

OBTENCIÓN DE INFORMACIÓN DE SEGURIDAD PARA DESCUBRIMIENTO DE RETRANSMISIÓN

CAMPO

- 5 Diversas realizaciones de ejemplo de la presente divulgación se refieren, en general, al campo de las telecomunicaciones y, en particular a dispositivos, métodos, aparato y medios de almacenamiento legibles por ordenador para obtener información de seguridad para descubrimiento de retransmisión.

ANTECEDENTES

- 10 El sistema de quinta generación (5G) soporta la característica de servicios basados en proximidad (ProSe). Las características de ProSe de 5G pueden comprender descubrimiento directo de ProSe de 5G, comunicación directa de ProSe de 5G y retransmisión de UE a red (U2N) de ProSe de 5G. En la característica de retransmisión de UE a red de ProSe de 5G, un equipo de
- 15 usuario (UE) remoto se puede conectar a una retransmisión de UE a red a través de una interfaz PC5 con comunicación directa de ProSe de 5G, y comunicarse con una red de datos a través de la retransmisión de UE a red y la red de 5G. Para realizar la comunicación directa de ProSe de 5G entre el UE remoto y la retransmisión de U2N, el UE remoto y la retransmisión de U2N
- 20 pueden realizar un procedimiento de descubrimiento directo de ProSe de 5G usando información de seguridad para descubrimiento de retransmisión.

SUMARIO

- En general, las realizaciones de ejemplo de la presente divulgación proporcionan una solución para obtener información de seguridad para
- 25 descubrimiento de retransmisión.

En un primer aspecto, se proporciona un primer dispositivo de red en una primera red móvil pública terrestre doméstica (HPLMN). El primer dispositivo de red comprende al menos un procesador y al menos una memoria que almacena instrucciones. Cuando las instrucciones son ejecutadas por el al menos un

5 procesador, las instrucciones hacen que el primer dispositivo de red al menos: reciba, desde un dispositivo terminal atendido por el primer dispositivo de red, una primera solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la primera solicitud un código de servicio de retransmisión (RSC); obtenga al menos una identidad basándose en

10 la primera solicitud, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; obtenga al menos un conjunto de información de seguridad basándose en la al menos una identidad y el RSC, estando asociado cada uno del al menos un conjunto de información de seguridad con uno del al menos un

15 grupo de dispositivos terminales de retransmisión objetivo; y transmita el al menos un conjunto de información de seguridad al dispositivo terminal.

En un segundo aspecto, se proporciona un dispositivo terminal. El dispositivo terminal comprende al menos un procesador y al menos una memoria que almacena instrucciones. Cuando las instrucciones son ejecutadas

20 por el al menos un procesador, las instrucciones hacen que el dispositivo terminal al menos: transmita, a un dispositivo de red en una red móvil pública terrestre doméstica (HPLMN), una solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la solicitud un código de servicio de retransmisión (RSC); reciba al menos un conjunto de

25 información de seguridad desde el dispositivo de red, estando asociado cada

uno del al menos un conjunto de información de seguridad con uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; y realice el descubrimiento de retransmisión basándose en el al menos un conjunto de información de seguridad.

5 En un tercer aspecto, se proporciona un primer dispositivo de función de control de políticas (PCF) en una primera red móvil pública terrestre doméstica (HPLMN). El primer dispositivo de PCF comprende al menos un procesador y al menos una memoria que almacena instrucciones. Cuando las instrucciones son
10 ejecutadas por el al menos un procesador, las instrucciones hacen que el primer dispositivo de PCF al menos: reciba, desde un primer dispositivo de red en la primera HPLMN, una segunda solicitud de al menos una identidad, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan un código de servicio de retransmisión (RSC), comprendiendo al menos la segunda solicitud el RSC;
15 obtenga la al menos una identidad basándose en la segunda solicitud; y transmita, al primer dispositivo de red, una segunda respuesta a la segunda solicitud, comprendiendo al menos la segunda respuesta la al menos una identidad.

 En un cuarto aspecto, se proporciona un segundo dispositivo de red en
20 una segunda red móvil pública terrestre doméstica (HPLMN). El segundo dispositivo de red comprende al menos un procesador y al menos una memoria que almacena instrucciones. Cuando las instrucciones son ejecutadas por el al menos un procesador, las instrucciones hacen que el segundo dispositivo de red al menos: reciba, desde un primer dispositivo de red en una primera HPLM,
25 una tercera solicitud de al menos un segundo conjunto de información de

seguridad para un código de servicio de retransmisión (RSC), comprendiendo al menos la solicitud el RSC, siendo la segunda HPLMN diferente de la primera HPLMN; obtenga el al menos un segundo conjunto de información de seguridad basándose en la tercera solicitud; y transmita una tercera respuesta al primer
5 dispositivo de red, comprendiendo al menos la tercera respuesta el al menos un segundo conjunto de información de seguridad.

En un quinto aspecto, se proporciona un segundo dispositivo de función de control de políticas (PCF) en una segunda red móvil pública terrestre doméstica (HPLMN). El segundo dispositivo de PCF comprende al menos un
10 procesador y al menos una memoria que almacena instrucciones. Cuando las instrucciones son ejecutadas por el al menos un procesador, las instrucciones hacen que el segundo dispositivo de PCF al menos: reciba una solicitud de al menos una identidad, siendo cada una de la al menos una identidad para un dispositivo terminal de retransmisión objetivo que soporta un código de servicio
15 de retransmisión (RSC), comprendiendo al menos la solicitud el RSC; obtenga la al menos una identidad basándose en la solicitud; y transmita una respuesta a la solicitud, comprendiendo la respuesta la al menos una identidad.

En un sexto aspecto, se proporciona un aparato. El aparato comprende: medios para recibir, en un primer dispositivo de red en una primera red móvil pública terrestre doméstica (HPLMN) desde un dispositivo terminal atendido por
20 el primer dispositivo de red, una primera solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la primera solicitud un código de servicio de retransmisión (RSC); medios para obtener al menos una identidad basándose en la primera solicitud, siendo cada una de la
25 al menos una identidad para uno de al menos un grupo de dispositivos

terminales de retransmisión objetivo que soportan el RSC; medios para obtener al menos un conjunto de información de seguridad basándose en la al menos una identidad y el RSC, estando asociado cada uno del al menos un conjunto de información de seguridad con uno del al menos un grupo de dispositivos terminales de retransmisión objetivo; y medios para transmitir el al menos un conjunto de información de seguridad al dispositivo terminal.

En un séptimo aspecto, se proporciona un aparato. El aparato comprende: medios para transmitir, desde un dispositivo terminal a un dispositivo de red en una red móvil pública terrestre doméstica (HPLMN), una solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la solicitud un código de servicio de retransmisión (RSC); medios para recibir al menos un conjunto de información de seguridad desde el dispositivo de red, estando asociado cada uno del al menos un conjunto de información de seguridad con uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; y medios para realizar el descubrimiento de retransmisión basándose en el al menos un conjunto de información de seguridad.

En un octavo aspecto, se proporciona un aparato. El aparato comprende: medios para recibir, en un primer dispositivo de función de control de políticas (PCF) en una primera red móvil pública terrestre doméstica (HPLMN) desde un primer dispositivo de red en la primera HPLMN, una segunda solicitud de al menos una identidad, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan un código de servicio de retransmisión (RSC), comprendiendo al menos la segunda solicitud el RSC; medios para obtener la al menos una

identidad basándose en la segunda solicitud; y medios para transmitir, al primer dispositivo de red, una segunda respuesta a la segunda solicitud, comprendiendo al menos la segunda respuesta la al menos una identidad.

En un noveno aspecto, se proporciona un aparato. El aparato comprende:

5 medios para recibir, en un segundo dispositivo de red en una segunda red móvil pública terrestre doméstica (HPLMN) desde un primer dispositivo de red en una primera HPLM, una tercera solicitud de al menos un segundo conjunto de información de seguridad para un código de servicio de retransmisión (RSC), comprendiendo al menos la solicitud el RSC, siendo la segunda HPLMN

10 diferente de la primera HPLMN; medios para obtener el al menos un segundo conjunto de información de seguridad basándose en la tercera solicitud; y medios para transmitir una tercera respuesta al primer dispositivo de red, comprendiendo al menos la tercera respuesta el al menos un segundo conjunto de información de seguridad.

15 En un décimo aspecto, se proporciona un aparato. El aparato comprende: medios para recibir, en un segundo dispositivo de PCF en una segunda red móvil pública terrestre doméstica (HPLMN), una solicitud de al menos una identidad, siendo cada una de la al menos una identidad para un dispositivo terminal de retransmisión objetivo que soporta un código de servicio de

20 retransmisión (RSC), comprendiendo al menos la solicitud el RSC; medios para obtener la al menos una identidad basándose en la solicitud; y medios para transmitir una respuesta a la solicitud, comprendiendo la respuesta la al menos una identidad.

En un undécimo aspecto, se proporciona un método. El método

25 comprende: recibir, en un primer dispositivo de red en una primera red móvil

pública terrestre doméstica (HPLMN) desde un dispositivo terminal atendido por el primer dispositivo de red, una primera solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la primera solicitud un código de servicio de retransmisión (RSC); obtener al menos una
5 identidad basándose en la primera solicitud, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; obtener al menos un conjunto de información de seguridad basándose en la al menos una identidad y el RSC, estando asociado cada uno del al menos un conjunto de información de
10 seguridad con uno del al menos un grupo de dispositivos terminales de retransmisión objetivo; y transmitir el al menos un conjunto de información de seguridad al dispositivo terminal.

En un duodécimo aspecto, se proporciona un método. El método comprende: transmitir, desde un dispositivo terminal a un dispositivo de red en
15 una red móvil pública terrestre doméstica (HPLMN), una solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la solicitud un código de servicio de retransmisión (RSC); recibir al menos un conjunto de información de seguridad desde el dispositivo de red, estando asociado cada uno del al menos un conjunto de información de seguridad con
20 uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; y realizar el descubrimiento de retransmisión basándose en el al menos un conjunto de información de seguridad.

En un decimotercer aspecto, se proporciona un método. El método comprende: recibir, en un primer dispositivo de función de control de políticas
25 (PCF) en una primera red móvil pública terrestre doméstica (HPLMN) desde un

primer dispositivo de red en la primera HPLMN, una segunda solicitud de al menos una identidad, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan un código de servicio de retransmisión (RSC), comprendiendo al menos la segunda solicitud el RSC; obtener la al menos una identidad basándose en la segunda solicitud; y transmitir, al primer dispositivo de red, una segunda respuesta a la segunda solicitud, comprendiendo al menos la segunda respuesta la al menos una identidad.

En un decimocuarto aspecto, se proporciona un método. El método comprende: recibir, en un segundo dispositivo de red en una segunda red móvil pública terrestre doméstica (HPLMN) desde un primer dispositivo de red en una primera HPLM, una tercera solicitud de al menos un segundo conjunto de información de seguridad para un código de servicio de retransmisión (RSC), comprendiendo al menos la solicitud el RSC, siendo la segunda HPLMN diferente de la primera HPLMN; obtener el al menos un segundo conjunto de información de seguridad basándose en la tercera solicitud; y transmitir una tercera respuesta al primer dispositivo de red, comprendiendo al menos la tercera respuesta el al menos un segundo conjunto de información de seguridad.

En un decimoquinto aspecto, se proporciona un método. El método comprende: recibir, en un segundo dispositivo de PCF en una segunda red móvil pública terrestre doméstica (HPLMN), una solicitud de al menos una identidad, siendo cada una de la al menos una identidad para un dispositivo terminal de retransmisión objetivo que soporta un código de servicio de retransmisión (RSC), comprendiendo al menos la solicitud el RSC; obtener la al

menos una identidad basándose en la solicitud; y transmitir una respuesta a la solicitud, comprendiendo la respuesta la al menos una identidad.

En un decimosexto aspecto, se proporciona un medio legible por ordenador. El medio legible por ordenador comprende instrucciones de programa que, cuando son ejecutadas por al menos un procesador, hacen que un aparato realice al menos el método de acuerdo con cualquiera del undécimo al decimoquinto aspectos.

Se ha de entender que la sección de sumario no pretende identificar características clave o esenciales de las realizaciones de ejemplo de la presente divulgación, ni se pretende que se use para limitar el alcance de la presente divulgación. Otras características de la presente divulgación se volverán fácilmente comprensibles a través de la siguiente descripción.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Algunas realizaciones de ejemplo se describirán a continuación con referencia a los dibujos adjuntos, en los que:

la figura 1 ilustra una red de comunicación de ejemplo en la que se pueden implementar realizaciones de ejemplo de la presente divulgación;

la figura 2 ilustra un gráfico de señalización que ilustra un procedimiento de seguridad para el Modelo A de descubrimiento directo de ProSe de 5G restringido;

la figura 3 ilustra un gráfico de señalización que 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;

la figura 4 ilustra un gráfico de señalización que ilustra un proceso para obtener información de seguridad para descubrimiento de retransmisión de

acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 5 ilustra un gráfico de señalización que ilustra un proceso para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas otras realizaciones de ejemplo de la presente divulgación;

5 la figura 6 ilustra un gráfico de señalización que ilustra un proceso para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas otras realizaciones de ejemplo de la presente divulgación;

la figura 7 ilustra un gráfico de señalización que ilustra una implementación de ejemplo de un proceso para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 8 ilustra un gráfico de señalización que ilustra una implementación de ejemplo de un proceso para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas otras realizaciones de ejemplo de la presente divulgación;

la figura 9 ilustra un gráfico de señalización que ilustra una implementación de ejemplo de un proceso para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas otras realizaciones de ejemplo de la presente divulgación;

20 la figura 10 ilustra un gráfico de señalización que ilustra una implementación de ejemplo de un proceso para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con otras realizaciones de ejemplo más de la presente divulgación;

la figura 11 ilustra un gráfico de señalización que ilustra una implementación de ejemplo de un proceso para obtener información de

25

seguridad para descubrimiento de retransmisión de acuerdo con aún otras realizaciones de ejemplo de la presente divulgación;

la figura 12 ilustra un diagrama de flujo de un método implementando en un primer dispositivo de red de acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 13 ilustra un diagrama de flujo de un método implementando en un dispositivo terminal de acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 14 ilustra un diagrama de flujo de un método implementando en un primer dispositivo de función de control de políticas (PCF) de acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 15 ilustra un diagrama de flujo de un método implementando en un segundo dispositivo de red de acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 16 ilustra un diagrama de flujo de un método implementando en un segundo dispositivo de PCF de acuerdo con algunas realizaciones de ejemplo de la presente divulgación;

la figura 17 ilustra un diagrama de bloques simplificado de un aparato que es adecuado para implementar realizaciones de ejemplo de la presente divulgación; y

la figura 18 ilustra un diagrama de bloques de un medio legible por ordenador de ejemplo de acuerdo con algunas realizaciones de ejemplo de la presente divulgación.

En todos los dibujos, los mismos números de referencia, o unos similares, 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 de ejemplo se describen solo para fines de ilustración y para
5 ayudar a 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
10 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
15 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
20 del conocimiento de un experto en la materia afectar a tal rasgo, estructura o característica en conexión con otras realizaciones de ejemplo, 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,
25 estos elementos no deberían estar limitados por estos términos. Estos términos

se usan solo para distinguir un elemento de otro. Por ejemplo, un primer elemento se podría denominar segundo elemento y, de forma similar, un segundo elemento se podría denominar primer elemento, sin apartarse del alcance de las realizaciones de ejemplo. 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 describir realizaciones de ejemplo 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 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 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

5 (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.

10 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 implementación de meramente un circuito de hardware o procesador (o múltiples procesadores) o una porción de un circuito de hardware o procesador
15 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 circuito integrado similar en servidor, un dispositivo de red celular u otro dispositivo informático o de red.

20 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 Plazo (LTE), LTE Avanzada (LTE-A), Acceso Múltiple por División de Código de Banda Ancha (WCDMA), Acceso por Paquetes de Alta Velocidad (HSPA),
25 Internet de las Cosas de Banda Estrecha (NB-IoT) y así sucesivamente.

Además, las comunicaciones entre un dispositivo terminal y un dispositivo de red en la red de comunicación se pueden realizar de acuerdo con cualquier protocolo de comunicación de generación adecuado, incluyendo, pero sin limitación, los protocolos de comunicación de la primera generación (1G), la
5 segunda generación (2G), 2.5G, 2.75G, la tercera generación (3G), la cuarta generación (4G), 4.5G, nueva radio (NR) de la quinta generación (5G), y/o cualquier otro protocolo o bien conocido en la actualidad o bien que se vaya a desarrollar en el futuro. Las realizaciones de ejemplo de la presente divulgación se pueden aplicar en diversos sistemas de comunicación. Dado el rápido
10 desarrollo en las comunicaciones, 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.

Como se usa en el presente documento, la expresión "dispositivo de red"
15 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), 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
20 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 centralizada, que aloja RRC, SDAP y PDCP) que controla una
25 pluralidad de gNB-DU (unidad distribuida, que aloja RLC, MAC y PHY).

La expresión "dispositivo terminal" se refiere a cualquier dispositivo de extremo que pueda ser capaz de una comunicación inalámbrica. A modo de ejemplo en lugar de limitación, un dispositivo terminal también se puede denominar dispositivo de comunicación, equipo de usuario (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 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 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 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 similares. En la siguiente descripción, se pueden usar de forma intercambiable las expresiones "dispositivo terminal", "dispositivo de comunicación", "terminal", "equipo de usuario" y "UE".

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

5 ordenador de tipo tableta u ordenador portátil u ordenador de sobremesa o dispositivo de IoT móvil o dispositivo de IoT fijo). Este aparato de equipo de usuario puede, por ejemplo, estar equipado con capacidades correspondientes como se describe en conexión con el/los nodo(s) de red fijo(s) y/o inalámbrico(s), según sea apropiado. El aparato de equipo de usuario puede ser el equipo de

10 usuario y/o un dispositivo de control, 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 dotando, al aparato de equipo de usuario, de

15 software configurado para hacer que el aparato de equipo de usuario funcione desde el punto de vista de estas funciones/nodos.

La figura 1 muestra un entorno de comunicación 100 de ejemplo en el que se pueden implementar realizaciones de ejemplo de la presente divulgación. El entorno 100 puede comprender una primera red móvil pública terrestre

20 doméstica (HPLMN) 110 y una segunda HPLMN 120.

Un primer dispositivo terminal 112 puede usar un abono de la primera HPLMN 110. El primer dispositivo terminal 112 se puede comunicar con un primer dispositivo de red 114 y una primera PCF 116 en la primera HPLMN 110.

En algunas realizaciones de ejemplo, el primer dispositivo de red 114

25 puede comprender un dispositivo de función de gestión de nombres de

descubrimiento directo (DDNMF) de 5G, o un dispositivo de función de gestión de claves de ProSe (PKMF).

Un segundo dispositivo terminal 122 puede usar un abono de la segunda HPLMN 120. El segundo dispositivo terminal 122 se puede comunicar con un
5 segundo dispositivo de red 124 y una segunda PCF 126 en la segunda HPLMN 120.

En algunas realizaciones de ejemplo, el segundo dispositivo de red 124 puede comprender un dispositivo de función de gestión de nombres de descubrimiento directo (DDNMF) de 5G, o un dispositivo de función de gestión
10 de claves de ProSe (PKMF).

Se ha de entender que el número de dispositivos es solo 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 implementar realizaciones de la presente divulgación.

15 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
20 (5G) o de la sexta generación (6G) futura, 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 vaya a desarrollar en el futuro. Además, la comunicación puede utilizar cualquier tecnología de comunicación inalámbrica apropiada,
25 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
5 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.

En algunas realizaciones de ejemplo, el entorno de comunicación 100 puede soportar la característica de servicios basados en proximidad (ProSe), tal
10 como ProSe de 5G, ProSe de 4G y así sucesivamente. En lo sucesivo en el presente documento, se describirán realizaciones de ejemplo de la presente divulgación tomando ProSe de 5G como ejemplo. Sin embargo, la presente divulgación puede ser aplicable a ProSe de 4G o cualquier ProSe futuro.

Las características de ProSe de 5G pueden comprender descubrimiento
15 directo de ProSe de 5G, comunicación directa de ProSe de 5G y retransmisión de UE a red (U2N) de ProSe de 5G.

En la característica de retransmisión de UE a red de ProSe de 5G, el primer dispositivo terminal 112 se puede conectar al segundo dispositivo terminal 122 a través de una interfaz PC5 con comunicación directa de ProSe
20 de 5G, y comunicarse con una red de datos a través del segundo dispositivo terminal 122 y la red de 5G. A este respecto, el primer dispositivo terminal 112 se puede denominar dispositivo terminal remoto o equipo de usuario (UE) remoto, y el segundo dispositivo terminal 122 se puede denominar retransmisión de UE a red (U2N).

25 Para realizar la comunicación directa de ProSe de 5G entre el primer

dispositivo terminal 112 y el segundo dispositivo terminal 122, el primer dispositivo terminal 112 y el segundo dispositivo terminal 122 pueden realizar un procedimiento de descubrimiento directo de ProSe de 5G usando información de seguridad para descubrimiento de retransmisión. Por lo tanto, existe una
5 necesidad de obtener la información de seguridad para descubrimiento de retransmisión.

La figura 2 ilustra un gráfico de señalización que ilustra un procedimiento de seguridad 200 para el Modelo A de descubrimiento directo de ProSe de 5G restringido.

10 En el procedimiento 200, las etapas 211-214 se refieren a un UE de anuncio 202.

En 211, el UE de anuncio 202 envía un mensaje de solicitud de descubrimiento que contiene el ID de usuario de aplicación de ProSe restringida (RPAUID) a la DDNMF de 5G 205 en su HPLMN para conseguir el código de
15 ProSe para anunciar y conseguir el material de seguridad asociado. Además, el UE de anuncio 202 deberá incluir su capacidad de seguridad de UE de PC5 que contiene la lista de algoritmos de cifrado soportados por el UE en el mensaje de solicitud de descubrimiento.

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, la
20 retransmisión de UE a red de ProSe de 5G desempeña el papel del UE de anuncio 202 y envía una solicitud de clave de descubrimiento de retransmisión en lugar de una solicitud de descubrimiento. El mensaje de solicitud de clave de descubrimiento de retransmisión incluye el código de servicio de retransmisión (RSC) y la capacidad de seguridad de PC5 de la retransmisión de UE a red de
25 ProSe de 5G.

En 212, la DDNMF de 5G 205 puede comprobar la autorización de anuncio con el servidor de aplicación de ProSe. Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se omite esta etapa.

En 213, si el UE de anuncio 202 está en itinerancia, las DDNMF de 5G 205 en la HPLMN y la VPLMN 204 del UE de anuncio 202 intercambian Autenticación de Anuncio.

En 214, la DDNMF de 5G 205 en la HPLMN del UE de anuncio 202 devuelve el código restringido de ProSe y los parámetros de seguridad de envío de código correspondientes, junto con los parámetros TIEMPO_ACTUAL y DESPLAZAMIENTO_MÁX. Los parámetros de seguridad de envío de código proporcionan la información necesaria para que el UE de anuncio 202 proteja la transmisión del código restringido de ProSe y se almacenan con el código restringido de ProSe. El UE de anuncio 202 emprende las mismas acciones con TIEMPO_ACTUAL y DESPLAZAMIENTO_MÁX. La DDNMF de 5G 205 en la HPLMN del UE de anuncio 202 deberá incluir el algoritmo de cifrado de PC5 elegido en el mensaje de respuesta de descubrimiento. La DDNMF de 5G 205 determina el algoritmo de cifrado de PC5 elegido basándose en el código restringido de ProSe y la capacidad de seguridad de UE de PC5 recibida en la etapa 211. El UE almacena el algoritmo de cifrado de PC5 elegido junto con el código restringido de ProSe.

Además, la DDNMF de 5G 205 en la HPLMN del UE de anuncio 202 puede asociar el código restringido de ProSe con las políticas de seguridad de PC5 e incluir las políticas de seguridad de PC5 en el mensaje de respuesta de descubrimiento.

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se

usa una respuesta de clave de descubrimiento de retransmisión en lugar de la respuesta de descubrimiento, y se usa el RSC en lugar del código restringido de ProSe. El mensaje de respuesta contiene los materiales de seguridad de descubrimiento.

- 5 Se deberá hacer notar que la DDNMF de 5G puede conseguir las políticas de seguridad de PC5 de diferentes formas (por ejemplo, desde la PCF, desde el servidor de aplicación de ProSe o basándose en la configuración local).

Las etapas 215-220 se refieren a un UE de monitorización 201.

- 10 En 215, el UE de monitorización 201 envía un mensaje de solicitud de descubrimiento que contiene el RPAUID y su capacidad de seguridad de UE de PC5 a la DDNMF de 5G 203 en su HPLMN para que se le permita monitorizar en busca de uno o más ID de usuario de aplicación de ProSe restringida.

- 15 Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, el UE remoto de ProSe de 5G desempeña el papel del UE de monitorización 201 y envía una solicitud de clave de descubrimiento de retransmisión en lugar de la solicitud de descubrimiento. El mensaje de solicitud de clave de descubrimiento de retransmisión incluye el RSC y la capacidad de seguridad de PC5 del UE remoto de ProSe de 5G.

- 20 En 216, la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 envía una solicitud de autorización al servidor de aplicación de ProSe. Si, basándose en los ajustes de permiso, se permite que el RPAUID descubra al menos uno de los RPAUID objetivo contenidos en el contenedor de nivel de aplicación, el servidor de aplicación de ProSe devuelve una respuesta de
25 autorización.

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se omite esta etapa.

En 217, si se autoriza la solicitud de descubrimiento, y el ID de PLMN en el RPAUID objetivo indica una PLMN diferente, la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 entra en contacto con la DDNMF de 5G de la PLMN indicada (es decir, la DDNMF de 5G en la HPLMN del UE de anuncio 202) enviando un mensaje de solicitud de clave de descubrimiento que incluye la capacidad de seguridad de UE de PC5 recibida en la etapa 215.

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se usan solicitud de clave de descubrimiento de retransmisión y RSC en lugar de solicitud de descubrimiento y RPAUID.

En 218, la DDNMF de 5G 205 en la HPLMN del UE de anuncio 202 puede intercambiar mensajes de autorización con el servidor de aplicación de ProSe 206.

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se omite esta etapa.

En 219, si la capacidad de seguridad de UE de PC5 en la etapa 5 incluye el algoritmo de cifrado de PC5 elegido, la DDNMF de 5G 205 en la HPLMN del UE de anuncio 202 responde a la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 con una respuesta de clave de descubrimiento mensaje que incluye el código restringido de ProSe, los parámetros de seguridad de recepción de código correspondientes, una clave de integridad de usuario de descubrimiento (DUIK) opcional y el algoritmo de cifrado de PC5 elegido (basándose en la información/claves almacenadas en la etapa 214). Los parámetros de seguridad de recepción de código proporcionan la información

que necesita el UE de monitorización 201 para deshacer la protección aplicada por el UE de anuncio 202. La DUIK se deberá incluir como un parámetro separado si los parámetros de seguridad de recepción de código indican que el UE de monitorización 201 usa informes de coincidencia para comprobación de MIC. La DDNMF de 5G 203 en la HPLMN del UE de monitorización 201
5 almacena el código restringido de ProSe y la clave de integridad de usuario de descubrimiento (si esta recibió una fuera de los parámetros de seguridad de recepción de código).

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se
10 usa una respuesta de clave de descubrimiento de retransmisión en lugar de la respuesta de descubrimiento, y se usa el RSC en lugar del código restringido de ProSe. El mensaje de respuesta contiene los materiales de seguridad de descubrimiento.

La DDNMF de 5G 205 en la HPLMN del UE de anuncio 202 puede enviar
15 las políticas de seguridad de PC5 asociadas con el código restringido de ProSe a la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201.

Se deberá hacer notar que hay dos posibles configuraciones para la comprobación de integridad, en concreto, MIC comprobada por la DDNMF de 5G 203 del UE de monitorización 201, y MIC comprobada en el lado del UE de
20 monitorización 201. Qué configuración usar es decidido por la DDNMF de 5G, que asigna el código de ProSe Restringido monitorizado y señala el UE de monitorización 201 en los parámetros de seguridad de recepción de código.

Se deberá hacer notar que el algoritmo de cifrado de PC5 elegido está asociado con el código restringido de ProSe.

25 En 220, la DDNMF de 5G 203 en la HPLMN del UE de monitorización

201 devuelve el filtro de descubrimiento y los parámetros de seguridad de recepción de código, junto con los parámetros TIEMPO_ACTUAL y DESPLAZAMIENTO_MÁX y el algoritmo de cifrado de PC5 elegido. El UE de monitorización 201 emprende las mismas acciones con TIEMPO_ACTUAL y
5 DESPLAZAMIENTO_MÁX. El UE almacena el filtro de descubrimiento, los parámetros de seguridad de recepción de código y el algoritmo de cifrado de PC5 elegido junto con el código restringido de ProSe.

Si la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 recibe las políticas de seguridad de PC5 asociadas con el código restringido de
10 ProSe en la etapa 219, la DDNMF de 5G del UE de monitorización 201 reenvía las políticas de seguridad de PC5 al UE de monitorización 201.

Las etapas 11 y 12 tienen lugar a través de PC5.

En 221, el UE empieza a anunciar, si el contador basado en UTC proporcionado por el sistema asociado con la ranura de descubrimiento está
15 dentro del DESPLAZAMIENTO_MÁX del reloj de ProSe del UE de anuncio 202 y si no ha expirado el temporizador de validez. El UE forma el mensaje de descubrimiento y lo protege. Los cuatro bits menos significativos del contador basado en UTC se transmiten junto con el mensaje de descubrimiento protegido.

20 En 222, el UE de monitorización 201 escucha en busca de un mensaje de descubrimiento que satisface su filtro de descubrimiento si el contador basado en UTC asociado con esa ranura de descubrimiento está dentro del DESPLAZAMIENTO_MÁX del reloj de ProSe del UE de monitorización. Para hallar un mensaje coincidente de este tipo, este procesa el mensaje. Si no se
25 pidió al UE de monitorización 201 que enviara informes de coincidencia para

comprobación de MIC, se detiene en esta etapa desde una perspectiva de seguridad. De lo contrario, este procede a la etapa 223.

Se deberá hacer notar que el UE que comprueba la integridad del mensaje de descubrimiento por sí mismo no evita que el UE envíe un informe de
5 coincidencia debido a los requisitos en la TS 23.304. Si se envía un informe de coincidencia de este tipo, entonces no hay ninguna funcionalidad de seguridad implicada.

Las etapas 13-16 se refieren a un UE de monitorización 201 que ha encontrado una coincidencia.

10 En 223, o bien si el UE no ha hecho que la DDNMF de 5G compruebe en la MIC el código restringido de ProSe descubierto, previamente, o bien si la DDNMF de 5G ha comprobado en una MIC el código restringido de ProSe y ha expirado el temporizador de renovación de informe de coincidencia asociado (véase la etapa 225 para obtener detalles de este temporizador), o según se
15 requiera basándose en el procedimiento especificado en la TS 23.304, entonces el UE de monitorización 201 envía un mensaje de informe de coincidencia a la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201. El informe de coincidencia contiene el valor de contador basado en UTC con los cuatro bits menos significativos iguales a los cuatro bits menos significativos recibidos junto
20 con el mensaje de descubrimiento y más cercano al contador basado en UTC del UE de monitorización 201 asociado con la ranura de descubrimiento en donde este escuchó el anuncio, y otros parámetros de mensaje de descubrimiento que incluyen el código restringido de ProSe y MIC. La DDNMF de 5G comprueba la MIC.

25 En 224, la DDNMF de 5G 203 en la HPLMN del UE de monitorización

201 puede intercambiar una solicitud de autenticación/respuesta de autenticación con el servidor de aplicación de ProSe 206 para asegurar que el UE de monitorización 201 está autorizado a descubrir el UE de anuncio 202.

Para el descubrimiento de retransmisión de UE a red de ProSe de 5G, se omite esta etapa.

En 225, la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 devuelve al UE de monitorización 201 un acuse de recibo de que se ha pasado la comprobación de integridad. Este también proporciona el parámetro TIEMPO_ACTUAL, mediante el cual el UE (r)establece su reloj de ProSe. La DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 incluyó el temporizador de renovación de informe de coincidencia en el mensaje al UE de monitorización 201. El temporizador de renovación de informe de coincidencia indica cuánto tiempo esperará el UE antes de enviar un nuevo informe de coincidencia para el código restringido de ProSe.

En 226, la DDNMF de 5G 203 en la HPLMN del UE de monitorización 201 puede enviar un mensaje de información de informe de coincidencia a la DDNMF de 5G 205 en la HPLMN del UE de anuncio 202.

La figura 3 ilustra un gráfico de señalización que ilustra un procedimiento de establecimiento de seguridad de PC5 300 para comunicación de retransmisión de UE a red de ProSe de 5G a través de plano de usuario.

El UE remoto de ProSe de 5G 301 se aprovisiona con los materiales de seguridad de descubrimiento y la clave de usuario remota de ProSe (UP-PRUK) cuando está en cobertura. Estos materiales de seguridad están 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 necesita conectarse a la PKMF de 5G y obtener unos nuevos para usar los servicios de retransmisión de UE a red de ProSe de 5G.

Se deberá hacer notar que 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 de la retransmisión de UE a red de ProSe de 5G. Si tanto el UE remoto de ProSe de 5G como la retransmisión de UE a red de ProSe de 5G son atendidos por una única PKMF de 5G, la PKMF de 5G asume el papel de la PKMF de 5G del UE remoto de ProSe de 5G y la PKMF de 5G de la retransmisión de UE a red de ProSe de 5G y los intercambios de mensajes de PKMF inter 5G no son necesarios.

Las etapas 310a, 310b, 311a, 311b se realizan cuando el UE remoto de ProSe de 5G 301 está en cobertura.

En 310a, el UE remoto de ProSe de 5G 301 consigue la dirección de PKMF de 5G desde la DDNMF de 5G 303 de su HPLMN. Como alternativa, el UE remoto de ProSe de 5G 301 puede ser aprovisionado con la dirección de PKMF de 5G por PCF. Si el UE remoto de ProSe de 5G 301 se aprovisiona con la dirección de PKMF de 5G, el UE remoto de ProSe de 5G 301 puede acceder a la PKMF de 5G directamente sin solicitar la misma desde la DDNMF de 5G. En caso de que el UE remoto de ProSe de 5G 310 no pueda acceder a la PKMF de 5G usando la dirección de PKMF de 5G aprovisionada, el UE remoto de ProSe de 5G 301 puede solicitar la dirección de PMKF de 5G a la DDNMF de 5G.

En 310b, el UE remoto de ProSe de 5G 301 deberá establecer una conexión segura con la PKMF de 5G 304 a través de punto de referencia de PC8. La seguridad para la interfaz PC8 se basa en la seguridad de Ua si se usa

GBA especificado en la TS 33.220 (véase la cláusula 5.2.3.4) o la seguridad de Ua* si se usa AKMA especificado en la TS 33.535 (véase la cláusula 5.2.5.4). La PKMF de 5G 304 del UE remoto de ProSe de 5G 301 deberá comprobar si el UE remoto de ProSe de 5G 301 está autorizado a recibir el servicio de retransmisión de UE a red, y si el UE está autorizado, la PKMF de 5G 304 del UE remoto de ProSe de 5G 301 proporciona los materiales de seguridad de descubrimiento al UE remoto de ProSe de 5G 301. Si el UE remoto de ProSe de 5G 301 proporciona una lista de redes visitadas, la PKMF de 5G 304 del UE remoto de ProSe de 5G 301 deberá solicitar los materiales de seguridad de descubrimiento de las PKMF de 5G de las retransmisiones de UE a red de ProSe de 5G potenciales desde los que el UE remoto de ProSe de 5G 301 consigue los servicios de retransmisión. La PKMF de 5G de la retransmisión de UE a red de ProSe de 5G puede incluir las políticas de seguridad de PC5 para el UE remoto de ProSe de 5G 301.

Se deberá hacer notar que la PKMF de 5G se puede configurar localmente con la información de autorización del UE. De lo contrario, la PKMF de 5G interacciona con la UDM del UE para recuperar la información de autorización del UE.

Se deberá hacer notar que el UE remoto de ProSe de 5G 301 es provisionado por PCF con una lista de las redes visitadas potenciales para el servicio de retransmisión de UE a red de ProSe de 5G (que es identificado por RSC).

En 310c, la retransmisión de UE a red de ProSe de 5G 302 consigue la dirección de PKMF de 5G desde su HPLMN de la misma forma que se describe en la etapa 310a.

En 310d, la retransmisión de UE a red de ProSe de 5G 302 deberá establecer una conexión segura con la PKMF de 5G a través de punto de referencia de PC8 como en la etapa 310b. La PKMF de 5G 306 de la retransmisión de UE a red de ProSe de 5G 302 deberá comprobar si la retransmisión de UE a red de ProSe de 5G 302 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 306 de la retransmisión de UE a red de ProSe de 5G 302 proporciona los materiales de seguridad de descubrimiento a la retransmisión de UE a red de ProSe de 5G 302. La PKMF de 5G 306 de la retransmisión de UE a red de ProSe de 5G 302 puede incluir las políticas de seguridad de PC5 para la retransmisión de UE a red de ProSe de 5G 302.

En 311a, el UE remoto de ProSe de 5G 301 envía un mensaje de solicitud de PRUK a su PKMF de 5G. El mensaje indica que el UE remoto de ProSe de 5G 301 está solicitando una UP-PRUK desde la PKMF de 5G. Si el UE remoto de ProSe de 5G 301 ya tiene una UP-PRUK desde esta PKMF de 5G, el mensaje deberá contener también el ID de UP-PRUK de la UP-PRUK.

El ID de UP-PRUK deberá adoptar la forma o bien del formato de NAI o bien de la cadena de 64 bits. Si el ID de UP-PRUK está en formato de NAI, es decir, nombre de usuario@reino, la parte de reino deberá incluir Identificador de red doméstica (es decir, ID de HPLMN). La parte de nombre de usuario deberá incluir la cadena de 64 bits.

En 311b, la PKMF de 5G 304 comprueba si el UE remoto de ProSe de 5G 301 está autorizado a recibir servicios de retransmisión de UE a red. Esto se hace usando la identidad del UE Remoto de ProSe de 5G 301 asociada con la clave usada para establecer la conexión segura entre el UE Remoto de ProSe

de 5G 301 y la PKMF de 5G en la etapa 310b. Si el UE remoto de ProSe de 5G 301 está autorizado a recibir el servicio, la PKMF de 5G envía una UP-PRUK y un ID de UP-PRUK al UE remoto de ProSe de 5G 301. Si se incluyen UP-PRUK y ID de UP-PRUK, el UE remoto de ProSe de 5G 301 deberá almacenar estos y
 5 borrar cualquiera previamente almacenado para esta PKMF de 5G.

En 312, el procedimiento de descubrimiento se realiza entre el UE Remoto de ProSe de 5G 301 y la retransmisión de UE a red de ProSe de 5G 302 usando los parámetros de descubrimiento y el material de seguridad de descubrimiento.

10 Con las etapas 313 - 315, se establece una comunicación directa segura entre el UE remoto de ProSe de 5G 301 y la retransmisión de U2N.

En lo sucesivo en el presente documento, se describirá la autorización y aprovisionamiento para servicio ProSe.

En general, en 5GS, los parámetros para servicio de descubrimiento
 15 directo de ProSe de 5G, comunicación directa de ProSe de 5G y retransmisión de UE a red de ProSe de 5G se pueden poner a disposición del UE de las siguientes formas:

- aprovisionados en la ME; o
- configurados en la UICC; o
- 20 - aprovisionados en la ME y configurados en la UICC; o
- proporcionados o actualizados por el servidor de aplicación de ProSe a través de PCF y/o punto de referencia de PC1; o
- proporcionados o actualizados por la PCF al UE.

Si los mismos parámetros descritos en las cláusulas 5.1.2.1, 5.1.3.1 y
 25 5.1.4.1 son proporcionados por diferentes fuentes, el UE deberá considerar

estos en el siguiente orden de prioridad:

- proporcionados o actualizados por la PCF (incluyendo parámetros determinados por la propia PCF y parámetros proporcionados por el servidor de aplicación de ProSe a la PCF);
- 5 - proporcionados o actualizados por el servidor de aplicación de ProSe a través de punto de referencia de PC1;
- configurados en la UICC;
- aprovisionados en la ME.

Los parámetros proporcionados o actualizados por el servidor de aplicación de ProSe a través de punto de referencia de PC1 pueden necesitar complementarse con datos de configuración desde otras fuentes enumeradas anteriormente.

Se deberá hacer notar que el servidor de aplicación de ProSe puede aprovisionar los mismos parámetros de ProSe a través de 5GC o directamente al UE a través de punto de referencia de PC1, y puede revocar (por ejemplo, borrar) los parámetros de ProSe a través de 5GC para que el aprovisionamiento a través de punto de referencia de PC1 tome efecto.

Los principios básicos de autorización y aprovisionamiento de servicio para descubrimiento directo de ProSe de 5G, comunicación directa de ProSe de 5G y retransmisión de UE a red de ProSe de 5G son como sigue:

- La PCF en la HPLMN puede configurar una lista de PLMN en donde el UE está autorizado a usar descubrimiento directo de ProSe de 5G.
- La PCF en la HPLMN puede configurar una lista de PLMN en donde el UE está autorizado a usar comunicación directa de ProSe de

5G.

- 5 - La PCF en la HPLMN puede configurar una lista de PLMN en donde el UE está autorizado a actuar como retransmisión de UE a red de ProSe de 5G. Las autorizaciones para retransmisión de UE a red de capa 2 de ProSe de 5G y retransmisión de UE a red de capa 3 de ProSe de 5G son independientes entre sí.
- 10 - La PCF en la HPLMN puede configurar una lista de PLMN en donde el UE está autorizado a acceder a 5GC a través de retransmisión de UE a red de ProSe de 5G (es decir, a actuar como UE remoto de ProSe de 5G). Las autorizaciones para acceder a través de retransmisión de UE a red de capa 2 de ProSe de 5G y a través de retransmisión de UE a red de capa 3 de ProSe de 5G son independientes entre sí.
- 15 - La PCF en la HPLMN fusiona información de autorización a partir de PLMN domésticas y otras y proporciona al UE la información de autorización definitiva.
- 20 - La PCF en la red móvil pública terrestre visitada (VPLMN) o la HPLMN puede revocar la autorización (a través de H-PCF cuando se está en itinerancia) en cualquier momento usando el procedimiento de actualización de configuración de UE para el procedimiento de entrega de política de UE transparente definido en la cláusula 4.2.4.3 de la TS 23.502.
- 25 - El aprovisionamiento de política/parámetros de ProSe al UE es controlado por la PCF y puede ser desencadenado por el UE. La PCF aprovisiona uno o más de la política/parámetros de ProSe siguientes:

- Política/parámetros de ProSe para descubrimiento directo de ProSe de 5G como se especifica en la cláusula 5.1.2.1;
- Política/parámetros de ProSe para comunicaciones directas de ProSe de 5G como se especifica en la cláusula 5.1.3.1;
- 5 - Política/parámetros de ProSe para retransmisión de UE a red de capa 2 y/o capa 3 de ProSe de 5G como se especifica en la cláusula 5.1.4.1;
- Política/parámetros de ProSe para UE remoto de capa 2 y/o capa 3 de ProSe de 5G como se especifica en la cláusula 5.1.4.1.
- 10 - La PCF incluye la política/parámetros de ProSe de 5G en una sección de política identificada por un identificador de sección de política (PSI) como se especifica en la cláusula 6.1.2.2.2 de la TS 23.503 [9].

Además de lo anterior, la configuración de informe de uso de ProSe y las
 15 reglas para la tarificación se pueden (pre)configurar en el UE o ser proporcionadas por la PCF.

Además de lo anterior, la política de selección de trayectoria se puede (pre)configurar en el UE o puede ser proporcionada por la PCF como se define en la cláusula 5.11. Una preferencia de trayectoria para servicios ProSe puede
 20 ser proporcionada por el servidor de aplicación de ProSe a UDR, y puede ser usada por PCF para generación y actualización de política de selección de trayectoria.

Cuando un UE remoto de capa 3 de ProSe de 5G está usando una retransmisión de UE a red de capa 3 de ProSe de 5G sin implicar una función de
 25 interfuncionamiento de acceso no de 3GPP (N3IWF), no se soportan el

aprovisionamiento basado en PCF y la actualización de política/parámetros de ProSe de 5G al UE remoto de capa 3 de ProSe de 5G.

Basándose en la información de antecedentes, hay dos problemas en el procedimiento de seguridad para el descubrimiento directo de ProSe de 5G restringido, especialmente para descubrimiento de retransmisión de UE a red de ProSe de 5G.

Por un lado, la DDNMF/PKMF del UE remoto no puede localizar o descubrir la DDNMF/PKMF de una retransmisión potencial si el UE remoto y la retransmisión potencial pertenecen a diferentes HPLMN por la razón que se analiza a continuación.

De acuerdo con el descubrimiento de DDNMF de 5G en la sección 4.3.2.2 de la TS 23.304, una DDNMF de 5G en una HPLMN usa una función de repositorio de red (NRF) para descubrir otras DDNMF de 5G en otras PLMN. Basándose en la sección 6.3.1 de la TS 23.501, la NRF de una PLMN de origen alcanza la NRF en la PLMN remota usando un ID de PLMN objetivo. Sin embargo, la DDNMF de 5G del UE remoto no tiene información de ID de HPLMN de al menos una retransmisión objetivo o potencial.

A partir de la descripción sobre "autorización y aprovisionamiento para servicio ProSe", solo VPLMN o PLMN de servicio posibles del UE remoto se aprovisionan en el UE remoto, y el UE remoto puede informar estas PLMN a su DDNMF en solicitud de clave de descubrimiento como se muestra en 310b de la figura 3. Sin embargo, esas PLMN son VPLMN o PLMN de servicio posibles del UE remoto, que podrían ser definitivamente diferentes de la HPLMN de las retransmisiones. Por lo tanto, existe una laguna obvia en la especificación actual si el UE remoto y el UE de retransmisión pertenecen a diferentes HPLMN, y

especialmente el UE remoto o el UE de retransmisión está en itinerancia.

En concreto, en 217 de la figura 2, la DDNMF del UE remoto no puede localizar o descubrir la DDNMF de al menos una retransmisión potencial debido a que esta no conoce el ID de HPLMN de todas las retransmisiones potenciales.

5 Por otro lado, el procedimiento de descubrimiento de seguridad no puede funcionar para el caso de retransmisión de U2N si el RSC asociado al descubrimiento es soportado/autorizado por/para más de una retransmisión de U2N potencial de al menos diferentes HPLMN

Basándose en el procedimiento de descubrimiento actual, especialmente
10 en 219 y 220 de la figura 2, los parámetros de seguridad y el algoritmo de cifrado están asociados con el RSC. Si hay más de una retransmisión de U2N potencial que soporta el RSC, los parámetros de seguridad y los algoritmos de cifrado no se pueden distinguir a menos que todas las retransmisiones compartan unos mismos parámetros y algoritmos de seguridad. Como se usan
15 parámetros de seguridad y algoritmos de cifrado para proteger un mensaje de descubrimiento intercambiado a través de un enlace de PC5, no es seguro o ni siquiera es factible compartir los mismos entre todas las retransmisiones potenciales, o al menos entre las retransmisiones que pertenecen a diferentes HPLMN.

20 La presente divulgación proporciona una solución para obtener información de seguridad para descubrimiento de retransmisión. De acuerdo con la solución, un primer dispositivo de red en una primera HPLMN recibe, desde un dispositivo terminal atendido por el primer dispositivo de red, una primera solicitud de información de seguridad para descubrimiento de
25 retransmisión. La primera solicitud comprende al menos un código de servicio

de retransmisión (RSC). El primer dispositivo de red obtiene al menos una identidad basándose en la primera solicitud. Cada una de la al menos una identidad es para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC. A su vez, el primer dispositivo de red obtiene al menos un conjunto de información de seguridad basándose en la al menos una información de identidad. Cada uno del al menos un conjunto de información de seguridad está asociado con uno del al menos un grupo de dispositivos terminales de retransmisión objetivo. El primer dispositivo de red transmite el al menos un conjunto de información de seguridad al dispositivo terminal. De esta forma, el primer dispositivo de red puede descubrir una DDNMF objetivo y diferenciar información de seguridad para diferentes grupos de dispositivos terminales de retransmisión objetivo.

En lo sucesivo en el presente documento, el principio de la presente divulgación se describirán con referencia a las figuras 4 a 18.

La figura 4 ilustra un gráfico de señalización que ilustra un proceso 400 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el proceso 400 se describirá con referencia a la figura 1. El proceso 400 puede implicar al primer dispositivo terminal 112 y el primer dispositivo de red 114 en la figura 1. Como alternativa, el proceso 400 puede implicar al segundo dispositivo terminal 122 y el segundo dispositivo terminal 124 en la figura 1. En lo sucesivo en el presente documento, el proceso 400 se describirá tomando el primer dispositivo terminal 112 y el primer dispositivo de red 114, por ejemplo.

Como se muestra en la figura 4, el primer dispositivo terminal 112

transmite 410, al primer dispositivo de red 114, una primera solicitud de información de seguridad para descubrimiento de retransmisión. La primera solicitud comprende al menos un código de servicio de retransmisión (RSC).

En consecuencia, el primer dispositivo de red 114 recibe, desde el primer
5 dispositivo terminal 112, la primera solicitud de información de seguridad para descubrimiento de retransmisión.

El primer dispositivo de red 114 obtiene 420 al menos una identidad basándose en la primera solicitud. Cada una de la al menos una identidad es para uno de al menos un grupo de dispositivos terminales de retransmisión
10 objetivo que soportan el RSC. En lo sucesivo en el presente documento, un dispositivo terminal de retransmisión objetivo también se denomina como uno de los siguientes: un UE de retransmisión objetivo, una retransmisión objetivo, un dispositivo terminal de retransmisión potencial, un UE de retransmisión potencial o una retransmisión potencial.

A su vez, el primer dispositivo de red 114 obtiene 430 al menos un
15 conjunto de información de seguridad basándose en la al menos una información de identidad. Cada uno del al menos un conjunto de información de seguridad está asociado con uno del al menos un grupo de dispositivos terminales de retransmisión objetivo.

El primer dispositivo de red 114 transmite 450 el al menos un conjunto de
20 información de seguridad al primer dispositivo terminal 112.

En consecuencia, el primer dispositivo terminal 112 recibe el al menos un conjunto de información de seguridad desde el primer dispositivo de red 114.

A su vez, el primer dispositivo terminal 112 realiza 460 el descubrimiento
25 de retransmisión basándose en el al menos un conjunto de información de

seguridad.

Con el proceso 400, el primer dispositivo de red 114 puede descubrir una DDNMF objetivo y diferenciar información de seguridad para diferentes grupos de dispositivos terminales de retransmisión objetivo.

- 5 En algunas realizaciones de ejemplo, el primer dispositivo de red 114 puede obtener un conjunto de información de seguridad asociada con una identidad (ID) restringida de retransmisión. El ID restringido de retransmisión se puede generar basándose en el RSC y una identidad para un grupo de dispositivos terminales de retransmisión objetivo. El primer dispositivo de red
- 10 114 puede transmitir el conjunto de información de seguridad en asociación con el ID restringido de retransmisión.

En algunas realizaciones de ejemplo, opcionalmente, antes de transmitir el al menos un conjunto de información de seguridad, el primer dispositivo de red 114 puede construir 440 una lista de información de seguridad para el

15 descubrimiento de retransmisión. Cada elemento en la lista puede estar asociado con uno del al menos un conjunto de información de seguridad.

En algunas realizaciones de ejemplo, cada elemento en la lista puede estar asociado con un conjunto de información de seguridad y un ID restringido de retransmisión asociado con el conjunto de información de seguridad. La tabla

20 1 proporciona un ejemplo de la lista.

Tabla 1

ID restringido de retransmisión n.º 1	Un conjunto de información de seguridad n.º 1
ID restringido de retransmisión n.º 2	Un conjunto de información de seguridad n.º 2

ID restringido de retransmisión n.º 3	Un conjunto de información de seguridad n.º 3
---------------------------------------	---

En la Tabla 1, cada fila puede presentar un elemento de la lista de información de seguridad para el descubrimiento de retransmisión. Cada elemento puede estar asociado con un conjunto de información de seguridad para un grupo de dispositivos terminales de retransmisión objetivo y un ID restringido de retransmisión. Por ejemplo, el conjunto de información de seguridad n.º 1 está asociado con el ID restringido de retransmisión n.º 1.

Se deberá hacer notar que el número de conjuntos de información de seguridad e ID restringidos de retransmisión asociados con los conjuntos de información de seguridad son ilustrativos. Se pueden aplicar más o menos conjuntos de información de seguridad e ID restringidos de retransmisión a la presente divulgación.

En algunas realizaciones de ejemplo, cada uno del al menos un conjunto de información de seguridad puede comprender al menos uno de los siguientes: parámetros de seguridad para descubrimiento de retransmisión, o algoritmo de cifrado de PC5, o clave de integridad de usuario de descubrimiento (DUK) para descubrimiento de retransmisión.

En algunas realizaciones de ejemplo, el primer dispositivo de PCF 116 se puede configurar con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y soporta un RSC. De forma similar, el segundo dispositivo de PCF 126 se puede configurar con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la segunda HPLMN 120 y soporta un RSC. En tales realizaciones de ejemplo, el primer dispositivo de red 114 puede obtener la al

menos una identidad desde el primer dispositivo de PCF 116 en la primera HPLMN 110. Esto se describirá con referencia a la figura 5.

La figura 5 ilustra un gráfico de señalización que ilustra un proceso 500 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el proceso 500 se describirá con referencia a la figura 1. El proceso 500 puede implicar el primer dispositivo de red 114 y el primer dispositivo de PCF 116 en la figura 1.

Como se muestra en la figura 5, el primer dispositivo de red 114 transmite una segunda solicitud de la al menos una identidad al primer dispositivo de PCF 116. Cada una de la al menos una identidad es para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan un RSC. La segunda solicitud comprende al menos el RSC.

En consecuencia, el primer dispositivo de PCF 116 recibe, desde el primer dispositivo de red 114, la segunda solicitud de la al menos una identidad.

El primer dispositivo de PCF 116 obtiene la al menos una identidad basándose en la segunda solicitud.

A su vez, el primer dispositivo de PCF 116 transmite una segunda respuesta a la segunda solicitud al primer dispositivo de red 114. La segunda respuesta comprende al menos la al menos una identidad.

En consecuencia, el primer dispositivo de red 114 recibe la segunda respuesta que comprende la al menos una identidad.

En algunas realizaciones de ejemplo, el primer dispositivo de red 114 se puede configurar con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y soporta un

RSC. De forma similar, el segundo dispositivo de red 124 se puede configurar con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la segunda HPLMN 120 y soporta un RSC.

En tales realizaciones de ejemplo, si un primer grupo de dispositivos
5 terminales de retransmisión objetivo de entre el al menos un grupo pertenece a la primera HPLMN 110, el primer dispositivo de red 114 puede obtener una primera identidad para el primer grupo de dispositivos terminales de retransmisión objetivo localmente. A su vez, el primer dispositivo de red 114 puede obtener un primer conjunto de información de seguridad asociada con el
10 primer grupo de dispositivos terminales de retransmisión objetivo localmente.

En tales realizaciones de ejemplo, si un segundo grupo de dispositivos terminales de retransmisión objetivo de entre el al menos un grupo pertenece a la segunda HPLMN 120, el primer dispositivo de red 114 puede obtener, desde el segundo dispositivo de red 124, un segundo conjunto de información de
15 seguridad asociada con el segundo grupo de dispositivos terminales de retransmisión objetivo. Esto se describirá con referencia a la figura 6.

La figura 6 ilustra un gráfico de señalización que ilustra un proceso 600 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para
20 fines de análisis, el proceso 600 se describirá con referencia a la figura 1. El proceso 600 puede implicar el primer dispositivo de red 114 y el segundo dispositivo de red 124 en la figura 1.

Como se muestra en la figura 6, el primer dispositivo de red 114 transmite 610, al segundo dispositivo de red 124, una tercera solicitud de al menos un
25 segundo conjunto de información de seguridad para el RSC. La tercera solicitud

comprende al menos el RSC.

En consecuencia, el segundo dispositivo de red 124 recibe, desde el primer dispositivo de red 114, la tercera solicitud del al menos un segundo conjunto de información de seguridad para el RSC.

5 El segundo dispositivo de red 124 obtiene 620 el al menos un segundo conjunto de información de seguridad basándose en la tercera solicitud. Cada uno del al menos un segundo conjunto de información de seguridad está asociado con un segundo grupo de dispositivos terminales de retransmisión objetivo que pertenecen a la segunda HPLMN 120.

10 A su vez, el segundo dispositivo de red 124 transmite 630, al primer dispositivo de red 114, una tercera respuesta a la tercera solicitud. La tercera respuesta comprende al menos el al menos un segundo conjunto de información de seguridad.

En lo sucesivo en el presente documento, algunas implementaciones de ejemplo de los procesos 400, 500 y 600 se describirán con referencia a las figuras 7 a 11.

En las implementaciones de ejemplo de las figuras 7 a 11, un UE remoto y una retransmisión de U2N se toman como un ejemplo del primer dispositivo terminal 112 y el segundo dispositivo terminal 122, respectivamente. Una DDNMF o PKMF se toma como un ejemplo de cada uno del primer dispositivo de red 114 y el segundo dispositivo de red 124. Además, la primera HPLMN 110 está configurada con un ID de PLMN n.º 1, y la segunda HPLMN 120 está configurada con un ID de PLMN n.º 2.

La figura 7 ilustra un gráfico de señalización que ilustra un proceso 700 para obtener información de seguridad para descubrimiento de retransmisión de

acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el proceso 700 se describirá con referencia a la figura 1. El proceso 700 puede implicar el primer dispositivo terminal 112 (tal como un UE remoto 112), el segundo dispositivo terminal 122 (tal como una retransmisión de U2N 122), el primer dispositivo de red 114 (tal como una DDNMF 114), el primer dispositivo de PCF 116, el segundo dispositivo de red 124 (tal como una DDNMF 124) y el segundo dispositivo de PCF 126 en la figura 1.

En el proceso 700, el primer dispositivo de PCF 116 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y soporta un RSC. De forma similar, el segundo dispositivo de PCF 126 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la segunda HPLMN 120 y soporta un RSC.

Además, en el proceso 700, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y una identidad para un grupo de dispositivos terminales de retransmisión objetivo comprende una identidad de retransmisión para descubrimiento.

Como se muestra en la figura 7, en 701, la retransmisión de U2N 122 transmite una solicitud de clave de descubrimiento a su DDNMF 124 para conseguir información de seguridad para el descubrimiento de retransmisión para proteger mensajes de descubrimiento de PC5. La solicitud puede incluir un RSC y capacidades de seguridad de la retransmisión de U2N 122.

La acción en 701 se puede considerar como una implementación de ejemplo de la acción en 410 en la figura 4.

En 702, la DDNMF 124 de la retransmisión de U2N 122 genera un ID restringido de retransmisión para la retransmisión de U2N 122 con un temporizador válido. El ID restringido de retransmisión está asociado con el RSC y una identidad de retransmisión para descubrimiento para la retransmisión de U2N 122. En lo sucesivo en el presente documento, la identidad de retransmisión para descubrimiento también se denomina "ID de retransmisión" por brevedad. Por ejemplo, el ID de retransmisión puede incluir el ID de HPLMN (tal como el ID de PLMN n.º 2) de la retransmisión de U2N 122. Entonces, la DDNMF 124 obtiene la información de seguridad asociada con el ID restringido de retransmisión. Por ejemplo, la DDNMF 124 puede generar parámetros de seguridad y seleccionar el algoritmo de cifrado de PC5.

A su vez, la DDNMF 124 transmite una respuesta de clave de descubrimiento a la retransmisión de U2N 122. La respuesta incluye el RSC, el código de restricción de ProSe y el temporizador válido, los parámetros de seguridad específicos de código y el algoritmo de cifrado de PC5 elegido, TIEMPO_ACTUAL, DESPLAZAMIENTO_MÁX y políticas de seguridad de PC5 opcionales.

La acción en 702 se puede considerar como una implementación de ejemplo de las acciones en 420, 430, 440 y 450 en la figura 4.

En 703, el UE remoto 112 transmite una solicitud de clave de descubrimiento a su DDNMF 114 para conseguir información de seguridad para el descubrimiento de retransmisión para proteger mensajes de descubrimiento de PC5. La solicitud puede incluir una identidad de UE del UE remoto 112, un RSC y capacidad de seguridad del UE remoto 112.

La acción en 703 se puede considerar como otra implementación de

ejemplo de la acción en 410 en la figura 4.

En 704, la DDNMF 114 del UE remoto 112 transmite una solicitud a su dispositivo de PCF 116 para obtener identidades para retransmisiones potenciales que soportan el RSC para el UE remoto 112. La solicitud puede
5 incluir una identidad de UE del UE remoto 112 y el RSC.

La acción en 704 se puede considerar como una implementación de ejemplo de la acción en 510 en la figura 5.

En 705, el dispositivo de PCF 116 del UE remoto 112 obtiene los ID de las HPLMN de retransmisiones potenciales localmente basándose en el RSC y la
10 configuración local.

En 706a, el dispositivo de PCF 116 del UE remoto 112 obtiene ID de retransmisiones potenciales localmente basándose en el RSC y la configuración local para aquellas retransmisiones potenciales que pertenecen a la misma HPLMN del UE remoto 112.

En 706b, para aquellas retransmisiones potenciales que pertenecen a una HPLMN diferente del UE remoto 112, el dispositivo de PCF 116 del UE remoto 112 obtiene identidades de las retransmisiones potenciales de un dispositivo de PCF de la otra PLMN. Por ejemplo, para aquellas retransmisiones potenciales que pertenecen a la segunda HPLMN 120, el dispositivo de PCF
15 116 del UE remoto 112 obtiene identidades de las retransmisiones potenciales desde el dispositivo de PCF 126.
20

En 706b.1, el dispositivo de PCF 116 del UE remoto 112 transmite, al dispositivo de PCF 126 de la retransmisión de U2N 112, una solicitud de identidades para retransmisiones potenciales que pertenecen a la segunda
25 HPLMN 120. Esta solicitud también se denomina "solicitud de obtener

retransmisión potencial". La solicitud puede incluir el ID de PLMN n.º 1 de la primera HPLMN 110 del UE remoto 112 y el RSC.

En 706b.2, el dispositivo de PCF 116 del UE remoto 112 recibe una respuesta a la "solicitud de obtener retransmisión potencial". Esta respuesta
5 también se denomina "respuesta de obtener retransmisión potencial". La "respuesta de obtener retransmisión potencial" puede incluir el ID de PLMN n.º 2 de la segunda HPLMN 120, el RSC y una lista de ID de retransmisión.

Las acciones en 705, 706a, 706b.1, 706b.2 se pueden considerar como una implementación de ejemplo de la acción en 520 en la figura 5.

10 En algunas implementaciones de ejemplo, las acciones en 706a, 706b.1, 706b.2 se pueden repetir para cada HPLMN de retransmisiones potenciales.

En 707, el dispositivo de PCF 116 del UE remoto 112 transmite una respuesta a la DDNMF 114 del UE remoto 112. Esta respuesta también se denomina "respuesta de obtener retransmisión potencial". La respuesta puede
15 incluir la identidad de UE del UE remoto 112, el RSC y una lista de ID de retransmisión de las retransmisiones potenciales.

La acción en 707 se puede considerar como una implementación de ejemplo de la acción en 530 en la figura 5.

En 708a, si una retransmisión potencial pertenece a la misma HPLMN del
20 UE remoto 112, la DDNMF 114 genera un ID restringido de retransmisión para la retransmisión potencial con un temporizador válido. El ID restringido de retransmisión está asociado con el RSC y el ID de retransmisión para la retransmisión potencial. Entonces, la DDNMF 114 obtiene la información de seguridad asociada con el ID restringido de retransmisión. Por ejemplo, la
25 DDNMF 114 puede generar parámetros de seguridad, DUK y seleccionar el

algoritmo de cifrado de PC5 asociado con el ID restringido de retransmisión.

En 708b.1, si una retransmisión potencial pertenece a una HPLMN diferente, la DDNMF 114 del UE remoto 112 transmite una solicitud de clave de descubrimiento a la DDNMF de la HPLMN de la retransmisión potencial, para
5 obtener información de seguridad asociada con el RSC. Por ejemplo, la DDNMF 114 del UE remoto 112 transmite la solicitud de clave de descubrimiento a la DDNMF 124 de la segunda HPLMN 120. La DDNMF 114 del UE remoto 112 puede descubrir la DDNMF de la retransmisión potencial basándose en el ID de PLMN de la HPLMN de la retransmisión potencial que puede ser parte del ID de
10 retransmisión de la retransmisión potencial. La solicitud puede incluir capacidad de seguridad del UE remoto 112, el RSC y el ID de retransmisión de la retransmisión potencial.

La acción en 708b.1 se puede considerar como una implementación de ejemplo de la acción en 610 en la figura 6.

15 En 708b.2, la DDNMF 114 del UE remoto 112 recibe una respuesta de clave de descubrimiento desde la DDNMF 124 de la retransmisión de U2N 122. La respuesta puede incluir un ID restringido de retransmisión para la retransmisión potencial con un temporizador válido, parámetros de seguridad, DUIK y algoritmo de cifrado de PC5 elegido asociado al ID restringido de
20 retransmisión. El ID restringido de retransmisión está asociado con el RSC y el ID de retransmisión.

La acción en 708b.2 se puede considerar como una implementación de ejemplo de la acción en 630 en la figura 6.

En algunas implementaciones de ejemplo, las acciones en 708a, 708b.1
25 y 708b.2 se pueden repetir para cada retransmisión potencial.

En 709, la DDNMF 114 del UE remoto 112 construye una lista de ID restringido de retransmisión con un temporizador válido, parámetros de seguridad de código, DUIK y algoritmos de cifrado de PC5 correspondientes.

La acción en 709 se puede considerar como una implementación de
5 ejemplo de la acción en 440 en la figura 4.

En 710, la DDNMF del UE remoto 112 transmite una respuesta de clave de descubrimiento al UE remoto 112. La respuesta puede incluir el RSC, políticas de seguridad de PC5 opcionales, TIEMPO_ACTUAL, DESPLAZAMIENTO_MÁX, una lista de (ID restringido de retransmisión,
10 temporizador válido, Code-Rcv-SecParams (es decir, los parámetros de seguridad), algoritmo de cifrado de PC5 elegido).

TIEMPO_ACTUAL contiene el tiempo basado en UTC actual en la DDNMF de 5G. El UE puede obtener el tiempo UTC desde cualquier fuente disponible, por ejemplo, la RAN a través de SIB9, NITZ, NTP, GPS, a través de
15 la interfaz Ub (en GBA) (dependiendo de cuál esté disponible).

El parámetro DESPLAZAMIENTO_MÁX se usa para limitar la capacidad de un atacante para reproducir con éxito mensajes de descubrimiento u obtener correctamente un mensaje de descubrimiento sometido a MIC para su uso posterior. Esto se logra usando DESPLAZAMIENTO_MÁX como una diferencia
20 máxima entre el contador basado en UTC asociado con la ranura de descubrimiento y el reloj de ProSe mantenido por el UE.

La acción en 710 se puede considerar como una implementación de ejemplo de la acción en 450 en la figura 4.

En 711, el UE remoto 112 y la retransmisión de U2N 122 realizan el
25 descubrimiento de retransmisión a través de PC5. Los mensajes de

descubrimiento se protegen con el al menos un conjunto de información de seguridad. Cada uno del al menos un conjunto de información de seguridad está asociado con el ID restringido de retransmisión (que es para cada retransmisión para cada RSC).

5 La acción en 711 se puede considerar como una implementación de ejemplo de la acción en 460 en la figura 4.

 El proceso 700 se puede alinear con el sistema de paquetes evolucionado (EPS) heredado/procedimiento de descubrimiento directo de 5G con extensión para soportar solicitud de clave de descubrimiento para
10 descubrimiento de retransmisión. Además, el proceso 700 puede reducir la carga de señalización desde el UE remoto 112 a su HPLMN 110.

 La figura 8 ilustra un gráfico de señalización que ilustra un proceso 800 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para
15 fines de análisis, el proceso 800 se describirá con referencia a la figura 1. El proceso 800 puede implicar el primer dispositivo terminal 112 (tal como el UE remoto 112), el segundo dispositivo terminal 122 (tal como la retransmisión de U2N 122), el primer dispositivo de red 114 (tal como la DDNMF 114), el primer dispositivo de PCF 116, el segundo dispositivo de red 124 (tal como la DDNMF
20 124) y el segundo dispositivo de PCF 126 en la figura 1.

 El proceso 800 es similar al proceso 700 en que el primer dispositivo de PCF 116 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y soporta un RSC. De forma similar, el segundo dispositivo de PCF 126 está configurado con
25 una identidad de al menos un dispositivo terminal de retransmisión objetivo que

pertenece a la segunda HPLMN 120 y soporta un RSC.

Además, el proceso 800 es similar al proceso 700 en que cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y una identidad para un grupo de dispositivos terminales de retransmisión objetivo comprende una
5 identidad de retransmisión para descubrimiento.

El proceso 800 es diferente del proceso 700 en que se puede evitar la interacción entre dispositivos de PCF de diferentes HPLMN y se pueden reducir los mensajes entre DDNMF de dos HPLMN.

10 Específicamente, las acciones en 801, 802, 803, 805, 808a, 809, 810 y 811 en el proceso 800 son similares a las acciones en 701, 702, 703, 705, 708a, 709, 710 y 711 en el proceso 700. Por lo tanto, los detalles de estas acciones se omiten por brevedad.

Las acciones en 804, 806, 807, 808b.1, 808b.2 y 808b.3 en el proceso
15 800 son diferentes de las acciones en el proceso 700.

En 804, la DDNMF 114 del UE remoto 112 transmite una solicitud a su dispositivo de PCF 116 para obtener unos ID para unas HPLMN que soportan un RSC para el UE remoto 112. La solicitud puede incluir una identidad de UE del UE remoto 112 y el RSC. Esta solicitud también se denomina "solicitud de
20 obtener HPLMN de retransmisiones potenciales".

La acción en 804 se puede considerar como otra implementación de ejemplo de la acción en 510 en la figura 5.

En 805, el dispositivo de PCF 116 del UE remoto 112 obtiene los ID de las HPLMN de retransmisiones potenciales localmente basándose en el RSC y la
25 configuración local.

La acción en 805 se puede considerar como otra implementación de ejemplo de la acción en 530 en la figura 5.

En 806, el dispositivo de PCF 116 del UE remoto 112 transmite una respuesta a la DDNMF 114. Esta respuesta también se denomina "respuesta de
5 obtener las HPLMN de retransmisiones potenciales". La respuesta puede incluir la identidad de UE del UE remoto 112, el RSC y una lista de ID de PLMN. Por ejemplo, la lista de ID de PLMN puede comprender al menos uno de los siguientes: el ID de la primera HPLMN 110 (tal como ID de PLMN n.º 1), o el ID de la segunda HPLMN 120 (tal como el ID de PLMN n.º 2)

10 La acción en 806 se puede considerar como otra implementación de ejemplo de la acción en 530 en la figura 5.

En 807, si la lista de ID de PLMN puede comprender el ID de la primera HPLMN 110 (tal como el ID de PLMN n.º 1), la DDNMF 114 del UE remoto 112 obtiene los ID de retransmisiones potenciales desde el dispositivo de PCF 116
15 del UE remoto 112 basándose en el RSC.

La acción en 807 se puede considerar como otra implementación de ejemplo de las acciones en 510, 520 y 530 en la figura 5.

En 808b.1, si la lista de ID de PLMN puede comprender el ID de la segunda HPLMN 120 (tal como el ID de PLMN n.º 2), la DDNMF 114 del UE
20 remoto 112 transmite una solicitud de clave de descubrimiento a la DDNMF 124 de la HPLMN 120, para obtener información de seguridad asociada con el RSC. La solicitud puede incluir capacidad de seguridad del UE remoto 112 y el RSC. Se deberá hacer notar que la solicitud puede incluir o no el ID de la segunda HPLMN 120 (tal como el ID de PLMN n.º 2). Esto significa que es necesario
25 obtener información de seguridad asociada con cada una de las

retransmisiones potenciales en la segunda HPLMN 120.

La acción en 808b.1 se puede considerar como otra implementación de ejemplo de la acción en 610 en la figura 6.

En 808b.2, la DDNMF 124 de la retransmisión de U2N 122 obtiene, desde el dispositivo de PCF 126, unos ID de retransmisión para las retransmisiones potenciales en la segunda HPLMN 120 basándose en el RSC. Entonces, la DDNMF 124 genera un ID restringido de retransmisión para cada una de las retransmisiones potenciales con un temporizador válido. El ID restringido de retransmisión está asociado con el RSC y el ID de retransmisión para la retransmisión potencial. Entonces, la DDNMF 124 obtiene la información de seguridad asociada con el ID restringido de retransmisión. Por ejemplo, la DDNMF 124 puede generar parámetros de seguridad y seleccionar el algoritmo de cifrado de PC5 asociado con el ID restringido de retransmisión. A su vez, la DDNMF 124 construye una lista de ID restringido de retransmisión con un temporizador válido, parámetros de seguridad de código y algoritmos de cifrado de PC5 correspondientes.

En algunas realizaciones de ejemplo, cada elemento en la lista puede estar asociado con un segundo conjunto de información de seguridad y un ID restringido de retransmisión asociado con el segundo conjunto de información de seguridad. La tabla 2 proporciona un ejemplo de la lista.

Tabla 2

ID restringido de retransmisión n.º 3	Un segundo conjunto de información de seguridad n.º 3
ID restringido de retransmisión n.º 4	Un segundo conjunto de información de seguridad n.º 4

En la Tabla 2, cada fila puede presentar un elemento de la lista de información de seguridad para el descubrimiento de retransmisión. Cada elemento puede estar asociado con un segundo conjunto de información de seguridad para un dispositivo terminal de retransmisión objetivo y un ID restringido de retransmisión. Por ejemplo, el segundo conjunto de información de seguridad n.º 3 está asociado con un primer dispositivo terminal de retransmisión objetivo y el ID restringido de retransmisión n.º 3. El ID restringido de retransmisión n.º 3 se puede generar basándose en el RSC y un ID de retransmisión del primer dispositivo terminal de retransmisión objetivo.

Se deberá hacer notar que el número de conjuntos de información de seguridad e ID restringidos de retransmisión asociados con los conjuntos de información de seguridad son ilustrativos. Se pueden aplicar más o menos conjuntos de información de seguridad e ID restringidos de retransmisión a la presente divulgación.

En 808b.3, la DDNMF 114 del UE remoto 112 recibe una respuesta de clave de descubrimiento desde la DDNMF 124 de la retransmisión de U2N 122. La respuesta puede incluir una lista de ID restringido de retransmisión con un temporizador válido, parámetros de seguridad de código y algoritmos de cifrado de PC5 correspondientes.

La acción en 808b.3 se puede considerar como otra implementación de ejemplo de la acción en 630 en la figura 6.

La figura 9 ilustra un gráfico de señalización que ilustra un proceso 900 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el proceso 900 se describirá con referencia a la figura 1. El

proceso 900 puede implicar el primer dispositivo terminal 112 (tal como el UE remoto 112), el segundo dispositivo terminal 122 (tal como la retransmisión de U2N 122), el primer dispositivo de red 114 (tal como la DDNMF 114), el primer dispositivo de PCF 116 y el segundo dispositivo de red 124 (tal como la DDNMF 124) en la figura 1.

El proceso 900 es similar al proceso 800 en que el primer dispositivo de PCF 116 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y soporta un RSC. De forma similar, el segundo dispositivo de PCF 126 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la segunda HPLMN 120 y soporta un RSC.

Además, el proceso 900 es diferente del proceso 800 en que cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo en una de la primera HPLMN 110 o la segunda HPLMN 120. Una identidad para un grupo de dispositivos terminales de retransmisión objetivo comprende uno de los siguientes: una identidad (ID) de PLMN de la primera HPLMN 110 o la segunda HPLMN 120 a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o un ID de grupo de la pluralidad de dispositivos terminales de retransmisión objetivo. Por ejemplo, el ID de grupo puede incluir el ID de PLMN de la primera HPLMN 110 o la segunda HPLMN 120.

Específicamente, las acciones en 901, 902, 903, 904, 905, 906, 908b.1, 909, 910 y 911 en el proceso 900 son similares a las acciones en 801, 802, 803, 804, 805, 806, 808b.1, 809, 810 y 811 en el proceso 800. Por lo tanto, los detalles de estas acciones se omiten por brevedad.

Las acciones en 908a y 908b.2 en el proceso 900 son diferentes de las acciones en el proceso 800.

En 908a, si la lista de ID de PLMN puede comprender el ID de la primera HPLMN 110 (tal como el ID de PLMN n.º 1), la DDNMF 114 del UE remoto 112
5 genera un ID restringido de retransmisión para todas las retransmisiones potenciales que soportan el RSC en la primera HPLMN 110. El ID restringido de retransmisión está asociado con el RSC y el ID de PLMN n.º 1. Entonces, la DDNMF 114 obtiene la información de seguridad asociada con el ID restringido de retransmisión. Por ejemplo, la DDNMF 114 puede generar parámetros de
10 seguridad y seleccionar el algoritmo de cifrado de PC5 asociado con el ID restringido de retransmisión. Además, la DDNMF 114 del UE remoto 112 puede generar un temporizador válido para el ID restringido de retransmisión.

En 908b.1, si la lista de ID de PLMN puede comprender el ID de la segunda HPLMN 120 (tal como el ID de PLMN n.º 2), la DDNMF 114 del UE
15 remoto 112 transmite una solicitud de clave de descubrimiento a la DDNMF 124 de la HPLMN 120, para obtener información de seguridad asociada con el RSC. La solicitud puede incluir capacidad de seguridad del UE remoto 112 y el RSC. Se deberá hacer notar que la solicitud puede incluir o no el ID de la segunda HPLMN 120 (tal como el ID de PLMN n.º 2). Esto significa que es necesario
20 obtener información de seguridad asociada con todas las retransmisiones potenciales en la segunda HPLMN 120.

La acción en 908b.1 se puede considerar como otra implementación de ejemplo de la acción en 610 en la figura 6.

En 908b.2, la DDNMF 114 del UE remoto 112 recibe una respuesta de
25 clave de descubrimiento desde la DDNMF 124 de la retransmisión de U2N 122.

La respuesta puede incluir el ID restringido de retransmisión con un temporizador válido, parámetros de seguridad de código y algoritmos de cifrado de PC5 correspondientes.

La acción en 908b.2 se puede considerar como otra implementación de
5 ejemplo de la acción en 630 en la figura 6.

En algunas implementaciones de ejemplo, las acciones en 908b.1 y 908b.2 se pueden repetir para cada HPLMN de retransmisiones potenciales asociadas con el RSC.

La figura 10 ilustra un gráfico de señalización que ilustra un proceso 1000
10 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el proceso 1000 se describirá con referencia a la figura 1. El proceso 1000 puede implicar el primer dispositivo terminal 112 (tal como el UE remoto 112), el segundo dispositivo terminal 122 (tal como la retransmisión de
15 U2N 122), el primer dispositivo de red 114 (tal como la DDNMF 114) y el segundo dispositivo de red 124 (tal como la DDNMF 124) en la figura 1.

El proceso 1000 es similar al proceso 800 en que cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y una identidad para un
20 grupo de dispositivos terminales de retransmisión objetivo comprende una identidad de retransmisión para descubrimiento.

El proceso 1000 es diferente del proceso 800 en que el primer dispositivo de red 114 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y
25 soporta un RSC. De forma similar, el segundo dispositivo de red 124 está

configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la segunda HPLMN 120 y soporta un RSC.

5 Específicamente, las acciones en 1001, 1002, 1003, 1008a, 1008b.1, 1008b.4, 1009, 1010 y 1011 en el proceso 1000 son similares a las acciones en 801, 802, 803, 808a, 808b.1, 808b.3, 809, 810 y 811 en el proceso 800. Por lo tanto, los detalles de estas acciones se omiten por brevedad.

Las acciones en 1005, 1006, 1008b.2 y 1008b.3 en el proceso 900 son diferentes de las acciones en el proceso 800.

10 En 1005, la DDNMF 114 del UE remoto 112 obtiene los ID de las HPLMN de retransmisiones potenciales localmente basándose en el RSC y la configuración local.

15 En 1006, la DDNMF 114 del UE remoto 112 obtiene ID de retransmisiones potenciales localmente basándose en el RSC y la configuración local para aquellas retransmisiones potenciales que pertenecen a la misma HPLMN del UE remoto 112.

En 1008b.2, la DDNMF 114 del UE remoto 112 obtiene unos ID de retransmisión para las retransmisiones potenciales en la segunda HPLMN 120 basándose en el RSC y la configuración local.

20 En 1008b.3, la DDNMF 124 genera un ID restringido de retransmisión para cada una de las retransmisiones potenciales con un temporizador válido. El ID restringido de retransmisión está asociado con el RSC y el ID de retransmisión para la retransmisión potencial. La DDNMF 124 también obtiene la información de seguridad asociada con el ID restringido de retransmisión. Por
25 ejemplo, la DDNMF 124 puede generar parámetros de seguridad y seleccionar

el algoritmo de cifrado de PC5 asociado con el ID restringido de retransmisión. A su vez, la DDNMF 124 construye una lista de ID restringido de retransmisión con un temporizador válido, parámetros de seguridad de código y algoritmos de cifrado de PC5 correspondientes. Un ejemplo de la lista se ha descrito en la

5 Tabla 2.

En algunas realizaciones de ejemplo, las acciones desde 1008b.1 a 1008b.4 se pueden repetir para cada PLMN de retransmisiones potenciales asociadas con el RSC.

La figura 11 ilustra un gráfico de señalización que ilustra un proceso 1100
10 para obtener información de seguridad para descubrimiento de retransmisión de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el proceso 1100 se describirá con referencia a la figura 1. El proceso 1100 puede implicar el primer dispositivo terminal 112 (tal como el UE remoto 112), el segundo dispositivo terminal 122 (tal como la retransmisión de
15 U2N 122), el primer dispositivo de red 114 (tal como la DDNMF 114) y el segundo dispositivo de red 124 (tal como la DDNMF 124) en la figura 1.

El proceso 1100 es similar al proceso 900 en que cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo en una de la
20 primera HPLMN 110 o la segunda HPLMN 120. Una identidad para un grupo de dispositivos terminales de retransmisión objetivo comprende uno de los siguientes: una identidad (ID) de PLMN de la primera HPLMN 110 o la segunda HPLMN 120 a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o un ID de grupo de la pluralidad de dispositivos
25 terminales de retransmisión objetivo. Por ejemplo, el ID de grupo puede incluir el

ID de PLMN de la primera HPLMN 110 o la segunda HPLMN 120.

El proceso 1100 es diferente del proceso 900 en que el primer dispositivo de red 114 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la primera HPLMN 110 y
5 soporta un RSC. De forma similar, el segundo dispositivo de red 124 está configurado con una identidad de al menos un dispositivo terminal de retransmisión objetivo que pertenece a la segunda HPLMN 120 y soporta un RSC.

Específicamente, las acciones en 1101, 1102, 1103, 1108a, 1108b.1,
10 1108b.2, 1109, 1110 y 1111 en el proceso 1100 son similares a las acciones en 901, 902, 903, 908a, 908b.1, 908b.2, 909, 910 y 911 en el proceso 900. Por lo tanto, los detalles de estas acciones se omiten por brevedad.

Una acción en 1105 en el proceso 1100 es diferente de las acciones en el proceso 900.

15 En 1105, la DDNMF 114 del UE remoto 112 obtiene los ID de las HPLMN de retransmisiones potenciales localmente basándose en el RSC y la configuración local.

En algunas realizaciones de ejemplo, las acciones en 1108b.1 y 1108b.2 se pueden repetir para cada PLMN de retransmisiones potenciales asociadas
20 con el RSC.

La figura 12 muestra un diagrama de flujo de un método 1200 de ejemplo implementado en un primer dispositivo de red de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el método 1200 se describirá desde la perspectiva del primer dispositivo de red
25 114 con respecto a la figura 1.

En el bloque 1210, el primer dispositivo de red 114 recibe, desde un dispositivo terminal atendido por el primer dispositivo de red, una primera solicitud de información de seguridad para descubrimiento de retransmisión. La primera solicitud comprende al menos un código de servicio de retransmisión (RSC).

En el bloque 1220, el primer dispositivo de red 114 obtiene al menos una identidad basándose en la primera solicitud. Cada una de la al menos una identidad es para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC.

En el bloque 1230, el primer dispositivo de red 114 obtiene al menos un conjunto de información de seguridad basándose en la al menos una identidad y el RSC. Cada uno del al menos un conjunto de información de seguridad está asociado con uno del al menos un grupo de dispositivos terminales de retransmisión objetivo.

En el bloque 1240, el primer dispositivo de red 114 transmite el al menos un conjunto de información de seguridad al dispositivo terminal.

En algunas realizaciones de ejemplo, obtener la al menos una identidad puede comprender: obtener la al menos una identidad desde un primer dispositivo de función de control de políticas (PCF) en la primera HPLMN.

En algunas realizaciones de ejemplo, obtener la al menos una identidad desde el primer dispositivo de PCF puede comprender: transmitir una segunda solicitud de la al menos una identidad al primer dispositivo de PCF, comprendiendo al menos la segunda solicitud el RSC; y recibir una segunda respuesta a la segunda solicitud desde el primer dispositivo de PCF, comprendiendo al menos la segunda respuesta la al menos una identidad.

En algunas realizaciones de ejemplo, obtener el al menos un conjunto de información de seguridad puede comprender: obtener un conjunto de información de seguridad asociada con una identidad restringida de retransmisión, generándose la identidad restringida de retransmisión basándose en el RSC y una identidad para uno del al menos un grupo de dispositivos terminales de retransmisión objetivo. En algunas realizaciones de ejemplo, transmitir el al menos un conjunto de información de seguridad puede comprender: transmitir el conjunto de información de seguridad en asociación con la identidad restringida de retransmisión.

10 En algunas realizaciones de ejemplo, obtener el al menos un conjunto de información de seguridad puede comprender: basándose en determinar que un primer grupo de dispositivos terminales de retransmisión objetivo de entre el al menos un grupo pertenece a la primera HPLMN, generar una primera identidad restringida de retransmisión basándose en el RSC y una primera identidad para
15 el primer grupo de dispositivos terminales de retransmisión objetivo, y obtener un primer conjunto de información de seguridad asociada con la primera identidad restringida de retransmisión.

En algunas realizaciones de ejemplo, obtener el al menos un conjunto de información de seguridad puede comprender: basándose en determinar que un
20 segundo grupo de dispositivos terminales de retransmisión objetivo de entre el al menos un grupo pertenece a una segunda HPLMN diferente de la primera HPLMN, transmitir, a un segundo dispositivo de red en la segunda HPLMN, una tercera solicitud de un segundo conjunto de información de seguridad para el RSC, y recibir, desde el segundo dispositivo de red, una tercera respuesta a la
25 tercera solicitud, comprendiendo la tercera respuesta el segundo conjunto de

información de seguridad y una segunda identidad restringida de retransmisión, estando asociada la segunda identidad restringida de retransmisión con el RSC y una segunda identidad para el segundo grupo.

En algunas realizaciones de ejemplo, la tercera solicitud incluye la
5 segunda identidad.

En algunas realizaciones de ejemplo, obtener la al menos una identidad puede comprender: obtener la al menos una identidad localmente.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a la primera HPLMN
10 o una segunda HPLMN, siendo la segunda HPLMN diferente de la primera HPLMN.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y cada una de la al menos una
15 identidad comprende una identidad de retransmisión para descubrimiento.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y cada una de la al menos una identidad comprende una de las siguientes: una identidad de PLMN de la
20 primera HPLMN o la segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo de la pluralidad de dispositivos terminales de retransmisión objetivo.

La figura 13 muestra un diagrama de flujo de un método de ejemplo 1300 implementado en un dispositivo terminal de acuerdo con algunas realizaciones
25 de ejemplo de la presente divulgación. Para fines de análisis, el método 1300 se

describirá desde la perspectiva del primer dispositivo terminal 112 con respecto a la figura 1. Como alternativa, el método 1300 se puede implementar en el segundo dispositivo terminal 122.

En el bloque 1310, el primer dispositivo terminal 112 transmite, a un
5 dispositivo de red en una red móvil pública terrestre doméstica (HPLMN), una solicitud de información de seguridad para descubrimiento de retransmisión. La solicitud comprende al menos un código de servicio de retransmisión (RSC).

En el bloque 1320, el primer dispositivo terminal 112 recibe al menos un
conjunto de información de seguridad desde el dispositivo de red. Cada uno del
10 al menos un conjunto de información de seguridad está asociado con uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC.

En el bloque 1330, el primer dispositivo terminal 112 realiza el
descubrimiento de retransmisión basándose en el al menos un conjunto de
15 información de seguridad.

En algunas realizaciones de ejemplo, recibir el al menos un conjunto de
información de seguridad puede comprender: recibir un conjunto de información
de seguridad en asociación con una identidad restringida de retransmisión,
estando asociada la identidad restringida de retransmisión con el RSC y una
20 identidad para uno del al menos un grupo de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de
dispositivos terminales de retransmisión objetivo pertenece a una primera
HPLMN o una segunda HPLMN, siendo la segunda HPLMN diferente de la
25 primera HPLMN.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y cada una de la al menos una identidad comprende una identidad de retransmisión para descubrimiento.

- 5 En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y cada una de la al menos una identidad comprende una de las siguientes: una identidad de PLMN para la primera o la segunda HPLMN a la que pertenece la pluralidad de dispositivos
- 10 terminales de retransmisión objetivo, o una identidad de grupo para la pluralidad de dispositivos terminales de retransmisión objetivo.

La figura 14 muestra un diagrama de flujo de un método 1400 de ejemplo implementado en un primer dispositivo de PFC de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el

15 método 1400 se describirá desde la perspectiva del primer dispositivo de PFC 116 con respecto a la figura 1.

En el bloque 1410, el primer dispositivo de PCF 116 recibe, desde un primer dispositivo de red en la primera HPLMN, una segunda solicitud de al menos una identidad. Cada una de la al menos una identidad es para uno de al

20 menos un grupo de dispositivos terminales de retransmisión objetivo que soportan un código de servicio de retransmisión (RSC), comprendiendo al menos la segunda solicitud el RSC.

En el bloque 1420, el primer dispositivo de PCF 116 obtiene la al menos una identidad basándose en la segunda solicitud.

25 En el bloque 1430, el primer dispositivo de PCF 116 transmite, al primer

dispositivo de red, una segunda respuesta a la segunda solicitud. Comprendiendo al menos la segunda respuesta la al menos una identidad.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a la primera HPLMN o una segunda HPLMN. La segunda HPLMN es diferente de la primera HPLMN.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y cada una de la al menos una identidad comprende una identidad de retransmisión para descubrimiento.

En algunas realizaciones de ejemplo, obtener la al menos una identidad puede comprender: basándose en determinar que el al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a la primera HPLMN, obtener, basándose en la segunda solicitud, una primera identidad de la primera HPLMN localmente; y obtener una identidad de retransmisión para descubrimiento para cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo localmente.

En algunas realizaciones de ejemplo, obtener la al menos una identidad puede comprender: basándose en determinar que el al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a la segunda HPLMN, transmitir, a un segundo dispositivo de PCF en la segunda HPLMN, una cuarta solicitud de al menos una identidad de retransmisión para descubrimiento para el al menos un grupo de dispositivos terminales de retransmisión objetivo, y recibir, desde el segundo dispositivo de PCF, una cuarta respuesta a la cuarta solicitud, comprendiendo la cuarta respuesta la al menos una identidad de retransmisión.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y la al menos una identidad comprende una de las siguientes: una identidad de PLMN para la primera o la
5 segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo para la pluralidad de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, obtener la al menos una identidad puede comprender: obtener la identidad de PLMN o la identidad de grupo
10 basándose en la segunda solicitud.

La figura 15 muestra un diagrama de flujo de un método 1500 de ejemplo implementado en un segundo dispositivo de red de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el método 1500 se describirá desde la perspectiva del segundo dispositivo de red
15 124 con respecto a la figura 1.

En el bloque 1510, el segundo dispositivo de red 124 recibe, desde un primer dispositivo de red en una primera HPLM, una tercera solicitud de al menos un segundo conjunto de información de seguridad para un código de servicio de retransmisión (RSC), la solicitud comprende al menos el RSC, y la
20 segunda HPLMN es diferente de la primera HPLMN.

En el bloque 1520, el segundo dispositivo de red 124 obtiene el al menos un segundo conjunto de información de seguridad basándose en la tercera solicitud.

En el bloque 1530, el segundo dispositivo de red 124 transmite una
25 tercera respuesta al primer dispositivo de red. La tercera respuesta comprende

al menos el al menos un segundo conjunto de información de seguridad.

En algunas realizaciones de ejemplo, cada uno del al menos un segundo conjunto de información de seguridad está asociado con un segundo grupo de dispositivos terminales de retransmisión objetivo que pertenecen a la segunda

5 HPLMN.

En algunas realizaciones de ejemplo, el segundo grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y una segunda identidad para el segundo grupo comprende una identidad de retransmisión para descubrimiento.

10 En algunas realizaciones de ejemplo, el segundo grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y una segunda identidad para el segundo grupo comprende una de las siguientes: una identidad de PLMN para la segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo para la pluralidad de dispositivos terminales de retransmisión objetivo.

15 En algunas realizaciones de ejemplo, obtener el al menos un segundo conjunto de información de seguridad puede comprender: generar una segunda identidad restringida de retransmisión basándose en el RSC y una segunda identidad para el segundo grupo, obtener uno del al menos un segundo conjunto de información de seguridad que está asociado con la segunda identidad restringida de retransmisión.

20 En algunas realizaciones de ejemplo, transmitir el al menos un segundo conjunto de información de seguridad puede comprender: transmitir el uno del al menos un segundo conjunto de información de seguridad en asociación con la

25

segunda identidad restringida de retransmisión.

En algunas realizaciones de ejemplo, la tercera solicitud comprende una segunda identidad para el segundo grupo de dispositivos terminales de retransmisión objetivo.

5 La figura 16 muestra un diagrama de flujo de un método 1600 de ejemplo implementado en un segundo dispositivo de PCF de acuerdo con algunas realizaciones de ejemplo de la presente divulgación. Para fines de análisis, el método 1600 se describirá desde la perspectiva del segundo dispositivo de PCF 126 con respecto a la figura 1.

10 En el bloque 1610, el segundo dispositivo de PCF 126 recibe una solicitud de al menos una identidad, siendo cada una de la al menos una identidad para un dispositivo terminal de retransmisión objetivo que soporta un código de servicio de retransmisión (RSC), comprendiendo al menos la solicitud el RSC.

15 En el bloque 1620, el segundo dispositivo de PCF 126 obtiene la al menos una identidad basándose en la solicitud.

En el bloque 1630, el segundo dispositivo de PCF 126 transmite una respuesta a la solicitud, comprendiendo la respuesta la al menos una identidad.

20 En algunas realizaciones de ejemplo, recibir la solicitud de al menos una identidad comprende recibir la solicitud desde uno de los siguientes: un primer dispositivo de red en una primera HPLMN diferente de la segunda HPLMN, o un segundo dispositivo de red en la segunda HPLMN.

25 En algunas realizaciones de ejemplo, un aparato capaz de realizar cualquiera del método 1200 (por ejemplo, el primer dispositivo de red 114) puede comprender medios para realizar las operaciones respectivas del método

1200. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de software. El aparato se puede implementar como, o se puede incluir en, el primer dispositivo de red 114. En algunas realizaciones de ejemplo, los medios
5 pueden comprender un procesador y una memoria.

En algunas realizaciones de ejemplo, el aparato comprende: medios para recibir, en un primer dispositivo de red en una primera red móvil pública terrestre doméstica (HPLMN) desde un dispositivo terminal atendido por el primer dispositivo de red, una primera solicitud de información de seguridad para
10 descubrimiento de retransmisión, comprendiendo al menos la primera solicitud un código de servicio de retransmisión (RSC); medios para obtener al menos una identidad basándose en la primera solicitud, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; medios para obtener al menos
15 un conjunto de información de seguridad basándose en la al menos una identidad y el RSC, estando asociado cada uno del al menos un conjunto de información de seguridad con uno del al menos un grupo de dispositivos terminales de retransmisión objetivo; y medios para transmitir el al menos un conjunto de información de seguridad al dispositivo terminal.

20 En algunas realizaciones de ejemplo, los medios para obtener la al menos una identidad pueden comprender: medios para obtener la al menos una identidad desde un primer dispositivo de función de control de políticas (PCF) en la primera HPLMN.

En algunas realizaciones de ejemplo, los medios para obtener la al
25 menos una identidad desde el primer dispositivo de PCF pueden comprender:

medios para transmitir una segunda solicitud de la al menos una identidad al primer dispositivo de PCF, comprendiendo al menos la segunda solicitud el RSC; y medios para recibir una segunda respuesta a la segunda solicitud desde el primer dispositivo de PCF, comprendiendo al menos la segunda respuesta la al
5 menos una identidad.

En algunas realizaciones de ejemplo, los medios para obtener el al menos un conjunto de información de seguridad pueden comprender: medios para obtener un conjunto de información de seguridad asociada con una identidad restringida de retransmisión, generándose la identidad restringida de
10 retransmisión basándose en el RSC y una identidad para uno del al menos un grupo de dispositivos terminales de retransmisión objetivo. En algunas realizaciones de ejemplo, los medios para transmitir el al menos un conjunto de información de seguridad pueden comprender: medios para transmitir el conjunto de información de seguridad en asociación con la identidad restringida
15 de retransmisión.

En algunas realizaciones de ejemplo, los medios para obtener el al menos un conjunto de información de seguridad pueden comprender: basándose en determinar que un primer grupo de dispositivos terminales de retransmisión objetivo de entre el al menos un grupo pertenece a la primera
20 HPLMN, medios para generar una primera identidad restringida de retransmisión basándose en el RSC y una primera identidad para el primer grupo de dispositivos terminales de retransmisión objetivo, y medios para obtener un primer conjunto de información de seguridad asociada con la primera identidad restringida de retransmisión.

25 En algunas realizaciones de ejemplo, los medios para obtener el al

menos un conjunto de información de seguridad pueden comprender:
basándose en determinar que un segundo grupo de dispositivos terminales de
retransmisión objetivo de entre el al menos un grupo pertenece a una segunda
HPLMN diferente de la primera HPLMN, medios para transmitir, a un segundo
5 dispositivo de red en la segunda HPLMN, una tercera solicitud de un segundo
conjunto de información de seguridad para el RSC, y medios para recibir, desde
el segundo dispositivo de red, una tercera respuesta a la tercera solicitud,
comprendiendo la tercera respuesta el segundo conjunto de información de
seguridad y una segunda identidad restringida de retransmisión, estando
10 asociada la segunda identidad restringida de retransmisión con el RSC y una
segunda identidad para el segundo grupo.

En algunas realizaciones de ejemplo, la tercera solicitud incluye la
segunda identidad.

En algunas realizaciones de ejemplo, los medios para obtener la al
15 menos una identidad pueden comprender: medios para obtener la al menos una
identidad localmente.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de
dispositivos terminales de retransmisión objetivo pertenece a la primera HPLMN
o una segunda HPLMN, siendo la segunda HPLMN diferente de la primera
20 HPLMN.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de
dispositivos terminales de retransmisión objetivo comprende un único
dispositivo terminal de retransmisión objetivo, y cada una de la al menos una
identidad comprende una identidad de retransmisión para descubrimiento.

25 En algunas realizaciones de ejemplo, cada uno del al menos un grupo de

dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y cada una de la al menos una identidad comprende una de las siguientes: una identidad de PLMN de la primera HPLMN o la segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo de la pluralidad de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, un aparato capaz de realizar cualquiera del método 1300 (por ejemplo, el primer dispositivo terminal 112) puede comprender medios para realizar las operaciones respectivas del método 1300. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de software. El aparato se puede implementar como, o se puede incluir en, el primer dispositivo terminal 112. En algunas realizaciones de ejemplo, los medios pueden comprender un procesador y una memoria.

En algunas realizaciones de ejemplo, el aparato comprende: medios para transmitir, desde un dispositivo terminal a un dispositivo de red en una red móvil pública terrestre doméstica (HPLMN), una solicitud de información de seguridad para descubrimiento de retransmisión, comprendiendo al menos la solicitud un código de servicio de retransmisión (RSC); medios para recibir al menos un conjunto de información de seguridad desde el dispositivo de red, estando asociado cada uno del al menos un conjunto de información de seguridad con uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan el RSC; y medios para realizar el descubrimiento de retransmisión basándose en el al menos un conjunto de información de seguridad.

En algunas realizaciones de ejemplo, recibir el al menos un conjunto de

información de seguridad puede comprender: recibir un conjunto de información de seguridad en asociación con una identidad restringida de retransmisión, estando asociada la identidad restringida de retransmisión con el RSC y una identidad para uno del al menos un grupo de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a una primera HPLMN o una segunda HPLMN, siendo la segunda HPLMN diferente de la primera HPLMN.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y cada una de la al menos una identidad comprende una identidad de retransmisión para descubrimiento.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y cada una de la al menos una identidad comprende una de las siguientes: una identidad de PLMN para la primera o segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo para la pluralidad de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, un aparato capaz de realizar cualquiera del método 1400 (por ejemplo, el primer dispositivo de PFC 116) puede comprender medios para realizar las operaciones respectivas del método 1400. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de

software. El aparato se puede implementar como, o se puede incluir en, el primer dispositivo de PCF 116. En algunas realizaciones de ejemplo, los medios pueden comprender un procesador y una memoria.

En algunas realizaciones de ejemplo, el aparato comprende: medios para
5 recibir, en un primer dispositivo de función de control de políticas (PCF) en una primera red móvil pública terrestre doméstica (HPLMN) desde un primer dispositivo de red en la primera HPLMN, una segunda solicitud de al menos una identidad, siendo cada una de la al menos una identidad para uno de al menos un grupo de dispositivos terminales de retransmisión objetivo que soportan un
10 código de servicio de retransmisión (RSC), comprendiendo al menos la segunda solicitud el RSC; medios para obtener la al menos una identidad basándose en la segunda solicitud; y medios para transmitir, al primer dispositivo de red, una segunda respuesta a la segunda solicitud, comprendiendo al menos la segunda respuesta la al menos una identidad.

15 En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a la primera HPLMN o una segunda HPLMN. La segunda HPLMN es diferente de la primera HPLMN.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende un único
20 dispositivo terminal de retransmisión objetivo, y cada una de la al menos una identidad comprende una identidad de retransmisión para descubrimiento.

En algunas realizaciones de ejemplo, los medios para obtener la al menos una identidad pueden comprender: basándose en determinar que el al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece
25 a la primera HPLMN, medios para obtener, basándose en la segunda solicitud,

una primera identidad de la primera HPLMN localmente; y medios para obtener una identidad de retransmisión para descubrimiento para cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo localmente.

En algunas realizaciones de ejemplo, los medios para obtener la al
5 menos una identidad pueden comprender: basándose en determinar que el al menos un grupo de dispositivos terminales de retransmisión objetivo pertenece a la segunda HPLMN, medios para transmitir, a un segundo dispositivo de PCF en la segunda HPLMN, una cuarta solicitud de al menos una identidad de retransmisión para descubrimiento para el al menos un grupo de dispositivos
10 terminales de retransmisión objetivo, y medios para recibir, desde el segundo dispositivo de PCF, una cuarta respuesta a la cuarta solicitud, comprendiendo la cuarta respuesta la al menos una identidad de retransmisión.

En algunas realizaciones de ejemplo, cada uno del al menos un grupo de dispositivos terminales de retransmisión objetivo comprende una pluralidad de
15 dispositivos terminales de retransmisión objetivo, y la al menos una identidad comprende una de las siguientes: una identidad de PLMN para la primera o la segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo para la pluralidad de dispositivos terminales de retransmisión objetivo.

20 En algunas realizaciones de ejemplo, los medios para obtener la al menos una identidad pueden comprender: medios para obtener la identidad de PLMN o la identidad de grupo basándose en la segunda solicitud.

En algunas realizaciones de ejemplo, un aparato capaz de realizar cualquiera del método 1500 (por ejemplo, el segundo dispositivo de red 124)
25 puede comprender medios para realizar las operaciones respectivas del método

1500. Los medios se pueden implementar en cualquier forma adecuada. Por ejemplo, los medios se pueden implementar en una circuitería o módulo de software. El aparato se puede implementar como, o se puede incluir en, el segundo dispositivo de red 124. En algunas realizaciones de ejemplo, los
5 medios pueden comprender un procesador y una memoria.

En algunas realizaciones de ejemplo, el aparato comprende: medios para recibir, en un segundo dispositivo de red en una segunda red móvil pública terrestre doméstica (HPLMN) desde un primer dispositivo de red en una primera HPLM, una tercera solicitud de al menos un segundo conjunto de información
10 de seguridad para un código de servicio de retransmisión (RSC), comprendiendo al menos la solicitud el RSC, siendo la segunda HPLMN diferente de la primera HPLMN; medios para obtener el al menos un segundo conjunto de información de seguridad basándose en la tercera solicitud; y
medios para transmitir una tercera respuesta al primer dispositivo de red,
15 comprendiendo al menos la tercera respuesta el al menos un segundo conjunto de información de seguridad.

En algunas realizaciones de ejemplo, cada uno del al menos un segundo conjunto de información de seguridad está asociado con un segundo grupo de dispositivos terminales de retransmisión objetivo que pertenecen a la segunda
20 HPLMN.

En algunas realizaciones de ejemplo, el segundo grupo de dispositivos terminales de retransmisión objetivo comprende un único dispositivo terminal de retransmisión objetivo, y una segunda identidad para el segundo grupo comprende una identidad de retransmisión para descubrimiento.

25 En algunas realizaciones de ejemplo, el segundo grupo de dispositivos

terminales de retransmisión objetivo comprende una pluralidad de dispositivos terminales de retransmisión objetivo, y una segunda identidad para el segundo grupo comprende una de las siguientes: una identidad de PLMN para la segunda HPLMN a la que pertenece la pluralidad de dispositivos terminales de retransmisión objetivo, o una identidad de grupo para la pluralidad de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, los medios para obtener el al menos un segundo conjunto de información de seguridad pueden comprender: medios para generar una segunda identidad restringida de retransmisión basándose en el RSC y una segunda identidad para el segundo grupo y medios para obtener uno del al menos un segundo conjunto de información de seguridad que está asociado con la segunda identidad restringida de retransmisión.

En algunas realizaciones de ejemplo, los medios para transmitir el al menos un segundo conjunto de información de seguridad pueden comprender: medios para transmitir el uno del al menos un segundo conjunto de información de seguridad en asociación con la segunda identidad restringida de retransmisión.

En algunas realizaciones de ejemplo, la tercera solicitud comprende una segunda identidad para el segundo grupo de dispositivos terminales de retransmisión objetivo.

En algunas realizaciones de ejemplo, un aparato capaz de realizar cualquiera del método 1600 (por ejemplo, el segundo dispositivo de PCF 126) puede comprender medios para realizar las operaciones respectivas del método 1600. Los medios se pueden implementar en cualquier forma adecuada. Por

ejemplo, los medios se pueden implementar en una circuitería o módulo de software. El aparato se puede implementar como, o se puede incluir en, el segundo dispositivo de PCF 126. En algunas realizaciones de ejemplo, los medios pueden comprender un procesador y una memoria.

5 En algunas realizaciones de ejemplo, el aparato comprende: medios para recibir, en un segundo dispositivo de PCF en una segunda red móvil pública terrestre doméstica (HPLMN), una solicitud de al menos una identidad, siendo cada una de la al menos una identidad para un dispositivo terminal de retransmisión objetivo que soporta un código de servicio de retransmisión (RSC),
10 comprendiendo al menos la solicitud el RSC; medios para obtener la al menos una identidad basándose en la solicitud; y medios para transmitir una respuesta a la solicitud, comprendiendo la respuesta la al menos una identidad.

 En algunas realizaciones de ejemplo, los medios para recibir la solicitud de al menos una identidad comprenden medios para recibir la solicitud desde
15 uno de los siguientes: un primer dispositivo de red en una primera HPLMN diferente de la segunda HPLMN, o un segundo dispositivo de red en la segunda HPLMN.

 Se deberá hacer notar que los detalles de las realizaciones de ejemplo de la presente divulgación que se han descrito con referencia a las figuras 7 a 11
20 también se aplican a los métodos 1200 a 1600.

 La figura 17 es un diagrama de bloques simplificado de un dispositivo 1700 que es adecuado para implementar realizaciones de la presente divulgación. El dispositivo 1700 se puede proporcionar para implementar el dispositivo de comunicación, por ejemplo, el primer dispositivo terminal 112, el
25 primer dispositivo de red 114, el primer dispositivo de PCF 116, el segundo

dispositivo terminal 122, el segundo dispositivo de red 124 o el segundo dispositivo de PCF 126 como se muestra en la figura 1. Como se muestra, el dispositivo 1700 incluye uno o más procesadores 1710, una o más memorias 1720 acopladas al procesador 1710 y uno o más módulos de comunicación 1740 acoplados al procesador 1710.

El módulo de comunicación 1740 es para comunicaciones bidireccionales. El módulo de comunicación 1740 tiene 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 1710 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 basándose en arquitectura de procesador de múltiples núcleos, como ejemplos no limitantes.

El dispositivo 1700 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 1720 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) 1724, 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) 1722 y otras memorias volátiles que no perdurarán en la

duración de bajada de potencia.

Un programa informático 1730 incluye instrucciones ejecutables por ordenador que son ejecutadas por el procesador 1710 asociado. El programa 1730 se puede almacenar en la ROM 1724. El procesador 1710 puede realizar
5 cualquier acción y procesamiento adecuados cargando el programa 1730 en la RAM 1722.

Las realizaciones de la presente divulgación se pueden implementar por medio del programa 1730 de tal modo que el dispositivo 1700 puede realizar cualquier proceso de la divulgación como se analiza con referencia a las figuras
10 1 a 16. Las realizaciones de la presente divulgación también se pueden implementar por hardware o por una combinación de software y hardware.

En algunas realizaciones de ejemplo, el programa 1730 se puede contener tangiblemente en un medio legible por ordenador que se puede incluir en el dispositivo 1700 (tal como en la memoria 1720) u otros dispositivos de
15 almacenamiento a los que puede acceder el dispositivo 1700. El dispositivo 1700 puede cargar el programa 1730 desde el medio legible por ordenador en la RAM 1722 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 18 muestra un
20 ejemplo del medio legible por ordenador 1800 en forma de CD o DVD. El medio legible por ordenador tiene el programa 1730 almacenado en el mismo.

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
25 implementar en hardware, mientras que otros aspectos se pueden implementar

en firmware o software que puede ser ejecutado por un controlador, microprocesador u otro 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, aparato, sistema, técnica o método descrito en el presente documento se puede implementar en, como ejemplos no limitantes, 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 almacenamiento legible por ordenador no transitorio. El producto de programa informático incluye instrucciones ejecutables por ordenador, tales como las incluidas en módulos de programa, que se ejecutan en un dispositivo en un procesador real o virtual objetivo, para llevar a cabo los métodos 1200 a 1600 como se ha descrito anteriormente con referencia a las figuras 12 a 16. En general, los 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 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 de programación. Estos códigos de programa se pueden proporcionar a un procesador o controlador de un ordenador de propósito general, ordenador de propósito especial u otro aparato de procesamiento de datos programable, de tal modo que los códigos de programa, cuando son ejecutados por el procesador o controlador, hacen que se implementen las funciones/operaciones especificadas 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.

En el contexto de la presente divulgación, los códigos de programa informático o datos relacionados pueden ser portados por cualquier soporte adecuado para habilitar que el dispositivo, aparato 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.

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, aparato o dispositivo electrónico, magnético, óptico, electromagnético, de infrarrojos o de semiconductores o cualquier combinación adecuada de los anteriores. Ejemplos 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 lectura (CD-ROM) portátil, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento magnético o cualquier combinación adecuada de los anteriores.

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. 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 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.