización de PC5 en el mensaje de DCR. El mensaje también puede incluir
5 código de servicio de retransmisión, Nonce_1.

Si el UE remoto de ProSe de 5G no tiene una clave de usuario remota de ProSe de 5G válida (CP-PRUK), el UE remoto de ProSe de 5G puede incluir SUCI en la DCR para desencadenar la autenticación específica de UE remoto de ProSe de 5G y establecer una CP-PRUK.

10 Si el UE remoto de ProSe de 5G ya tiene un CP-P válido para código de servicio de retransmisión, el UE remoto de ProSe de 5G puede incluir el ID de CP-PRUK asociado en la DCR para indicar que el UE remoto de ProSe de 5G desea obtener conectividad de retransmisión usando la CP-PRUK.

En 183, tras recibir el mensaje de DCR, el retransmisor de UE a red de ProSe de 5G puede enviar la solicitud de clave de retransmisión a la AMF del retransmisor de UE a red de ProSe de 5G, que incluye ID de SUCI o CP-PRUK, RSC y Nonce_1 recibidos en el mensaje de DCR. El retransmisor de UE a red de ProSe de 5G puede incluir también en el mensaje un identificador de transacción que identifica el UE remoto de ProSe de 5G para los mensajes posteriores a
15
20 través de mensajes de NAS del retransmisor de UE a red de ProSe de 5G.

En 184, la AMF del retransmisor de UE a red de ProSe de 5G puede verificar si el retransmisor de UE a red de ProSe de 5G está autorizado a proporcionar el servicio de retransmisión de UE a red.

En 185, la AMF del retransmisor de UE a red de ProSe de 5G puede
25 seleccionar una AUSF basándose en ID de SUCI o CP-PRUK y reenviar los

parámetros recibidos en solicitud de clave de retransmisión a la AUSF en el mensaje de solicitud Nausf_UEAuthentication_ProseAuthenticate. El mensaje de solicitud Nausf_UEAuthentication_ProseAuthenticate puede contener el SUCI o ID de CP-PRUK del UE remoto de ProSe de 5G, código de servicio de retransmisión, Nonce_1. Si se recibe el ID de CP-PRUK desde AMF del retransmisor de UE a red de ProSe de 5G, la AUSF del remoto de ProSe de 5G puede almacenar temporalmente Nonce_1 y el UE omite las etapas 186-189. Si la SUCI del UE remoto de ProSe de 5G se recibe desde la AMF del retransmisor de UE a red de ProSe de 5G, la AUSF del UE remoto de ProSe de 5G almacena temporalmente Nonce_1 y código de servicio de retransmisión y omite la etapa 190.

En 186, la AUSF puede iniciar una autenticación específica de UE remoto de ProSe de 5G usando los parámetros específicos de ProSe recibidos (es decir, RSC, etc.).

La AUSF del UE remoto de ProSe de 5G puede recuperar los vectores de autenticación y el indicador de encaminamiento del UE remoto de ProSe de 5G de la UDM a través del mensaje de solicitud de Nudm_UEAuthentication_GetProseAv. Tras la recepción de la solicitud de Nudm_UEAuthentication_GetProSeAv, la UDM puede invocar la SUCI de des-ocultación de SIDF para obtener SUPI antes de que la UDM pueda procesar la solicitud. La UDM comprueba si el UE está autorizado para usar un servicio de retransmisión de UE a red de ProSe basándose en información de autorización en los datos de suscripción del UE. Si el UE está autorizado, la UDM puede elegir el método de autenticación de acuerdo de clave y autenticación de protocolo de autenticación extensible (EAP-AKA) basándose en la solicitud de

Nudm_UEAuthentication_GetProseAv recibida.

En 187a, la AUSF puede almacenar temporalmente XRES, indicador de encaminamiento y SUPI. La AUSF del UE remoto de ProSe de 5G puede desencadenar la autenticación del UE remoto de ProSe de 5G basándose en EAP-AKA'. La AUSF del UE remoto de ProSe de 5G puede generar el mensaje de solicitud de EAP/desafío de AKA' y enviar un mensaje de solicitud de EAP/desafío de AKA' a la AMF del retransmisor de UE a red de ProSe de 5G en un mensaje de respuesta de Nausf_UEAuthentication_ProSeAuthenticate.

En 187b, la AMF del retransmisor de UE a red de ProSe de 5G puede reenviar la solicitud de autenticación de retransmisión (que incluye la solicitud de EAP/desafío de AKA') al retransmisor de UE a red de ProSe de 5G a través del mensaje de NAS, que incluye el identificador de transacción del UE remoto de ProSe de 5G en el mensaje. El mensaje de NAS se protege usando el contexto de seguridad de NAS creado para el retransmisor de UE a red de ProSe de 5G.

En 187c, basándose en el identificador de transacción, el retransmisor de UE a red de ProSe de 5G puede reenviar la solicitud de EAP/desafío de AKA' al UE remoto de ProSe de 5G a través de mensajes de PC5.

El USIM en el UE remoto de ProSe de 5G puede verificar la actualización de los valores recibidos comprobando si se puede aceptar AUTN.

Para EAP-AKA', el USIM calcula una respuesta RES. El USIM puede devolver RES, CK, IK a la ME. La ME puede derivar CK' e IK'.

En 187d, el UE remoto de ProSe de 5G puede devolver una respuesta de EAP/desafío de AKA' al retransmisor de UE a red de ProSe de 5G a través de mensajes de PC5.

En 187e, el retransmisor de UE a red de ProSe de 5G puede reenviar la

respuesta de EAP/desafío de AKA' junto con el identificador de transacción del UE remoto de ProSe de 5G a la AMF del retransmisor de UE a red de ProSe de 5G en una respuesta de autenticación de retransmisión de mensaje de NAS.

En 187f, la AMF del retransmisor de UE a red de ProSe de 5G puede reenviar la respuesta de EAP/desafío de AKA' a la AUSF del UE remoto de ProSe de 5G a través de la solicitud de Nausf_UEAuthentication_ProSeAuthenticate.

La AUSF del UE remoto de ProSe de 5G puede realizar la autenticación de UE verificando la información recibida.

Para EAP-AKA', la AUSF del UE remoto de ProSe de 5G y el UE remoto de ProSe de 5G pueden intercambiar mensajes de solicitud de EAP/notificación de AKA' y de respuesta de EAP/notificación de AKA' a través de la AMF del retransmisor de UE a red de ProSe de 5G y del retransmisor de UE a red de ProSe de 5G. Después de los intercambios, la AUSF del UE remoto de ProSe de 5G y el UE remoto de ProSe de 5G pueden derivar la KAUSF_P de la misma manera que se deriva la KAUSF.

En 188, en una autenticación satisfactoria, la AUSF del UE remoto de ProSe de 5G y el UE remoto de ProSe de 5G pueden generar CP-PRUK e ID de CP-PRUK.

El ID de CP-PRUK puede estar en formato de NAI, es decir, nombredeusuario@dominio. La parte de nombre de usuario incluye el indicador de encaminamiento de la etapa 186 y el ID de CP-PRUK, y la parte de dominio incluye el identificador de red doméstica.

En 189a, la AUSF del UE remoto de ProSe de 5G puede seleccionar la PANF basándose en ID de CP-PRUK y enviar la SUPI, RSC, CP-PRUK e ID de

CP-PRUK en el mensaje de solicitud de Npanf_ProseKey_Register a la PAnF.

En 189b, la PAnF puede almacenar la información de contexto de ProSe (es decir, SUPI, RSC, CP-PRUK, ID de CP-PRUK) para el UE remoto de ProSe de 5G y enviar el mensaje de respuesta Npanf_ProseKey_Register a la AUSF.

5 En 190a, la AUSF del UE remoto de ProSe de 5G puede seleccionar la PAnF basándose en el ID de CP-PRUK y enviar el ID de CP-PRUK recibido y el RSC en el mensaje de solicitud Npanf_ProseKey_get.

En 190b, la PAnF puede recuperar CP-PRUK basándose en el ID de CP-PRUK y comprueba si el UE remoto de ProSe de 5G está autorizado a usar
10 el servicio de retransmisión de UE a red basándose en el RSC recibido. Si el UE remoto de ProSe de 5G está autorizado y la CP-PRUK recuperada es válida, la PAnF envía el mensaje de respuesta de Npanf_ProseKey_get con CP-PRUK a la AUSF.

En 191, la AUSF del UE remoto de ProSe de 5G puede generar Nonce_2
15 y derivar la clave KNR_ProSe usando CP-PRUK, Nonce_1 y Nonce_2 como se define en la cláusula A.4.

En 192, la AUSF del UE remoto de ProSe de 5G puede enviar KNR_ProSe, Nonce_2 en el mensaje de respuesta de Nausf_UEAuthentication_ProseAuthenticate al retransmisor de UE a red de
20 ProSe de 5G a través de la AMF del retransmisor de UE a red de ProSe de 5G. El mensaje de éxito de EAP se puede incluir si la etapa 187 se realiza con éxito. La AUSF del UE remoto de ProSe de 5G se puede incluir también el ID de CP-PRUK en el mensaje.

En 193, cuando se recibe un KNR_ProSe desde la AUSF del UE remoto
25 de ProSe de 5G a través de la AMF del retransmisor de UE a red de ProSe de 5G,

el retransmisor de UE a red de ProSe de 5G puede derivar la clave de sesión PC5 Krelay-sess y la clave de confidencialidad Krelay-enc (si es aplicable) y la clave de integridad Krelay-int de KNR_ProSe. El ID de KNR_ProSe y el ID de Krelay-sess se establecen de la misma manera que el ID de KNRP y el ID de KNRP-sess. El ID de 5GPRUK se puede enviar desde la AMF del UE de ProSe de 5G al retransmisor de UE a red al retransmisor de UE a red. El mensaje de éxito de EAP se puede enviar también desde la AMF del retransmisor de UE a red de ProSe de 5G al retransmisor de UE a red si se recibe desde AUSF.

En 194, el retransmisor de UE a red de ProSe de 5G puede enviar el Nonce_2 recibido y la política de seguridad de señalización de PC5 del UE remoto de ProSe de 5G al UE remoto de ProSe de 5G en el mensaje de orden de modo de seguridad directo, que está protegido por integridad usando Krelay-int. El mensaje de éxito de EAP puede incluir si se recibe desde la AMF del retransmisor de UE a red de ProSe de 5G.

En 195, el UE remoto de ProSe de 5G puede generar la clave KNR_ProSe que se usará para acceso remoto a través del retransmisor de UE a red de 5G de la misma manera que se define en la etapa 191. El UE remoto de ProSe de 5G puede derivar la clave de sesión de PC5 Krelay-sess y las claves de confidencialidad e integridad de KNR_ProSe de la misma manera que se define en la etapa 193.

El UE remoto de ProSe de 5G puede verificar el mensaje de orden de modo de seguridad directo. La verificación satisfactoria del mensaje de orden de modo de seguridad directo garantiza al UE remoto de ProSe de 5G que el retransmisor de UE a red de ProSe de 5G está autorizado para proporcionar el servicio de retransmisión.

En 196, el UE remoto de ProSe de 5G puede enviar un mensaje de modo de seguridad directo completo que contiene sus políticas de seguridad de plano de usuario de PC5 al retransmisor de UE a red de ProSe de 5G, que está protegido por Krelay-int y/o Krelay-enc derivado de Krelay-sess de acuerdo con
5 las políticas de señalización de PC5 negociadas entre el UE remoto de ProSe de 5G y el retransmisor de UE a red de ProSe de 5G.

En 197, al recibir el mensaje de modo de seguridad directo completo, el retransmisor de UE a red de ProSe de 5G puede verificar el mensaje de modo de seguridad directo completo. La verificación satisfactoria del mensaje de modo de
10 seguridad directo completo garantiza al retransmisor de UE a red de ProSe de 5G que el UE remoto de ProSe de 5G está autorizado para obtener el servicio de retransmisión.

Después de la verificación satisfactoria del mensaje de modo de seguridad directo completo, el retransmisor de UE a red de ProSe de 5G puede
15 responder a un mensaje de aceptación de comunicación directa al UE remoto de ProSe de 5G para finalizar los procedimientos de establecimiento de conexión de PC5 y almacenar el ID de CP-PRUK en el contexto de seguridad asociado al enlace de PC5 con el UE remoto de ProSe de 5G.

La comunicación adicional entre el UE remoto de ProSe de 5G y la red
20 puede tener lugar de forma segura a través del retransmisor de UE a red de ProSe de 5G.

Cuando el retransmisor de UE a red de capa 3 de ProSe de 5G envía un informe de UE remoto a la SMF, el retransmisor de UE a red de capa 3 de ProSe de 5G puede incluir un ID de usuario remoto (es decir, el ID de 5GPRUK recibido
25 en la etapa 13) en el mensaje.

Como se describe, el UE remoto puede conmutar entre diferentes retransmisores de UE a Red (U2N), incluyendo conmutar entre retransmisores de U2N L3.

Además, se puede construir un enlace de seguridad entre el UE remoto y el retransmisor de U2N antes de que el UE remoto use el retransmisor para transmitir tráfico. Se puede realizar un procedimiento de seguridad para autenticar y autorizar al UE a usar el servicio de retransmisión de ProSe, y generar claves para proteger el enlace entre el UE remoto y el retransmisor U2N. 3GPP soporta dos modos de procedimientos de seguridad para autenticación y generación de claves para retransmisión L3, uno está basado en UP y otro está basado en CP.

Hay 6 posibles casos de uso. En algunos casos, se podría desencadenar la reautenticación basada en CP y la generación de claves, en algunos casos, se podría desencadenar la reautenticación basada en UP y la generación de claves, en algunos casos, no se desencadenará la reautenticación y se podría usar el mismo PRUK para derivar claves de comunicación. La Tabla 1 a continuación muestra casos de conmutación de trayectoria y si se puede desencadenar reautenticación y generación de claves para cada caso.

Tabla 1

Caso n.º 1	El UE de retransmisión inicial-UE remoto realizó L3-UP y durante la conmutación de trayectoria al nuevo UE de retransmisión, realiza L3-UP con el mismo RSC - sin reautenticación .
Caso n.º 2	El UE de retransmisión inicial-UE remoto realizó L3-UP y durante la conmutación de trayectoria al nuevo UE de retransmisión, realiza L3-UP con diferente RSC - sin reautenticación .

Caso n.º 3	El UE de retransmisión inicial-UE remoto realizó L3-UP y durante la conmutación de trayectoria al nuevo UE de retransmisión, realiza L3-CP con diferentes RSC - puede reautenticar si el contexto de seguridad para el RSC no es válido.
Caso n.º 4	El UE de retransmisión inicial-UE remoto realizó L3-CP y durante la conmutación de trayectoria al nuevo UE de retransmisión, realiza L3-CP con el mismo RSC - sin reautenticación.
Caso n.º 5	El UE de retransmisión inicial-UE remoto realizó L3-CP y durante la conmutación de trayectoria al nuevo UE de retransmisión, L3-CP con diferentes RSC - puede la reautenticación si el contexto de seguridad para el RSC no es válido.
Caso n.º 6	El UE de retransmisión inicial-UE remoto realizó L3-CP y durante la conmutación de trayectoria al nuevo UE de retransmisión, L3-UP con diferentes RSC - puede la reautenticación si el contexto de seguridad para el RSC no es válido.

Como se muestra en la tabla anterior, cuando un UE remoto conmuta a otro UE de retransmisión, puede desencadenar una nueva autenticación y la generación de PRUK, lo que puede costar tiempo y recursos, por lo tanto, puede

5 provocar la interrupción del servicio y afectar en la continuidad del servicio.

En algunas realizaciones, la presente divulgación propone una solución para optimizar el procedimiento de selección de retransmisor basándose en el indicador de seguridad de CP asociado con RSC. Por ejemplo, el UE remoto (es decir, dispositivo terminal remoto) puede seleccionar un RSC con contexto de

10 seguridad válido, por ejemplo, seleccionar RSC con indicación de seguridad de

CP si la CP-PRUK correspondiente es válida, e incluir ID de CP-PRUK en la DCR. En algunas realizaciones, el UE remoto puede seleccionar un RSC sin indicación de seguridad de CP si la UP-PRUK correspondiente es válida, e incluir el ID de UP-PRUK en la DCR. En algunas realizaciones, si tanto la CP-PRUK como la

5 UP-PRUK correspondientes al RSC son válidas, el UE remoto puede seleccionar el RSC con el mismo modo de CP/UP al RSC actual, e incluir el ID de CP/UP-PRUK en la DCR. En algunas realizaciones, si ni la CP-PRUK ni la UP-PRUK correspondientes al RSC son válidas, el UE remoto puede priorizar el RSC con el mismo modo de CP/UP al RSC actual, e incluir SUCI en la DCR. En

10 algunas realizaciones, el orden de prioridad se podría preconfigurar por HPLMN del UE remoto a través de procedimiento de autorización y aprovisionamiento o dependiente de implementación de UE.

La figura 2 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo 200 de selecciones de RSC de acuerdo con algunas

15 realizaciones de la presente divulgación. Para facilitar la comprensión, el proceso 200 puede implicar el UE remoto 110 (que también se puede denominar como el dispositivo terminal remoto) como se muestra en las figuras 1A-1C.

En el bloque 210, el UE remoto 110 obtiene una política de selección para seleccionar un RSC de una pluralidad de RSC. Un RSC de la pluralidad de RSC

20 está asociado con un indicador (por ejemplo, el indicador de seguridad de CP) para indicar si el RSC soporta un procedimiento de seguridad de CP o un procedimiento de seguridad de UP.

En el bloque 220, basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de

25 origen con un RSC de origen, el UE remoto 110 selecciona un RSC objetivo

basándose en la política de selección. Un indicador de origen está asociado con el RSC de origen, y una pluralidad de indicadores está asociada con la pluralidad de RSC. En el bloque 230, el UE remoto 110 selecciona, para la conmutación de trayectoria, un UE de retransmisión objetivo (es decir, un dispositivo terminal objetivo) basándose en el RSC objetivo.

En algunas realizaciones, el UE remoto 110 puede seleccionar el dispositivo terminal retransmisor objetivo con el RSC objetivo que es el mismo que el RSC de origen. En algunas realizaciones, el UE remoto 110 puede determinar la pluralidad de RSC y obtener la pluralidad de indicadores. Además, el UE remoto 110 puede determinar, basándose en el RSC de origen y la pluralidad de indicadores, si el RSC de origen y la pluralidad de RSC soportan el procedimiento de seguridad de CP o el procedimiento de seguridad de UP.

En algunas realizaciones, el UE remoto 110 puede seleccionar uno de la pluralidad de RSC para los que el dispositivo terminal remoto tiene una clave raíz válida como el RSC objetivo. En algunas realizaciones, basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de CP, el UE remoto 110 puede seleccionar, como el RSC objetivo, uno de la pluralidad de RSC para los que el dispositivo terminal remoto tiene la clave raíz válida y que soporta el procedimiento de seguridad de CP.

Como alternativa o además, basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de UP, el UE remoto 110 puede seleccionar, como el RSC objetivo, uno de la pluralidad de RSC para los que el dispositivo terminal remoto tiene la clave raíz válida y que soporta el procedimiento de seguridad de UP.

En algunas realizaciones, el UE remoto 110 puede generar un DCR que

incluye un ID de la clave raíz válida. La clave raíz válida se puede usar para generar al menos una clave de seguridad para establecer un enlace de seguridad para una comunicación directa entre el dispositivo terminal remoto y el dispositivo terminal retransmisor objetivo.

5 En algunas realizaciones, basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de CP, el UE remoto 110 puede seleccionar, como el RSC objetivo, uno del al menos un RSC candidato que soporta el procedimiento de seguridad de CP. Como alternativa o además, basándose en la determinación de que el RSC de origen soporta el
10 procedimiento de seguridad de UP, el UE remoto 110 puede seleccionar, como el RSC objetivo, uno de la pluralidad de RSC que soportan el procedimiento de seguridad de UP. Como alternativa o además, el UE remoto 110 puede seleccionar aleatoriamente uno de la pluralidad de RSC como el RSC objetivo.

 En algunas realizaciones, el UE remoto 110 puede generar una DCR que
15 incluye un SUCI usado para desencadenar un procedimiento de autenticación de ProSe del dispositivo terminal remoto.

 En algunas realizaciones, la política de selección puede comprender un orden de selección basándose en el procedimiento de seguridad de CP o el procedimiento de seguridad de UP que soportan el RSC de origen y el RSC
20 objetivo, y se puede basar además en la política de autenticación. Como alternativa o además, la política de selección puede comprender una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de ProSe. En algunas realizaciones, la política de selección y/o política de autenticación se pueden
25 preconfigurar por una HPLMN del UE remoto o basándose en una

implementación del UE remoto.

La figura 3 ilustra un diagrama de señalización de ejemplo que muestra un proceso de ejemplo 300 de selecciones de RSC de acuerdo con algunas realizaciones de la presente divulgación. El proceso de ejemplo 300 puede
5 implicar el UE remoto 110, los retransmisores 121 y 122, la AMF 171 del UE remoto 110 o la PKMF 152 del UE remoto 110 (denominada 201), la PKMF 154 del retransmisor 121, la PKMF 202 del retransmisor 122, una PCF 203 del UE remoto 110 y la AUSF 173 del UE remoto 110.

Como se muestra en la figura 3, en 310, el UE remoto 110 se puede
10 aprovisionar con una política de selección de RSC relacionada con indicador de CP (por ejemplo, un orden de prioridad de selección de RSC). Como alternativa o además, el UE remoto 110 se puede aprovisionar con políticas de reautenticación, etc.

En 311, el UE remoto 110 puede seleccionar el UE de retransmisión 121
15 para comunicación.

En 312, la conmutación de trayectoria se puede activar desde el UE retransmisor 121, por ejemplo, al UE de retransmisión 122.

En 313, el UE remoto 110 puede seleccionar el RSC y el correspondiente retransmisor basándose en un indicador de CP asociado con los RSC. Si el
20 orden de prioridad relacionado con el indicador de seguridad de CP está preconfigurado en el UE remoto, el UE debería seguir el orden requerido por la HPLMN para seleccionar RSC; de lo contrario, podría depender de la implementación del UE.

La figura 4 muestra un ejemplo 400 de selecciones de RSC basándose en
25 el indicador de CP. Como se muestra en la figura 4, después de desencadenarse

401 la conmutación de trayectoria, el UE remoto 110 puede determinar 402 si hay un retransmisor con el mismo RSC que el retransmisor actual (es decir, retransmisor de origen). Si se encuentra un retransmisor con el mismo RSC, el UE remoto 110 puede seleccionar 403 el retransmisor como el retransmisor objetivo para conmutación de trayectoria. Si no se encuentra ningún retransmisor con el mismo RSC, el UE remoto 110 puede seleccionar 404 RSC candidatos.

A continuación, el UE remoto 110 puede obtener 405 indicadores de seguridad de CP asociados con el RSC de origen y los RSC candidatos para decidir si los RSC soportan procedimiento de seguridad basado en CP o UP. Por ejemplo, si existe un indicador de seguridad de CP, puede representar que el RSC correspondiente soporta el procedimiento de seguridad basado en CP; de lo contrario, si el procedimiento de seguridad basado en CP o UP está ausente, puede representar que el RSC correspondiente soporta el procedimiento de seguridad basado en UP. Debe entenderse que el formato del indicador de seguridad de CP se describe únicamente para facilitar la comprensión sin sugerir ninguna limitación en cuanto al alcance de la divulgación, y el indicador de seguridad de CP se puede implementar en cualquier formato adecuado.

El UE remoto 110 puede determinar 406 si hay un RSC con PRUK válido y que soporta el mismo procedimiento de seguridad que el RSC de origen. Si se encuentra el RSC con PRUK válido y que soporta el mismo procedimiento de seguridad, el UE remoto 110 puede seleccionar el RSC como el RSC objetivo, usar 408 el RSC objetivo para seleccionar un retransmisor objetivo e incluir el ID de PRUK en la DCR. Si no se encuentra ningún RSC con PRUK válido y que soporte el mismo procedimiento de seguridad, el UE remoto 110 puede

determinar 407 si hay un RSC con PRUK válida. Si se encuentra un RSC con PRUK válida, el UE remoto 110 puede seleccionar el RSC como el RSC objetivo, usar 408 el RSC objetivo para seleccionar un retransmisor objetivo e incluir el ID de PRUK en la DCR.

- 5 Si no se encuentra ningún RSC con PRUK válido, el UE remoto 110 puede determinar 409 si hay un RSC que soporta el mismo procedimiento de seguridad que el RSC de origen. Si se encuentra el RSC que soporta el mismo procedimiento de seguridad, el UE remoto 110 puede seleccionar el RSC como el RSC objetivo, usar 410 el RSC objetivo para seleccionar un retransmisor
- 10 objetivo e incluir el SUCI en la DCR. Si no se encuentra ningún RSC que soporte el mismo procedimiento de seguridad, el UE remoto 110 puede seleccionar aleatoriamente un RSC de los RSC candidatos o basándose en una implementación del UE remoto. A continuación, el UE remoto 110 puede seleccionar el RSC seleccionado aleatoriamente como el RSC objetivo, usar 410
- 15 el RSC objetivo para seleccionar un retransmisor objetivo e incluir un SUCI en la DCR.

Debe entenderse que el diagrama de flujo 400 se da únicamente para facilitar la comprensión sin sugerir ninguna limitación, y la política de selección de RSC de la divulgación se puede implementar en cualquier orden adecuado.

- 20 Volviendo a la figura 3. En 314 (es decir, 314a-d), se pueden seguir los procedimientos para comunicación directa como se muestra en las figuras 1B y 1C. Por brevedad, los procedimientos no se repiten en este punto.

- De acuerdo con las realizaciones anteriores, la presente divulgación propone soluciones para optimizar el procedimiento de selección de
- 25 retransmisor basándose en el indicador de seguridad de CP asociado con el

RSC. Con las soluciones propuestas, se puede mejorar la continuidad del servicio después de la conmutación de trayectoria entre retransmisores de ProSe L3 y se pueden evitar retrasos o interrupciones en el servicio.

De acuerdo con otras realizaciones, la presente divulgación propone
5 además soluciones para optimizar el procedimiento de seguridad de CP y UP para reducir la reautenticación durante la conmutación de trayectoria, mientras aún se mantiene la actualización de la PRUK durante la movilidad del UE remoto. Por ejemplo, para ambos procedimientos basados en UP y CP, la reautenticación/autorización de ProSe y la regeneración de PRUK se pueden
10 desencadenar en los siguientes casos. En caso de que el UE remoto se mueva a una nueva PLMN, similar a la autenticación primaria, la reautenticación/autorización de ProSe y la regeneración de PRUK se pueden desencadenar por el UE remoto. En caso de que el UE remoto seleccione un retransmisor en una nueva PLMN, la reautenticación/autorización de ProSe y la
15 regeneración de PRUK se pueden desencadenar por el UE remoto. En caso de expiración de la PRUK, cambio de datos de suscripción, etc., la HPLMN puede desencadenar reautenticación. En algunas realizaciones, la reautenticación se puede no desencadenar, incluso para un procedimiento basado en CP, cuando el UE remoto conmuta a otro RSC.

20 En algunas realizaciones, se propone una política de reautenticación por la presente divulgación, y se usará la misma PRUK para un UE remoto independientemente del cambio de RSC. La reautenticación se podría determinar basándose en la política de reautenticación aprovisionada en el UE remoto a través del procedimiento de autorización y aprovisionamiento, o
25 dependiente de la implementación del UE.

La figura 5 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo 500 para optimizar procedimientos de seguridad de acuerdo con algunas realizaciones de la presente divulgación. Para facilitar la comprensión, el proceso 500 puede implicar el UE remoto 110 (que también se puede denominar como el dispositivo terminal remoto) como se muestra en las figuras 1A-1C.

En el bloque 510, el UE remoto 110 obtiene una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de ProSe. En el bloque 520, el UE remoto 110 determina desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

En algunas realizaciones, la política de autenticación se puede basar en la movilidad del dispositivo terminal remoto. En algunas realizaciones, el UE remoto 110 puede determinar desencadenar el procedimiento de autenticación de ProSe basándose en el dispositivo terminal remoto que se mueve a una nueva PLMN de servicio. En algunas realizaciones, el UE remoto 110 puede determinar desencadenar el procedimiento de autenticación de ProSe basándose en el dispositivo terminal remoto que selecciona un dispositivo terminal retransmisor en la nueva PLMN de servicio.

En algunas realizaciones, el UE remoto 110 puede determinar desencadenar el procedimiento de autenticación de ProSe basándose en que una clave raíz es no válida. La clave raíz se puede usar para generar al menos una clave de seguridad para establecer un enlace de seguridad para la comunicación directa entre el dispositivo terminal remoto y el dispositivo terminal retransmisor.

En algunas realizaciones, el procedimiento de autenticación de ProSe puede comprender un procedimiento de seguridad de CP. Además, el UE remoto 110 puede determinar desencadenar el procedimiento de autenticación de ProSe basándose en la política de autenticación independientemente del cambio de un RSC, siendo la generación de la clave raíz independiente del RSC.

La figura 6 ilustra un diagrama de flujo de ejemplo que muestra un proceso de ejemplo 600 para optimizar un procedimiento de seguridad de CP de acuerdo con algunas realizaciones de la presente divulgación. Para facilitar la comprensión, el proceso 600 puede implicar la AUSF 173 como se muestra en la figura 1C.

En el bloque 610, la AUSF 173 genera una clave raíz independiente de un RSC. La clave raíz se usa para generar al menos una clave de ProSe para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor. En el bloque 620, la AUSF 173 transmite, al dispositivo de PAnF 174, una solicitud de registro de clave de ProSe sin el RSC.

En algunas realizaciones, la AUSF 173 puede transmitir, al dispositivo de PAnF, una solicitud de obtención de clave de ProSe para desencadenar un procedimiento de autorización de servicio de retransmisión del dispositivo terminal remoto basándose en el RSC. En algunas realizaciones, la AUSF 173 puede generar la al menos clave de seguridad ProSe basándose al menos en el RSC. La al menos clave de seguridad ProSe puede ser específica de RSC. En algunas realizaciones, la clave raíz puede comprender una CP-PRUK.

La figura 7 ilustra un diagrama de señalización de ejemplo que muestra un procedimiento de seguridad de UP 700 optimizado de acuerdo con algunas

realizaciones de la presente divulgación. El procedimiento 700 puede implicar el UE remoto 110, el retransmisor de UE a red 121, la DDNMF de 5G 151 del UE remoto 110, la PKMF 152 del UE remoto 110, la DDNMF de 5G 153 del retransmisor 121, la PKMF 154 del retransmisor 121, y la UDM (o la BSF o el HSS) 155 del UE remoto 110.

Como se muestra en la figura 7, en 710a, el UE remoto 110 se puede aprovisionar con políticas de reautenticación, etc. En 710b-710d, el UE remoto 110 puede seguir los procedimientos como se muestra en la figura 1B para solicitud de PRUK, a continuación, descubrimiento y comunicación con un retransmisor de U2N de L3.

En 710e, el UE remoto 110 se puede mover a una nueva área. En 711, basándose en la disponibilidad de PRUK de UP y políticas de reautenticación preconfiguradas en el UE remoto, o implementación de UE, el UE remoto 110 puede desencadenar reautenticación. Por ejemplo, el UE remoto 110 puede desencadenar una reautenticación si el UE se mueve a una nueva PLMN de servicio, o la PRUK local es no válida (por ejemplo, ha expirado, está corrompida, etc.).

En 712a, si el UE remoto 110 está en área de cobertura, puede enviar solicitud de PRUK a HPLMN para obtener nueva clave, que puede desencadenar reautenticación/autorización y generación de PRUK. En 712b, si el UE remoto 110 no está en área de cobertura, incluye SUCI en la siguiente solicitud de DCR a un retransmisor de U2N, que puede desencadenar reautenticación/autorización y generación de PRUK.

El resto de procedimientos para el servicio de retransmisión pueden ser similares a los mostrados en la figura 1B, que no se repetirían en este punto.

La figura 8 ilustra un diagrama de señalización de ejemplo que muestra un procedimiento de seguridad de CP 800 optimizado de acuerdo con algunas realizaciones de la presente divulgación. El procedimiento 800 puede implicar el UE remoto 110, el retransmisor de UE a red 121, la AMF 171 del UE remoto 110, la AMF 172 del retransmisor 121, la AUSF 173 del UE remoto 110, la UDM 155 del UE remoto 110 y la PAnF 174 del UE remoto 110.

En 810, el UE remoto de ProSe de 5G y el retransmisor de UE a red de ProSe de 5G se pueden registrar con la red. El retransmisor de UE a red de ProSe de 5G se autentica y autoriza por la red para proporcionar el servicio de retransmisión de UE a red. El UE remoto de ProSe de 5G se autentica y autoriza por la red para recibir el servicio de retransmisión de UE a red. Las políticas de seguridad de PC5 se aprovisionan al UE remoto de ProSe de 5G y al retransmisor de UE a red de ProSe de 5G respectivamente durante este procedimiento de autorización y de aprovisionamiento de información.

Además, a diferencia del procedimiento que se muestra en la figura 1C, las políticas de reautenticación se aprovisionan al UE remoto de ProSe de 5G.

En 811, basándose en la disponibilidad de PRUK de CP y políticas de reautenticación preconfiguradas en el UE remoto, o implementación de UE, el UE remoto puede desencadenar autenticación/reautenticación de ProSe. Por ejemplo, el UE remoto puede desencadenar una reautenticación si el UE se mueve a una nueva PLMN de servicio, o la PRUK local es no válida (por ejemplo, ha expirado, está corrompida, etc.).

En 812, después del descubrimiento del retransmisor de UE a red de ProSe de 5G, el UE remoto de ProSe de 5G puede enviar una solicitud de comunicación directa al retransmisor de UE a red de ProSe de 5G para

establecer un enlace de unidifusión de PC5 seguro. El UE remoto de ProSe de 5G puede incluir sus capacidades de seguridad y política de seguridad de señalización de PC5 en el mensaje de DCR. El mensaje también puede incluir código de servicio de retransmisión, Nonce_1.

- 5 Si el UE remoto de ProSe de 5G no tiene una clave de usuario remota de ProSe de 5G válida (CP-PRUK) y es necesaria reautenticación, el UE remoto de ProSe de 5G puede incluir SUCI en la DCR para desencadenar la autenticación específica de UE remoto de ProSe de 5G y establecer una CP-PRUK.
- 10 Si el UE remoto de ProSe de 5G ya tiene un CP-P válido para el código de servicio de retransmisión y no es necesaria reautenticación, el UE remoto de ProSe de 5G puede incluir el ID de CP-PRUK en la DCR para indicar que el UE remoto de ProSe de 5G desea obtener conectividad de retransmisión usando la CP-PRUK.
- 15 Las etapas 813 y 814 son similares a las etapas 183 y 184 como se muestra en la figura 1C, que no se repetirían en este punto.

 En 815, la AMF del retransmisor de UE a red de ProSe de 5G puede seleccionar una AUSF basándose en ID de SUCI o CP-PRUK y reenviar los parámetros recibidos en solicitud de clave de retransmisión a la AUSF en el
20 mensaje de solicitud Nausf_UEAuthentication_ProseAuthenticate. El mensaje de solicitud Nausf_UEAuthentication_ProseAuthenticate puede contener el SUCI o ID de CP-PRUK del UE remoto de ProSe de 5G, código de servicio de retransmisión, Nonce_1. Si se recibe el ID de CP-PRUK desde AMF del retransmisor de UE a red de ProSe de 5G, la AUSF del remoto de ProSe de 5G
25 puede almacenar temporalmente Nonce_1 y el UE omite las etapas 186-189. Si

la SUCI del UE remoto de ProSe de 5G se recibe desde la AMF del retransmisor de UE a red de ProSe de 5G, la AUSF del UE remoto de ProSe de 5G almacena temporalmente Nonce_1 y código de servicio de retransmisión. A diferencia de la etapa 185 como se muestra en la figura 1C, la etapa 820 no se omitirá.

- 5 En 816, la AUSF puede iniciar una autenticación específica de UE remoto de ProSe de 5G sin usar los parámetros específicos de ProSe recibidos (es decir, RSC, etc.).

Las etapas 817a-818 son similares a las etapas 187a-188 como se muestra en la figura 1C, que no se repetirían en este punto.

- 10 En 819a, la AUSF del UE remoto de ProSe de 5G puede seleccionar la PAnF basándose en ID de CP-PRUK y enviar la SUPI, CP-PRUK e ID de CP-PRUK en el mensaje de solicitud de Npaf_ProseKey_Register a la PAnF. A diferencia de la etapa 189a como se muestra en la figura 1C, la AUSF del UE remoto de ProSe de 5G puede no enviar RSC en el mensaje de solicitud de
- 15 Npaf_ProseKey_Register a la PAnF.

- En 819b, la PAnF puede almacenar la información de contexto de ProSe (es decir, SUPI, CP-PRUK, ID de CP-PRUK) para el UE remoto de ProSe de 5G y enviar el mensaje de respuesta Npaf_ProseKey_Register a la AUSF. A diferencia de la etapa 189b como se muestra en la figura 1C, la AUSF del UE
- 20 remoto de ProSe de 5G puede almacenar la información de contexto de Prose sin RSC.

En 820a, la AUSF del UE remoto de ProSe de 5G puede seleccionar la PAnF basándose en el ID de CP-PRUK y enviar el ID de CP-PRUK recibido y el RSC en el mensaje de solicitud Npaf_ProseKey_get.

- 25 En 820b, la PAnF puede recuperar CP-PRUK basándose en el ID de

CP-PRUK y comprueba si el UE remoto de ProSe de 5G está autorizado a usar el servicio de retransmisión de UE a red basándose en el RSC recibido. Si el UE remoto de ProSe de 5G está autorizado y la CP-PRUK recuperada es válida, la PAnF envía el mensaje de respuesta de Npanf_ProseKey_get con CP-PRUK a la

5 AUSF.

En 821, la AUSF del UE remoto de ProSe de 5G puede generar Nonce_2 y derivar la clave K_{NR_ProSe} usando CP-PRUK, RSC, Nonce_1 y Nonce_2.

Las etapas 822-827 son similares a las etapas 192-197 como se muestra en la figura 1C, que no se repetirían en este punto.

10 En algunas realizaciones, un aparato capaz de realizar cualquiera del método 200 (por ejemplo, el UE remoto 110) puede comprender medios para realizar las etapas respectivas del método 200. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de software.

15 En algunas realizaciones, el aparato comprende: medios para obtener, en un dispositivo terminal remoto, una política de selección para seleccionar un código de selección de retransmisor (RSC) de una pluralidad de RSC, estando asociado un RSC de la pluralidad de RSC con un indicador para indicar si el RSC soporta un procedimiento de seguridad de plano de control (CP) o un

20 procedimiento de seguridad de plano de usuario (UP); medios para, basándose en la determinación de que se desencadena la conmutación de trayectoria desde un dispositivo terminal retransmisor de origen con un RSC de origen, seleccionar un RSC objetivo basándose en la política de selección, un indicador de origen asociado con el RSC de origen y una pluralidad de indicadores asociados con la

25 pluralidad de RSC; y medios para seleccionar, para la conmutación de

trayectoria, un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo.

En algunas realizaciones, los medios para seleccionar un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo comprenden
5 medios para: seleccionar el dispositivo terminal retransmisor objetivo con el RSC objetivo que es el mismo que el RSC de origen. En algunas realizaciones, el aparato comprende además medios para: determinar la pluralidad de RSC; obtener la pluralidad de indicadores; y determinar, basándose en el RSC de origen y la pluralidad de indicadores, si el RSC de origen y la pluralidad de RSC
10 soportan el procedimiento de seguridad de CP o el procedimiento de seguridad de UP.

En algunas realizaciones, los medios para seleccionar un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo comprenden medios para: seleccionar uno de la pluralidad de RSC para los que el dispositivo
15 terminal remoto tiene una clave raíz válida como el RSC objetivo. En algunas realizaciones, los medios para seleccionar un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo comprenden medios para: basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de CP, seleccionar, como el RSC objetivo, uno de la pluralidad de RSC para los
20 que el dispositivo terminal remoto tiene la clave raíz válida y soporta el procedimiento de seguridad de CP.

En algunas realizaciones, los medios para seleccionar un dispositivo terminal retransmisor objetivo basándose en el RSC objetivo comprenden medios para: basándose en la determinación de que el RSC de origen soporta el
25 procedimiento de seguridad de UP, seleccionar, como el RSC objetivo, uno de la

pluralidad de RSC para los que el dispositivo terminal remoto tiene la clave raíz válida y soporta el procedimiento de seguridad de UP.

En algunas realizaciones, el aparato comprende además medios para: generar una solicitud de comunicación directa (DCR) que incluye una identidad
5 (ID) de la clave raíz válida, usándose la clave raíz válida para generar al menos una clave de seguridad para establecer un enlace de seguridad para una comunicación directa entre el dispositivo terminal remoto y el dispositivo terminal retransmisor objetivo.

En algunas realizaciones, el aparato comprende además: medios para,
10 basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de CP, seleccionar, como el RSC objetivo, uno del al menos un RSC candidato que soporta el procedimiento de seguridad de CP; medios para, basándose en la determinación de que el RSC de origen soporta el procedimiento de seguridad de UP, seleccionar, como el RSC objetivo, uno de la
15 pluralidad de RSC que soportan el procedimiento de seguridad de UP; o medios para seleccionar aleatoriamente uno de la pluralidad de RSC como el RSC objetivo.

En algunas realizaciones, el aparato comprende además medios para: generar una DCR que incluye un identificador oculto de suscripción (SUCI)
20 usado para desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe) del dispositivo terminal remoto. En algunas realizaciones, la política de selección comprende al menos uno de: un orden de selección basado en el procedimiento de seguridad de CP o el procedimiento de seguridad de UP que soportan el RSC de origen y el RSC objetivo; o una política
25 de autenticación a usar por el dispositivo terminal remoto para determinar si

desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe). En algunas realizaciones, la política de selección está preconfigurada por una red móvil pública terrestre doméstica (HPLMN) del dispositivo terminal remoto o basándose en una implementación del dispositivo terminal remoto.

En algunas realizaciones, el aparato comprende además medios para realizar otras etapas en algunas realizaciones del método 200. En algunas realizaciones, los medios comprenden al menos un procesador y al menos una memoria que incluye código de programa informático, la al menos una memoria y el código de programa informático configurados para, con el al menos un procesador, provocar el funcionamiento del aparato.

En algunas realizaciones, un aparato capaz de realizar cualquiera del método 500 (por ejemplo, el UE remoto 110) puede comprender medios para realizar las etapas respectivas del método 500. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de software.

En algunas realizaciones, el aparato comprende: medios para obtener, en un dispositivo terminal remoto, una política de autenticación a usar por el dispositivo terminal remoto para determinar si desencadenar un procedimiento de autenticación de servicios basados en proximidad (ProSe); y medios para determinar desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación.

En algunas realizaciones, la política de autenticación se basa en la movilidad del dispositivo terminal remoto. En algunas realizaciones, los medios para determinar desencadenar el procedimiento de autenticación de ProSe

comprenden medios para: determinar desencadenar el procedimiento de autenticación de ProSe basándose en que el dispositivo terminal remoto se mueve a una nueva red móvil pública terrestre (PLMN) de servicio. En algunas realizaciones, los medios para determinar desencadenar el procedimiento de autenticación de ProSe comprenden medios para: determinar desencadenar el procedimiento de autenticación de ProSe basándose en que el dispositivo terminal remoto selecciona un dispositivo terminal retransmisor en la nueva PLMN de servicio.

En algunas realizaciones, los medios para determinar desencadenar el procedimiento de autenticación de ProSe comprenden medios para: determinar desencadenar el procedimiento de autenticación de ProSe basándose en que una clave raíz es no válida, en donde la clave raíz se usa para generar al menos una clave de seguridad para establecer un enlace de seguridad para la comunicación directa entre el dispositivo terminal remoto y el dispositivo terminal retransmisor.

En algunas realizaciones, el procedimiento de autenticación de ProSe comprende un procedimiento de seguridad de plano de control (CP). Además, los medios para determinar desencadenar el procedimiento de autenticación de ProSe al menos basándose en la política de autenticación comprenden medios para: determinar desencadenar el procedimiento de autenticación de ProSe basándose en la política de autenticación independientemente del cambio de un RSC, siendo la generación de la clave raíz independiente del RSC.

En algunas realizaciones, el aparato comprende además medios para realizar otras etapas en algunas realizaciones del método 500. En algunas realizaciones, los medios comprenden al menos un procesador y al menos una

memoria que incluye código de programa informático, la al menos una memoria y el código de programa informático configurados para, con el al menos un procesador, provocar el funcionamiento del aparato.

En algunas realizaciones, un aparato capaz de realizar cualquiera del
5 método 600 (por ejemplo, el dispositivo de AUSF 173) puede comprender medios para realizar las etapas respectivas del método 600. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de software.

En algunas realizaciones, el aparato comprende: medios para generar, en
10 un dispositivo de función de servidor de autenticación (AUSF), una clave raíz independiente de un código de selección de retransmisión (RSC), usándose la clave raíz para generar al menos una clave de servicio basado en proximidad (ProSe) para establecer un enlace de seguridad para una comunicación directa entre un dispositivo terminal remoto y un dispositivo terminal retransmisor; y
15 medios para transmitir, a un dispositivo de función de anclaje de ProSe (PAnF), una solicitud de registro de clave de ProSe sin el RSC.

En algunas realizaciones, el aparato comprende además medios para: transmitir, al dispositivo de PAnF, una solicitud de obtención de clave de ProSe para desencadenar un procedimiento de autorización de servicio de
20 retransmisión del dispositivo terminal remoto basándose en el RSC. En algunas realizaciones, el aparato comprende además medios para: generar la al menos clave de seguridad de ProSe basándose al menos en el RSC, siendo la al menos clave de seguridad de ProSe específica de RSC. En algunas realizaciones, la clave raíz comprende una clave de usuario remoto de ProSe de plano de control
25 (CP-PRUK).

En algunas realizaciones, el aparato comprende además medios para realizar otras etapas en algunas realizaciones del método 600. En algunas realizaciones, los medios comprenden al menos un procesador y al menos una memoria que incluye código de programa informático, la al menos una memoria y el código de programa informático configurados para, con el al menos un procesador, provocar el funcionamiento del aparato.

La figura 9 es un diagrama de bloques simplificado de un dispositivo 900 que es adecuado para implementar realizaciones de la presente divulgación. El dispositivo 900 se puede proporcionar para implementar el dispositivo de comunicación, por ejemplo, el UE remoto 110 y el dispositivo de AUSF 173. Como se muestra, el dispositivo 900 incluye uno o más procesadores 910, una o más memorias 920 acopladas al procesador 910 y uno o más módulos de comunicación (TX/RX) 940 acoplados al procesador 910.

Los uno o más módulos de comunicación 940 son para comunicaciones bidireccionales. Los uno o más módulos de comunicación 940 tienen al menos una antena para facilitar la comunicación. La interfaz de comunicación puede representar cualquier interfaz que es necesaria para la comunicación con otros elementos de red.

El procesador 910 puede ser de cualquier tipo adecuado para la red técnica local y puede incluir uno o más de los siguientes: ordenadores de propósito general, ordenadores de propósito especial, microprocesadores, procesadores de señales digitales (DSP) y procesadores basados en arquitectura de procesador de múltiples núcleos, como ejemplos no limitantes. El dispositivo 900 puede tener múltiples procesadores, tales como un chip de circuito integrado específico de la aplicación que es esclavo en el tiempo de un

reloj que sincroniza el procesador principal.

La memoria 920 puede incluir una o más memorias no volátiles y una o más memorias volátiles. Los ejemplos de las memorias no volátiles incluyen, pero sin limitación, una memoria de solo lectura (ROM) 924, una memoria de solo lectura programable eléctricamente (EPROM), una memoria flash, un disco duro, un disco compacto (CD), un disco de vídeo digital (DVD) y otro almacenamiento magnético y/o almacenamiento óptico. Los ejemplos de las memorias volátiles incluyen, pero sin limitación, una memoria de acceso aleatorio (RAM) 922 y otras memorias volátiles que no perdurarán en la duración de bajada de potencia.

Un programa informático 930 incluye instrucciones ejecutables por ordenador que son ejecutadas por el procesador 910 asociado. El programa 930 se puede almacenar en la ROM 920. El procesador 910 puede realizar cualquier acción y procesamiento adecuados cargando el programa 930 en la RAM 920.

Las realizaciones de la presente divulgación se pueden implementar por medio del programa 930 de modo que el dispositivo 900 puede realizar cualquier proceso de la divulgación como se ha analizado con referencia a las figuras 2 a 8. Las realizaciones de la presente divulgación también se pueden implementar por hardware o por una combinación de software y hardware.

En algunas realizaciones, el programa 930 puede estar contenido tangiblemente en un medio legible por ordenador que se puede incluir en el dispositivo 900 (tal como en la memoria 920) u otros dispositivos de almacenamiento que son accesibles por el dispositivo 900. El dispositivo 900 puede cargar el programa 930 desde el medio legible por ordenador en la RAM 922 para su ejecución. El medio legible por ordenador puede incluir cualquier

tipo de almacenamiento no volátil tangible, tal como ROM, EPROM, una memoria flash, un disco duro, CD, DVD y similares. La figura 10 muestra un ejemplo del medio legible por ordenador 1000 en forma de CD o DVD. El medio legible por ordenador tiene el programa 930 almacenado en el mismo.

5 En general, diversas realizaciones de la presente divulgación se pueden implementar en hardware o circuitos de propósito especial, software, lógica o cualquier combinación de los mismos. Algunos aspectos se pueden implementar en hardware, mientras que otros aspectos se pueden implementar en firmware o software que puede ser ejecutado por un controlador, microprocesador u otro
10 dispositivo informático. Aunque diversos aspectos de realizaciones de la presente divulgación se ilustran y se describen como diagramas de bloques, diagramas de flujo o usando algunas otras representaciones pictóricas, se ha de entender que el bloque, dispositivo, sistema, técnica o método descrito en el presente documento se puede implementar en, como ejemplos no limitantes,
15 hardware, software, firmware, circuitos o lógica de propósito especial, hardware o controlador de propósito general u otros dispositivos informáticos o alguna combinación de los mismos.

La presente divulgación también proporciona al menos un producto de programa informático almacenado tangiblemente en un medio de
20 almacenamiento legible por ordenador transitorio o no transitorio. El producto de programa informático incluye instrucciones ejecutables por ordenador, tal como las incluidas en módulos de programa, que se ejecutan en un dispositivo en un procesador real o virtual objetivo, para efectuar los métodos 200, 500 y 500 como se han descrito con referencia a las figuras 2, 5 y 6. En general, los
25 módulos de programa incluyen rutinas, programas, librerías, objetos, clases,

componentes, estructuras de datos o similares que realizan tareas particulares o implementan tipos de datos abstractos particulares. La funcionalidad de los módulos de programa se puede combinar o dividir entre módulos de programa según se desee en diversas realizaciones. Las instrucciones ejecutables por

5 máquina para módulos de programa se pueden ejecutar dentro de un dispositivo local o distribuido. En un dispositivo distribuido, los módulos de programa se pueden ubicar en medios de almacenamiento tanto locales como remotos.

El código de programa para llevar a cabo métodos de la presente divulgación se puede escribir en cualquier combinación de uno o más lenguajes

10 de programación. Este código de programa se puede proporcionar a un procesador o controlador de un ordenador de propósito general, ordenador de propósito especial u otro dispositivo de procesamiento de datos programable, de tal modo que el código de programa, cuando es ejecutado por el procesador o controlador, hace que se implementen las funciones/operaciones especificadas

15 en los diagramas de flujo y/o diagramas de bloques. El código de programa se puede ejecutar en su totalidad en una máquina, parcialmente en la máquina, como un paquete de software autónomo, parcialmente en la máquina y parcialmente en una máquina remota o en su totalidad en la máquina o servidor remoto.

20 En el contexto de la presente divulgación, las instrucciones o datos relacionados pueden ser portados por cualquier soporte adecuado para habilitar que el dispositivo, dispositivo o procesador realice diversos procesos y operaciones como se ha descrito anteriormente. Los ejemplos del soporte incluyen una señal, un medio legible por ordenador y similares.

25 El medio legible por ordenador puede ser un medio de señal legible por

ordenador o un medio de almacenamiento legible por ordenador. Un medio legible por ordenador puede incluir, pero sin limitación, un sistema, dispositivo o dispositivo electrónico, magnético, óptico, electromagnético, de infrarrojos o de semiconductores o cualquier combinación adecuada de los anteriores. Ejemplos

5 más específicos del medio de almacenamiento legible por ordenador incluirían una conexión eléctrica que tiene uno o más hilos, un disquete de ordenador portátil, un disco duro, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura borrrable y programable (EPROM o memoria flash), una fibra óptica, un disco compacto-memoria de solo

10 lectura (CD-ROM) portátil, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento magnético o cualquier combinación adecuada de los anteriores. La expresión "no transitorio", como se usa en el presente documento, es una limitación del propio medio (es decir, tangible, no una señal) en contraposición a una limitación en la persistencia del almacenamiento de

15 datos (por ejemplo, RAM frente a ROM).

Además, aunque se representan operaciones en un orden particular, esto no se debería entender como que requiere que, para lograr resultados deseables, tales operaciones se hayan de realizar en el orden particular mostrado o en orden secuencial, o que se hayan de realizar todas las operaciones ilustradas.

20 En ciertas circunstancias, la multitarea y el procesamiento paralelo pueden ser ventajosos. De forma similar, aunque varios detalles de implementación específicos están contenidos en los análisis anteriores, estos no se deberían interpretar como limitaciones al alcance de la presente divulgación, sino más bien como descripciones de características que pueden ser específicas de

25 realizaciones particulares. Ciertas características que se describen en el

contexto de realizaciones separadas también se pueden implementar en combinación en una única realización. A la inversa, diversas características que se describen en el contexto de una única realización también se pueden implementar en múltiples realizaciones de forma separada o en cualquier subcombinación adecuada.

Aunque la presente divulgación se ha descrito en lenguajes específicos de características estructurales y/o actos metodológicos, se ha de entender que la presente divulgación definida en las reivindicaciones adjuntas no se limita necesariamente a las características o actos específicos descritos anteriormente.

En su lugar, las características y actos específicos descritos anteriormente se divulgan como formas de ejemplo de implementación de las reivindicaciones.