(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 788 074**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 12/10 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.10.2018 PCT/EP2018/076650**

(87) Fecha y número de publicación internacional: **11.04.2019 WO19068644**

(96) Fecha de presentación y número de la solicitud europea: **01.10.2018 E 18785537 (4)**

(97) Fecha y número de publicación de la concesión europea: **01.04.2020 EP 3513584**

(54) Título: **Seguridad en el estrato de acceso en un sistema de comunicaciones inalámbricas**

(30) Prioridad:

02.10.2017 US 201762566840 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2020

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

WIFVESSON, MONICA;
SAARINEN, PASI;
TORVINEN, VESA y
NAKARMI, PRAJWOL, KUMAR

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Seguridad en el estrato de acceso en un sistema de comunicaciones inalámbricas

Antecedentes

La securización de un sistema de comunicaciones inalámbricas implica proteger la integridad y/o la confidencialidad de la comunicación intercambiada. Un sistema de Evolución a Largo Plazo (LTE), por ejemplo, exige que las comunicaciones del plano de usuario en el estrato de acceso (AS) entre el equipo de usuario (UE) y la red de acceso de radiocomunicaciones (RAN) estén protegidas en términos de confidencialidad, y que las comunicaciones del plano de control en el AS estén protegidas en términos tanto de integridad como de confidencialidad. Sin embargo, el hecho de requerir de manera inflexible este tipo de seguridad sin excepciones puede no ser deseable en todas las circunstancias, ya que puede resultar innecesariamente exigente con respecto a los recursos de la red, la potencia, el rendimiento del sistema, etcétera. No obstante, el permitir que la seguridad del plano de usuario en el AS sea opcional introduce desafíos en cuanto a garantizar que la seguridad se active selectivamente cuando así se desee y que se deje desactivada cuando no.

Sumario

Las reivindicaciones independientes definen aspectos de la invención. Las reivindicaciones dependientes definen realizaciones adicionales.

De acuerdo con algunas realizaciones del presente documento, una red central (CN) toma la decisión de si un nodo de red de acceso de radiocomunicaciones (RAN) debe activar o no la seguridad del plano de usuario en el estrato de acceso (AS), por ejemplo, en forma de protección de integridad y/o protección de confidencialidad del plano de usuario. Sin embargo, en particular, la CN indica al nodo de RAN si la CN permite o no que el nodo de RAN desestime esa decisión de la CN. En algunas realizaciones, esto permite efectivamente que la CN elija entre (i) imponer íntegramente la decisión de la CN como una orden que el nodo de RAN debe cumplir, por ejemplo, como una condición para que el nodo de RAN preste servicio a una sesión de plano de usuario; y (ii) ofrecer de manera flexible la decisión de la CN como una solicitud o preferencia que el nodo de RAN puede simplemente tener en cuenta, por ejemplo, junto con otra información disponible localmente en el nodo de RAN. Es decir, la CN puede mantener de forma centralizada un control absoluto sobre la activación de la seguridad del plano de usuario en el AS o ceder/distribuir al menos parte de ese control al nodo de RAN. La CN, por ejemplo, puede no permitir que el nodo de RAN desestime su decisión de activación de seguridad si la información en la CN (por ejemplo, referente a la sensibilidad, al tipo o a la prioridad del tráfico del plano de usuario) sugiere que la decisión de la CN debería prevalecer o primar sobre cualquier aportación que pudiera ofrecer el nodo de RAN sobre la conveniencia o la viabilidad de la activación de seguridad (por ejemplo, el impacto de la activación de seguridad sobre la carga o la eficiencia energética del nodo de RAN).

Por lo tanto, en estos y otros contextos, algunas realizaciones en el presente documento configuran ventajosamente la seguridad del plano de usuario en el AS de una manera robusta que distribuye flexiblemente la toma de decisiones de activación de seguridad entre la CN y la RAN según sea necesario para tener en cuenta información disponible localmente en la CN y la RAN, mientras que se centraliza estrictamente la toma de decisiones de activación de seguridad en la CN cuando sea necesario para priorizar íntegramente información disponible en la CN. Esto a su vez puede reforzar la seguridad del plano de usuario en términos de protección de la confidencialidad y/o la integridad, así como facilitar el equilibrado de la carga, la eficiencia de los recursos de radiocomunicaciones y la eficiencia energética en la red.

Más particularmente, realizaciones del presente documento incluyen un método para configurar la seguridad del plano de usuario en el estrato de acceso (AS) en un sistema de comunicaciones inalámbricas que incluye una red de acceso de radiocomunicaciones (RAN) y una red central (CN). El método lo lleva a cabo un nodo de RAN en la RAN. El método comprende recibir, desde la CN, señalización que indica una decisión de la CN sobre si el nodo de RAN debe activar o no la seguridad del plano de usuario en el AS y que indica si al nodo de RAN se le permite desestimar o no la decisión de la CN. El método en algunas realizaciones también incluye activar o no activar la seguridad del plano de usuario en el AS, dependiendo de la señalización.

En algunas realizaciones, el método comprende activar o no activar la seguridad del plano de usuario en el AS, dependiendo además de información que indica una capacidad o conveniencia del nodo de RAN para activar la seguridad del plano de usuario en el AS.

En algunas realizaciones, el método comprende además determinar si se activa o no la seguridad del plano de usuario en el AS, sobre la base de uno o más de: un nivel de carga del nodo de RAN; eficiencia energética o disponibilidad en el nodo de RAN; y autorización de la CN para activar la seguridad del plano de usuario en el AS; y un modo del nodo de RAN.

En algunas realizaciones, la señalización se aplica específicamente para una sesión de plano de usuario particular y se recibe durante un procedimiento para establecer la sesión de plano de usuario para un dispositivo de comunicaciones inalámbricas particular.

En algunas realizaciones, el método comprende además realizar una o más acciones cuando la decisión de la CN es que el nodo de RAN debe activar la seguridad del plano de usuario en el AS, al nodo de RAN no se le permite desestimar la decisión de la CN, y el nodo de RAN no puede, o la CN no está autorizada a, activar la seguridad del plano de usuario en el AS. La acción o acciones incluyen cancelar, rechazar o descartar una sesión de plano de usuario o un establecimiento de sesión de plano de usuario.

En algunas realizaciones, la decisión de la CN es una decisión sobre si el nodo de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la integridad del plano de usuario o es una decisión sobre si el nodo de RAN debe o no activar la seguridad del plano de usuario en el AS en forma de protección de la confidencialidad del plano de usuario.

En algunas realizaciones, la decisión la toma un nodo de CN que lleva a cabo la gestión de la sesión del plano de usuario.

En algunas realizaciones, la señalización indica si al nodo de RAN se le permite o no desestimar la decisión de la CN al indicar si la decisión de la CN es una orden que el nodo de RAN debe cumplir o una preferencia cuya desestimación se le permite al nodo de RAN.

Realizaciones del presente documento también incluyen un método para configurar la seguridad del plano de usuario en el estrato de acceso (AS) en un sistema de comunicaciones inalámbricas que incluye una red de acceso de radiocomunicaciones (RAN) y una red central (CN). El método lo lleva a cabo un nodo de CN en la CN. El método comprende tomar una decisión por parte de la CN sobre si un nodo de RAN en la RAN debe activar o no la seguridad del plano de usuario en el AS. El método también comprende transmitir señalización que indica la decisión de la CN y que indica si al nodo de RAN se le permite o no desestimar la decisión de la CN.

En algunas realizaciones, el método comprende además determinar si se permite o no que el nodo de RAN desestime la decisión, basándose en y/o específicamente para uno o más de: un tipo particular de seguridad del plano de usuario en el AS; un tipo o prioridad de servicio particular para el cual se debe comunicar el tráfico del plano de usuario a través del AS del plano de usuario; una ubicación o tipo de ubicación de nodo de RAN particular; un nivel de carga de nodo de RAN particular; un tipo o prioridad de abonado particular cuyo tráfico en el plano de usuario debe ser comunicación a través del AS del plano de usuario; y un momento o evento particular.

En algunas realizaciones, la señalización se aplica específicamente para una sesión de plano de usuario particular y se transmite durante un procedimiento para establecer la sesión de plano de usuario para un dispositivo de comunicaciones inalámbricas particular.

En algunas realizaciones, la decisión es una decisión sobre si el nodo de RAN debe activar o no la seguridad del plano del usuario en el AS en forma de protección de la integridad del plano del usuario o es una decisión sobre si el nodo de RAN debe activar o no la seguridad del plano del usuario en el AS en forma de protección de la confidencialidad del plano de usuario.

En algunas realizaciones, el nodo de CN está configurado para realizar la gestión de la sesión del plano de usuario.

En algunas realizaciones, la señalización indica si al nodo de RAN se le permite o no desestimar la decisión de la CN al indicar si la decisión de la CN es una orden que el nodo de RAN debe cumplir o una preferencia cuya desestimación se le permite al nodo de RAN .

Realizaciones también incluyen aparatos, programas informáticos y soportes correspondientes. Por ejemplo, realizaciones incluyen un nodo de red de acceso de radiocomunicaciones (RAN) para configurar la seguridad del plano de usuario en el estrato de acceso (AS) en un sistema de comunicaciones inalámbricas que incluye una RAN y una red central (CN). El nodo de RAN está configurado (por ejemplo, a través de circuitería de comunicación y circuitería de procesado) para recibir, desde la CN, señalización que indica una decisión de la CN sobre si el nodo de RAN debe activar o no la seguridad del plano de usuario en el AS y que indica si al nodo de RAN se le permite desestimar la decisión de la CN; y para activar o no activar la seguridad del plano de usuario en el AS, dependiendo de la señalización.

Además, las realizaciones incluyen un nodo de red central (CN) para configurar la seguridad del plano de usuario en el estrato de acceso (AS) en un sistema de comunicaciones inalámbricas que incluye una red de acceso de radiocomunicaciones (RAN) y una red central (CN). El nodo de CN está configurado (por ejemplo, a través de circuitería de comunicación y circuitería de procesado) para que la CN tome una decisión sobre si un nodo de RAN en la RAN debe activar o no la seguridad del plano de usuario en el AS; y transmitir señalización que indica la decisión de la CN y que indica si al nodo de RAN se le permite o no desestimar la decisión de la CN.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques de un sistema de comunicaciones inalámbricas de acuerdo con algunas realizaciones.

La Figura 2A es un diagrama de flujo lógico de un método llevado a cabo por un nodo de RAN de acuerdo con algunas realizaciones.

La Figura 2B es un diagrama de flujo lógico de un método llevado a cabo por un nodo de RAN de acuerdo con otras realizaciones.

La Figura 2C es un diagrama de flujo lógico de un método llevado a cabo por un nodo de RAN de acuerdo todavía con otras realizaciones.

La Figura 3A es un diagrama de flujo lógico de un método llevado a cabo por un nodo de CN de acuerdo con algunas realizaciones.

La Figura 3B es un diagrama de flujo lógico de un método llevado a cabo por un nodo de CN de acuerdo con otras realizaciones.

La Figura 3C es un diagrama de flujo lógico de un método llevado a cabo por un nodo de CN según todavía otras realizaciones.

La Figura 4 es un diagrama de flujo lógico de un método llevado a cabo por un dispositivo inalámbrico de acuerdo con algunas realizaciones.

La Figura 5A es un diagrama de bloques de un nodo de CN según algunas realizaciones.

La Figura 5B es un diagrama de bloques de un nodo de CN según otras realizaciones.

La Figura 6A es un diagrama de bloques de un nodo de RAN de acuerdo con algunas realizaciones.

La Figura 6B es un diagrama de bloques de un nodo de RAN de acuerdo con otras realizaciones.

La Figura 7A es un diagrama de bloques de un dispositivo inalámbrico de acuerdo con algunas realizaciones.

La Figura 7B es un diagrama de bloques de un dispositivo inalámbrico de acuerdo con otras realizaciones.

La Figura 8 es un diagrama de bloques de una red 5G de acuerdo con algunas realizaciones.

La Figura 9 es un diagrama de flujo de señalización de un Establecimiento de Sesión de PDU solicitado por un UE para seguimiento sin itinerancia e itinerante con desvío local (*local breakout*).

La Figura 10 es un diagrama de flujo de señalización de una Solicitud de Servicio desencadenada por un UE en un estado CM-IDLE.

La Figura 11 es un diagrama de flujo de señalización de algunas realizaciones para el control por parte de la CN sobre la desestimación, por parte de la RAN, de la decisión de la CN relativa a la seguridad del UP en el AS.

La Figura 12 es un diagrama de bloques de una red de comunicaciones con un ordenador anfitrión de acuerdo con algunas realizaciones.

La Figura 13 es un diagrama de bloques de un ordenador anfitrión de acuerdo con algunas realizaciones.

La Figura 14 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización.

La Figura 15 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización.

La Figura 16 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización.

La Figura 17 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización.

Descripción detallada

La Figura 1 muestra un sistema 10 de comunicaciones inalámbricas (por ejemplo, un sistema 5G) de acuerdo con algunas realizaciones. El sistema 10 incluye una red central (CN) 10A y una red de acceso de radiocomunicaciones (RAN) 10B. La RAN 10B incluye uno o más nodos 12 de RAN (por ejemplo, una o más estaciones base) para proporcionar acceso de radiocomunicaciones a dispositivos 14 de comunicaciones inalámbricas, mostrándose uno de ellos. A través de este acceso de radiocomunicaciones, un dispositivo 14 de comunicaciones inalámbricas se conecta a la CN 10A, que a su vez puede proporcionar al dispositivo 14 de comunicaciones inalámbricas acceso a una o más redes externas, como Internet. La CN 10A, por ejemplo, puede incluir diferentes nodos de CN, tales como un nodo

que implemente una función de acceso y movilidad, AMF, y un nodo que implemente una función de gestión de sesiones, SMF.

Desde el punto de vista de la estructura del protocolo, el sistema 10 se divide en un estrato de acceso (AS) y un estrato sin acceso (NAS). El AS contiene protocolos que administran actividades entre el dispositivo 14 de comunicaciones inalámbricas y la RAN 10B, por ejemplo, para transportar datos a través de una conexión de radiocomunicaciones y gestionar recursos de radiocomunicaciones. El NAS contiene protocolos que administran actividades entre el dispositivo 14 de comunicaciones inalámbricas y la CN 10A, por ejemplo, para establecer sesiones de comunicación y mantener comunicaciones continuas a medida que el dispositivo 14 de comunicaciones inalámbricas se mueve. El sistema 10 también se divide en un plano de usuario (UP) y un plano de control (CP). El plano de control contiene protocolos responsables de gestionar portadores de transporte, mientras que el plano de usuario contiene protocolos responsables de transportar tráfico de usuario.

La Figura 1 en particular muestra el plano de usuario (UP) del estrato de acceso (AS) 18 como la parte del sistema 10 responsable de transportar tráfico de usuario entre el dispositivo 14 de comunicaciones inalámbricas y la RAN 10B. El sistema 10 admite seguridad 18S para proteger el UP del AS 18, por ejemplo, en forma de protección de integridad y/o protección de confidencialidad (mediante encriptación o cifrado). Sin embargo, la activación o uso de esta seguridad 18S del UP del AS es opcional en algunas realizaciones, al menos en el sentido de que puede haber algunas condiciones bajo las cuales se permite dejar desactivada la seguridad 18S del UP del AS (en lugar de que el sistema 10 exija incondicionalmente que la seguridad del UP del AS esté siempre activada). Al ser opcional la activación de la seguridad 18S del UP del AS, se toma una decisión en el sistema 10 con respecto a si se activa o no la seguridad 18S del UP del AS.

En particular, de acuerdo con algunas realizaciones del presente documento, la CN 10A toma una decisión sobre si el nodo 12 de RAN debe activar o no la seguridad 18S del UP en el AS, por ejemplo, en forma de protección de la integridad y/o protección de la confidencialidad del plano de usuario. La Figura 1 muestra esta decisión como tomada por un nodo 16 de CN, por ejemplo, que realiza la gestión de la sesión en el plano de usuario, tal como mediante la implementación de una función de gestión de sesiones (SMF) en una CN 5G ó de Radiocomunicaciones Nuevas (NR). El nodo 16 de CN lleva a cabo la señalización 20 para señalizar esta decisión directa o indirectamente a la RAN 10B. En algunas realizaciones, por ejemplo, el nodo 16 de CN señaliza una indicación 20A de activación que indica la decisión de la CN sobre si el nodo 12 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS. El nodo 12 de RAN obtiene correspondientemente esta indicación 20A de activación (por ejemplo, al recibir la indicación 20A de la señalización 20) y usa la indicación 20A para determinar si se activa o no la seguridad 18S del UP del AS. La Figura 1, por ejemplo, muestra que un controlador 12A de seguridad del nodo 12 de RAN obtiene la indicación 20A de activación y controla la activación de seguridad del UP en el AS en función de la indicación 20A de activación.

Sin embargo, en particular, el nodo 12 de RAN también obtiene una indicación 22 de permiso de desestimación. La indicación de autorización desestimación indica si se permite o no (por ejemplo, por parte de la CN 10A) al nodo 12 de RAN desestimar la decisión de activación de la CN 10A. En algunas realizaciones, la CN 10A señaliza si al nodo 12 de RAN se le permite (por ejemplo, por parte de la CN 10A) desestimar la decisión de activación de la CN 10A, por ejemplo, señalizando la indicación 22 de permiso de desestimación directa o indirectamente al nodo 12 de RAN. Por ejemplo, la CN 10A puede señalizar la indicación 22 de permiso de desestimación dentro de un mensaje 24 dirigido o propagado de otro modo al nodo 22 de RAN (por ejemplo, junto con la indicación 20A de activación). Alternativamente, la CN 10A puede señalizar la indicación 22 de permiso de desestimación escribiendo la indicación 22 en un archivo 12A que se encuentra en el nodo 12 de RAN u obtenible de otro modo por este último, almacenando la indicación 22 en una base de datos (DB) 26 accesible para el nodo 12 de RAN, o similares. A continuación, en estos casos, el nodo 12 de RAN obtiene la indicación 22 de permiso de desestimación al recibir la indicación 22 del mensaje 24, leer la indicación 22 del archivo 12A, o recuperar la indicación 22 de la base 26 de datos. Sin embargo, todavía en otras realizaciones más, la indicación 22 de permiso de desestimación puede almacenarse en una configuración 12B del nodo 12 de RAN, por ejemplo, de tal manera que el nodo 12 de RAN esté preconfigurado con la indicación 22 de permiso de desestimación. En este caso, el nodo 12 de RAN obtiene la indicación de permiso de desestimación recuperándola de la configuración 12B.

En cualquier caso, el controlador 12A de seguridad del nodo 12 de RAN puede activar o no activar la seguridad 18S del UP en el AS, dependiendo de la decisión de la CN y de si al nodo 12 de RAN se le permite o no desestimar esa decisión, por ejemplo, dependiendo de la indicación 20A de activación y de la indicación 22 de permiso de desestimación. Por ejemplo, si la indicación 22 de permiso de desestimación indica que al nodo 12 de RAN no se le permite desestimar la decisión de la CN, el nodo 12 de RAN puede seguir incondicionalmente esa decisión para activar o no activar la seguridad 18S del UP del AS de acuerdo con la decisión de la CN (por ejemplo, siempre que el nodo 12 de RAN pueda hacerlo). Pero si la indicación 20B de permiso de desestimación indica que al nodo 12 de RAN se le permite desestimar la decisión de la CN, el nodo 12 de RAN está configurado para elegir de forma autónoma si activar o no la seguridad 18S del UP del AS, por ejemplo, teniendo en cuenta la decisión de la CN así como otra información disponible localmente en el nodo 12 de RAN.

Por lo tanto, algunas realizaciones permiten efectivamente (por ejemplo, A través de la indicación 22 de permiso de desestimación) que el sistema 10 seleccione entre (i) imponer íntegramente la decisión de la CN como una orden que el nodo 12 de RAN debe cumplir, por ejemplo, como una condición para que el nodo 12 de RAN preste servicio a una

sesión de plano de usuario; y (ii) ofrecer de manera flexible la decisión de la CN como una solicitud o preferencia que el nodo 12 de RAN puede simplemente tener en cuenta, por ejemplo, junto con otra información disponible localmente en el nodo 12 de RAN. Es decir, la CN 10A puede mantener de forma centralizada un control absoluto sobre la activación de la seguridad del plano de usuario en el AS o ceder/distribuir al menos parte de ese control al nodo 12 de RAN. El sistema 10 puede, por ejemplo, no permitir que el nodo 12 de RAN desestime la decisión de activación de seguridad de la CN si hay información en la CN 10A que sugiere que la decisión de la CN debería prevalecer o primar sobre cualquier aportación que el nodo 12 de RAN pueda proporcionar sobre la conveniencia o viabilidad de la activación de seguridad. En estos y otros contextos, por lo tanto, algunas realizaciones del presente documento configuran ventajosamente la seguridad 18S del plano de usuario en el AS de una manera robusta que distribuye de manera flexible la toma de decisiones de activación de seguridad entre la CN 10A y la RAN 10B según sea necesario para tener en cuenta información disponible localmente en la CN 10A y la RAN 10B, mientras se centraliza estrictamente la toma de decisiones de activación de seguridad en la CN 10A cuando sea necesario para priorizar íntegramente información disponible en la CN 10A.

Más particularmente en algunas realizaciones, la decisión de la CN y/o el hecho de si la decisión puede ser desestimada (por ejemplo, una o ambas de las indicaciones 20A, 20B) pueden configurarse (por ejemplo, por el nodo 16 de CN) basándose en ciertas reglas de política de red y/o reglas de política de suscripción, por ejemplo, que pueden estar disponibles para la CN 10A pero no para la RAN 10B. Estas reglas pueden especificar que la decisión de la CN y/o el hecho de si la decisión puede ser desestimada (por ejemplo, las indicaciones 20A, 20B) deben establecerse en función de cierta información. Cuando lo establece el nodo 16 de CN, esta cierta información puede estar disponible en el nodo 16 de CN (pero no en la RAN 10B).

La información puede referirse, por ejemplo, a la sensibilidad, al tipo o a la prioridad del tráfico del plano de usuario que se comunicará a través del UP del AS 18. Por ejemplo, si el tráfico del plano de usuario se considera altamente sensible o de alta prioridad, las indicaciones 20A, 20B pueden indicar que la CN 10A ha decidido activar la seguridad 18S del UP en el AS y que al nodo 12 de RAN no se le permite desestimar la decisión de la CN. Pero si el tráfico del plano de usuario es menos sensible o tiene una prioridad menor, la indicación 20B de permiso de desestimación puede indicar que al nodo 12 de RAN se le permite desestimar la decisión de la CN.

De manera similar, la información puede referirse al tipo o prioridad de servicio para el que se debe comunicar el tráfico del plano de usuario a través del UP del AS 18. Por ejemplo, si el tráfico del plano de usuario se debe comunicar para un servicio de Internet de las Cosas (IoT), las indicaciones 20A, 20B pueden indicar que la CN 10A ha decidido activar la seguridad 18S del UP en el AS y que al nodo 12 de RAN no se le permite desestimar la decisión de la CN. Pero si el tráfico del plano de usuario se va a comunicar para un servicio de vídeo, la indicación 20B de permiso de desestimación puede indicar que al nodo 12 de RAN se le permite desestimar la decisión de la CN.

Todavía en otras realizaciones, la información puede referirse de manera alternativa o adicional al tipo o prioridad de abonado(s) cuyo tráfico de plano de usuario se comunicará a través del UP del AS 18. Por ejemplo, si el abonado cuyo tráfico de plano de usuario se comunicará a través del UP del AS 18 es el Presidente de una nación, las indicaciones 20A, 20B pueden indicar que la CN 10A ha decidido activar la seguridad 18S del UP del AS y que al nodo 12 de RAN no se le permite desestimar la decisión de la CN. Pero si el abonado cuyo tráfico de plano de usuario se va a comunicar a través del UP del AS 18 es un abonado público, la indicación 20B de permiso de desestimación puede indicar que al nodo 12 de RAN se le permite desestimar la decisión de la CN.

De manera alternativa o adicional, la información puede referirse al momento o evento particular durante el cual se debe comunicar tráfico del plano de usuario a través del UP del AS 18. Por ejemplo, si el tráfico del plano de usuario se debe comunicar a través del UP del AS 18 durante las elecciones de una nación, las indicaciones 20A, 20B pueden indicar que la CN 10A ha decidido activar la seguridad 18S del UP en el AS y que al nodo 12 de RAN no se le permite desestimar la decisión de la CN. Pero si el tráfico del plano de usuario se debe comunicar a través del UP del AS 18 durante los juegos olímpicos o algún otro evento menos prioritario, la indicación 20B de permiso de desestimación puede indicar que al nodo 12 de RAN se le permite desestimar la decisión de la CN.

Aún en otras realizaciones, la información puede referirse a la ubicación o tipo de ubicación particular del nodo 12 de RAN. Por ejemplo, si el nodo 12 de RAN está ubicado en un área pública o en alguna otra ubicación menos segura, las indicaciones 20A, 20B pueden indicar que la CN 10A ha decidido activar la seguridad 18S del UP en el AS y que al nodo 12 de RAN no se le permite desestimar la decisión de la CN. Pero si el nodo 12 de RAN está ubicado en unas instalaciones aisladas físicamente o en alguna otra ubicación más segura, la indicación 20B de permiso de desestimación puede indicar que al nodo 12 de RAN se le permite desestimar la decisión de la CN.

Si al nodo 12 de RAN se le permite desestimar la decisión de la CN, el propio nodo 12 de RAN puede tener en cuenta cierta información al decidir de forma autónoma si activar o no la seguridad 18S del UP en el AS. Esta información puede referirse, por ejemplo, a la capacidad o conveniencia del nodo 12 de RAN para activar la seguridad del UP en el AS. Por ejemplo, la información puede reflejar el impacto de la activación de seguridad sobre el nivel de carga del nodo 12 de RAN, la eficiencia o la disponibilidad de energía en el nodo 12 de RAN, o sobre la carga, eficiencia o disponibilidad del uso de recursos de radiocomunicaciones en la RAN 10B. En algunas realizaciones, por ejemplo, el nodo 12 de RAN puede elegir no activar la seguridad 18S del UP en el AS si un alto nivel de carga o un bajo nivel de disponibilidad de energía en el nodo 16 de RAN o en los recursos de radiocomunicaciones en el sistema 10 sugieren

que dicha activación no es posible o deseable. A continuación, en un ejemplo particular, el nodo 12 de RAN puede configurarse para no activar la seguridad 18S del UP en el AS cuando el nivel de carga del nodo de RAN alcanza un cierto nivel considerado como sobrecarga, por ejemplo, debido a que presta servicio a un gran número de dispositivos de comunicaciones inalámbricas al mismo tiempo. En este caso, el nodo 12 de RAN prioriza la eficiencia computacional sobre la seguridad 18S del UP en el AS cuando la indicación 20B de permiso de desestimación permite que el nodo 12 de RAN así lo haga.

De manera alternativa o adicional, la información puede referirse a un modo del nodo 12 de RAN, tal como un modo de ahorro de energía, en el que el nodo 12 de RAN puede evitar la activación de la seguridad 18S del UP del AS. Por ejemplo, cuando el nodo 12 de RAN está funcionando en un modo de ahorro de energía, el nodo 12 de RAN puede no activar la seguridad 18S del UP del AS para priorizar la eficiencia de la batería sobre la seguridad 18S del UP del AS cuando la indicación 20B de permiso de desestimación permite que el nodo 12 de RAN así lo haga.

Aún en otras realizaciones, la información puede referirse a la autorización de la CN 10A para activar la seguridad 18S del plano de usuario en el AS. Por ejemplo, en algunas realizaciones donde las partes que son propietarias de y explotan la CN 10A y la RAN 10B son diferentes, múltiples redes centrales pueden compartir la misma RAN 10B. Esto puede significar que la parte RAN que comercializa servicios de RAN ha acordado diferentes políticas con cada una las partes CN que explotan redes centrales, y algunas partes CN pueden no estar autorizadas por la parte RAN para activar la seguridad del UP en el AS. En consecuencia, el nodo 12 de RAN puede no activar la seguridad 18S del plano de usuario en el AS si la CN 10A no está autorizada a activarla, por ejemplo, independientemente de la indicación 22 de permiso de desestimación.

Con independencia de la información particular de la CN 10A y la RAN 10B, el nodo 16 de CN y/o el nodo 16 de RAN pueden realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando de acuerdo con la indicación 20B de permiso de desestimación, al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede (o la CN 10A no está autorizada a) activar la seguridad 18S del UP del AS. La(s) acción(es) puede(n) incluir, por ejemplo, cancelar, rechazar o descartar una sesión de plano de usuario o establecimiento de sesión de plano de usuario. Esto impone efectivamente el cumplimiento de la decisión de la CN de activar la seguridad 18S del UP en el AS, o el cumplimiento de un requisito de que dicha seguridad 18S esté autorizada, de manera que su incumplimiento da como resultado la cancelación, rechazo o descarte de una sesión de UP o del establecimiento de una sesión de UP. Esto puede basarse en el razonamiento de que un UP de AS no seguro (o un UP de AS seguro pero no autorizado) es más perjudicial que ningún UP de AS en absoluto.

Sin embargo, en un esfuerzo por salvar la sesión de UP, la(s) acción(es) puede(n) incluir alternativamente (o en primer lugar) orientar un dispositivo de comunicaciones inalámbricas a un nodo de RAN diferente. Por ejemplo, cuando un dispositivo 14 de comunicaciones inalámbricas ha establecido o está estableciendo una sesión de plano de usuario con el nodo 12 de RAN, el nodo 12 de RAN puede transmitir señalización al dispositivo 14 la cual orienta el dispositivo 14 a un nodo de RAN diferente para establecer una sesión de plano de usuario con ese nodo de RAN diferente en su lugar. La señalización en algunas realizaciones incluye una indicación de motivo que indica el motivo de la orientación (por ejemplo, incapacidad o inconveniencia de la activación del UP en el AS en el nodo 16 de RAN). Con dicho motivo, el dispositivo 14 puede decidir si se conecta al otro nodo de RAN, o simplemente proceder con el nodo 12 de RAN sin seguridad del UP en el AS. Independientemente, el nodo 12 de RAN en algunas realizaciones selecciona el nodo de RAN diferente basándose en cierta información similar a la descrita anteriormente, pero con respecto al nodo de RAN diferente, es decir, para caracterizar la capacidad o conveniencia del nodo RAN diferente de activar la seguridad del UP en el AS. Por ejemplo, el nodo 12 de RAN puede seleccionar el nodo de RAN diferente basándose en información que describe el impacto de la activación de la seguridad sobre el nivel de carga del nodo de RAN diferente, sobre la eficiencia o disponibilidad de energía en el nodo de RAN diferente, o similares, por ejemplo, para seleccionar otro nodo de RAN que esté mejor capacitado o posicionado de otra manera para activar la seguridad del UP en el AS.

Al menos algunas realizaciones, entonces, garantizan ventajosamente que la seguridad 18S del UP en el AS se active o desactive selectivamente de una manera que tenga en cuenta holísticamente la información relevante distribuida por todo el sistema 10 entre la CN 10A y la RAN 10B. Esto a su vez puede garantizar que la seguridad 18S del UP del AS se active para el tráfico de plano de usuario, servicios o abonados que son lo suficientemente importantes como para justificar la imposición de esa activación, pero al mismo tiempo puede permitir que la RAN 10B, en algunas circunstancias, renuncie a la activación a favor de controlar su carga, su uso de recursos de radiocomunicaciones, su eficiencia energética o similares.

Obsérvese que la decisión de la CN y/o el hecho de si la decisión puede desestimarse (por ejemplo, la indicación 20A de activación y/o la indicación 22 de permiso de desestimación) en algunas realizaciones se establecen o son aplicables específicamente para una sesión de plano de usuario particular, es decir, sobre la base de cada sesión de UP específica. Por ejemplo, en algunas realizaciones, la CN decide si activar o no la seguridad 18S del UP en el AS para una sesión de UP particular y también señaliza si al nodo 16 de RAN se le permite desestimar esa decisión para la sesión de UP particular. De hecho, en estas y otras realizaciones, el nodo 16 de CN puede señalizar la indicación 22 de permiso de desestimación al nodo 12 de RAN durante un procedimiento para establecer una sesión de UP para un dispositivo 14 de comunicaciones inalámbricas particular (por ejemplo, dentro de un procedimiento o mensaje de establecimiento de sesión de unidades de datos por paquetes, PDU). La indicación 22 de permiso de desestimación

y la indicación 20A de activación pueden incluso incluirse en el mismo mensaje señalizado hacia la RAN 10B. En estas y otras realizaciones, a continuación, la indicación 22 de permiso de desestimación puede ser específica de la indicación 20A de activación para indicar si la CN 10A permite o no que el nodo 16 de RAN desestime la decisión indicada específicamente por la indicación 20A de activación.

En otras realizaciones, por el contrario, la decisión de la CN y/o el hecho de si la decisión puede desestimarse (por ejemplo, la indicación 20A de activación y/o la indicación 22 de permiso de desestimación) en algunas realizaciones se establecen o son aplicables para una categoría particular de sesiones de plano de usuario, para cualquier sesión de plano de usuario gestionada por un nodo de CN particular, y/o para cualquier sesión de plano de usuario asociada a un segmento (*slice*) de red particular. En estas y otras realizaciones, la indicación 20A de activación y/o la indicación 22 de permiso de desestimación pueden ser señalizadas por la CN 10A, obtenidas por el nodo 12 de RAN, y/o preconfiguradas en el nodo 12 de RAN antes del establecimiento de una sesión de plano de usuario particular para la cual la seguridad 18S del UP en el AS se activa o desactiva según dichas indicaciones 20A, 22. La(s) indicación(es) 20A, 22 puede(n) especificar, por ejemplo, ciertas condiciones bajo las cuales se aplican la(s) indicación(es), por ejemplo, para formar una política granular para su aplicación. Por ejemplo, la indicación 22 de permiso de desestimación puede especificar que se aplica para un tipo particular de seguridad del UP en el AS (por ejemplo, protección de confidencialidad, pero no de integridad), para un período de tiempo particular (por ejemplo, domingos), para un nivel de carga particular del nodo 16 de RAN (por ejemplo, cuando el número de dispositivos 14 de comunicaciones inalámbricas conectados supera los 10.000), o similares. En estos y otros ejemplos, a continuación, el nodo 16 de RAN puede evaluar si se aplican indicaciones 20A, 22, o cuáles se aplican, para determinar si la seguridad 18S del UP en el AS se debe activar para una sesión de UP particular, una categoría particular de sesiones de UP, o similares.

Además, obsérvese que, en algunas realizaciones, el hecho de si la seguridad 18S del UP del AS se activa se refiere a si la seguridad 18S del UP del AS es aplicada por el nodo 12 de RAN con cualquier tipo de algoritmo, ya sea ese algoritmo un algoritmo no nulo o un algoritmo nulo que no aplica ninguna encriptación o protección en cuanto a integridad en la práctica. En estas y otras realizaciones, la indicación 22 de permiso de desestimación puede establecerse en función de si la seguridad 18S del UP en el AS se activará con un algoritmo nulo o no nulo, por ejemplo, para no permitir que el nodo 16 de RAN desestime la decisión de la CN si el nodo 16 de RAN simplemente se activa con un algoritmo nulo. Sin embargo, en otras realizaciones, el hecho de si la seguridad 18S del UP del AS se activa se refiere a si la seguridad 18S del UP del AS es aplicada por el nodo 12 de RAN con un algoritmo no nulo, es decir, si la seguridad 18S del UP del AS se activa de una manera que realmente aplica una encriptación y/o una protección en cuanto a integridad en la práctica.

En vista de las modificaciones y variaciones anteriores, la Figura 2A muestra un método 100 realizado por el nodo 16 de RAN para configurar la seguridad 18S del UP en el AS de acuerdo con algunas realizaciones. El método 100 incluye la obtención de una indicación 20A de activación que indica una decisión de la CN 10A sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS (Bloque 102). El método 100 también incluye obtener una indicación 22 de permiso de desestimación que indica si al nodo de RAN se le permite o no (por ejemplo, por parte de la CN 10A) desestimar la decisión de la CN 10A (Bloque 104).

En algunas realizaciones, el método 100 incluye además activar o no activar la seguridad 18S del UP en el AS, dependiendo de la indicación 20A de activación y de la indicación 22 de permiso de desestimación (Bloque 106). De manera alternativa o adicional, el método 100 puede incluir además realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando de acuerdo con la indicación 22 de permiso de desestimación, al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS (Bloque 108). Por ejemplo, la(s) acción(es) puede(n) incluir cancelar, rechazar o descartar una sesión de plano de usuario o un establecimiento de sesión de plano de usuario, u orientar un dispositivo 14 de comunicaciones inalámbricas a un nodo de RAN diferente.

La Figura 3A muestra correspondientemente un método 200 realizado por el nodo 16 de CN para configurar la seguridad 18S del UP en el AS de acuerdo con algunas realizaciones. El método 200 incluye la señalización de una indicación 20A de activación que indica una decisión de la CN 10A sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS (Bloque 202). El método 200 también incluye la señalización de una indicación 22 de permiso de desestimación que indica si al nodo de RAN se le permite o no (por ejemplo, por parte de la CN 10A) desestimar la decisión de la CN 10A (Bloque 204).

En algunas realizaciones, el método 200 puede incluir además realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando de acuerdo con la indicación 22 de permiso de desestimación, al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS (Bloque 206). Por ejemplo, la(s) acción(es) puede(n) incluir aumentar recursos disponibles en el nodo de RAN para la seguridad del plano de usuario en el AS y/o modificar la decisión y/o la indicación de permiso de desestimación para permitir que se establezca una sesión de plano de usuario sin la seguridad del plano de usuario en el AS (en lugar de cancelar, rechazar o descartar la sesión del plano de usuario).

La Figura 2B muestra un método 110 realizado por el nodo 16 de RAN para configurar la seguridad 18S del UP en el AS de acuerdo con otras realizaciones donde la señalización 20 indica la decisión de la CN y el hecho de si la decisión puede desestimarse. El método 110 incluye recibir señalización 20 que indica una decisión por parte de la CN 10A sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS y eso indica si al nodo de RAN se le permite o no (por ejemplo, por parte de la CN 10A) desestimar la decisión de la CN 10A (Bloque 112).

En algunas realizaciones, el método 110 incluye además activar o no activar la seguridad 18S del UP en el AS, dependiendo de la señalización 20 (Bloque 114). De manera alternativa o adicional, el método 110 puede incluir además realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS (Bloque 116). Por ejemplo, la(s) acción(es) puede(n) incluir cancelar, rechazar o descartar una sesión de plano de usuario o establecimiento de sesión de plano de usuario, u orientar un dispositivo 14 de comunicaciones inalámbricas a un nodo de RAN diferente.

La Figura 3B muestra correspondientemente un método 210 realizado por el nodo 16 de CN para configurar la seguridad 18S del UP en el AS de acuerdo con algunas realizaciones. El método 210 incluye tomar una decisión (de la CN) sobre si el nodo 16 de RAN debe activar o no la seguridad del UP en el AS (Bloque 212). El método 210 incluye además transmitir señalización 20 que indica una decisión de la CN 10A sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS y eso indica si al nodo de RAN se le permite o no (por ejemplo, por parte de la CN 10A) desestimar la decisión de la CN 10A (Bloque 214).

En algunas realizaciones, el método 210 puede incluir además realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS (Bloque 216). Por ejemplo, la(s) acción(es) puede(n) incluir aumentar recursos disponibles en el nodo de RAN para la seguridad del plano de usuario en el AS y/o modificar la decisión y/o la indicación de permiso de desestimación para permitir que se establezca una sesión de plano de usuario sin la seguridad del plano de usuario en el AS (en lugar de cancelar, rechazar o descartar la sesión del plano de usuario).

La Figura 2C muestra un método 120 realizado por el nodo 16 de RAN para configurar la seguridad 18S del UP en el AS de acuerdo todavía con otras realizaciones. El método 120 incluye recibir señalización 20 que indica si una decisión de la CN 10A de activar o no la seguridad 18S del plano de usuario en el AS es una orden que debe cumplir el nodo 16 de RAN o una preferencia cuya desestimación se le permite al nodo 16 de RAN (Bloque 122).

En algunas realizaciones, el método 120 incluye además activar o no activar la seguridad 18S del UP en el AS, dependiendo de la señalización 20 (Bloque 124). De manera alternativa o adicional, el método 110 puede incluir además realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS (Bloque 126). Por ejemplo, la(s) acción(es) puede(n) incluir cancelar, rechazar o descartar una sesión de plano de usuario o establecimiento de sesión de plano de usuario, u orientar un dispositivo 14 de comunicaciones inalámbricas a un nodo de RAN diferente.

La Figura 3C muestra correspondientemente un método 220 realizado por el nodo 16 de CN para configurar la seguridad 18S del UP en el AS de acuerdo con otras realizaciones. El método 220 incluye tomar una decisión (de la CN) sobre si el nodo 16 de RAN debe activar o no la seguridad del UP en el AS (Bloque 222). El método 220 incluye además transmitir señalización 20 que indica si una decisión de la CN 10A para activar o no la seguridad 18S del plano de usuario en el AS es una orden que debe cumplir el nodo 16 de RAN o una preferencia cuya desestimación se le permite al nodo 16 de RAN (Bloque 224).

En algunas realizaciones, el método 220 puede incluir además realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS (Bloque 226). Por ejemplo, la(s) acción(es) puede(n) incluir aumentar recursos disponibles en el nodo de RAN para la seguridad del plano de usuario en el AS y/o modificar la decisión y/o la indicación de permiso de desestimación para permitir que se establezca una sesión de plano de usuario sin la seguridad del plano de usuario en el AS (en lugar de cancelar, rechazar o descartar la sesión del plano de usuario).

La Figura 4 muestra un método 300 realizado por un dispositivo 14 de comunicaciones inalámbricas según algunas realizaciones. El método 300 incluye, como respuesta a que un nodo 16 de RAN en la RAN 10B no pueda activar la seguridad 18S del UP en el AS de acuerdo con una decisión de la CN 10A de que al nodo de RAN no se le permite (por ejemplo, por parte de la CN 10A) la desestimación, recibir señalización que orienta el dispositivo 14 de comunicaciones inalámbricas para establecer una sesión de plano de usuario con un nodo de RAN diferente (Bloque

310). El método 300 en algunas realizaciones también puede incluir intentar establecer una sesión de plano de usuario con el nodo de RAN diferente de acuerdo con la señalización recibida (Bloque 320).

Obsérvese además que los aparatos descritos anteriormente pueden llevar a cabo los métodos del presente documento y cualquier otro procesado mediante la implementación de cualesquiera medios, módulos, unidades o circuitería funcionales. En una realización, por ejemplo, los aparatos comprenden circuitos o circuitería respectivos configurados para realizar las etapas mostradas en las figuras de los métodos. Los circuitos o circuitería a este respecto pueden comprender circuitos dedicados a realizar cierto procesado funcional y/o uno o más microprocesadores en combinación con memoria. Por ejemplo, la circuitería puede incluir uno o más microprocesadores o microcontroladores, así como otro *hardware* digital, que puede incluir procesadores de señal digital (DSPs), lógica digital de propósito especial y similares. La circuitería de procesado puede configurarse para ejecutar código de programa almacenado en memoria, la cual puede incluir uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria *flash*, dispositivos de almacenamiento óptico, etcétera. El código de programa almacenado en la memoria puede incluir instrucciones de programa para ejecutar uno o más protocolos de telecomunicaciones y/o de comunicaciones de datos, así como instrucciones para llevar a cabo una o más de las técnicas descritas en la presente, en varias realizaciones. En realizaciones que utilizan memoria, la memoria almacena código de programa que, cuando es ejecutado por el procesador o procesadores, lleva a cabo las técnicas descritas en este documento.

Un nodo 16 de red central según se ha descrito anteriormente puede implementar una función de acceso y movilidad (AMF) y/o una función de gestión de sesiones (SMF) al menos en algunas realizaciones. Independientemente, el nodo 16 de red central puede llevar a cabo cualquiera procesado de este documento mediante la implementación de cualesquiera medios o unidades funcionales. En una realización, por ejemplo, el nodo 16 de red central comprende circuitos o circuitería respectivos configurados para realizar cualquiera de las etapas mostradas en la Figura 3. Los circuitos o circuitería a este respecto pueden comprender circuitos dedicados a realizar cierto procesado funcional y/o uno o más microprocesadores en combinación con memoria. En realizaciones que utilizan memoria, que puede comprender uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria *flash*, dispositivos de almacenamiento óptico, etcétera, la memoria almacena código de programa que, cuando es ejecutado por el procesador o procesadores, lleva a cabo las técnicas descritas en este documento.

La Figura 5A ilustra el nodo 400 de red central de acuerdo con una o más realizaciones. El nodo 400 de red central se puede corresponder, por ejemplo, con el nodo 16 de red central aquí descrito, de manera que lleva a cabo la señalización 20 y/u otro procesado del presente documento. Independientemente, tal como se muestra, el nodo 400 de red central incluye circuitería 410 de procesado y circuitería 420 de comunicación. El circuito 420 de comunicación está configurado para transmitir y/o recibir información hacia y/o desde otro u otros nodos, por ejemplo, a través de cualquier tecnología de comunicación. La circuitería 410 de procesado está configurada para realizar el procesado descrito anteriormente, por ejemplo, en la Figura 3A, 3B y/ó 3C, tal como mediante la ejecución de instrucciones almacenadas en la memoria 430. La circuitería 410 de procesado a este respecto puede implementar ciertos medios, unidades, o módulos funcionales.

La Figura 5B ilustra el nodo 500 de red central implementado de acuerdo con otra u otras realizaciones. El nodo 500 de red central se puede corresponder, por ejemplo, con el nodo 16 de red central descrito en la presente de manera que lleva a cabo la señalización 20 y/u otro procesado de la presente. Independientemente, tal como se muestra, el nodo 500 de red central implementa varios medios, unidades o módulos funcionales, por ejemplo, a través de la circuitería 410 de procesado de la Figura 5A y/o mediante código de *software*. Estos medios, unidades o módulos funcionales, por ejemplo, para implementar cualquiera de las etapas de la Figura 3A, 3B y/ó 3C, incluyen, por ejemplo, una unidad o módulo 510 de señalización para transmitir señalización 20. En algunas realizaciones, por ejemplo, para implementar el método 100 de la Figura 3A, la unidad o módulo 510 de señalización está destinada a señalizar una indicación 20A de activación que indica una decisión por parte de la CN 10A sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS, y a señalizar una indicación 22 de permiso de desestimación que indica si al nodo de RAN se le permite o no (por ejemplo, por parte de la CN 10A) desestimar la decisión de la CN 10A. También se puede incluir una unidad o módulo 520 de decisión para tomar la decisión sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del UP en el AS y/o para decidir si al nodo 16 de RAN se le permite o no desestimar esa decisión.

De manera similar, el equipo de red de radiocomunicaciones según se ha descrito anteriormente puede realizar cualquier procesado de la presente implementando cualesquiera medios o unidades funcionales. En una realización, por ejemplo, el equipo de red de radiocomunicaciones comprende circuitos o circuitería respectivos configurados para realizar cualquiera de las etapas mostradas en cualquiera de las Figuras 2A-2C. Los circuitos o circuitería a este respecto pueden comprender circuitos dedicados a realizar cierto procesado funcional y/o uno o más microprocesadores en combinación con memoria. En realizaciones que utilizan memoria, que puede comprender uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria *flash*, dispositivos de almacenamiento óptico, etcétera, la memoria almacena código de programa que, cuando es ejecutado por el procesador o procesadores, lleva a cabo las técnicas descritas en este documento.

La Figura 6A ilustra el nodo 600 de red de radiocomunicaciones de acuerdo con una o más realizaciones. El nodo 600 de red de radiocomunicaciones se puede corresponder con el nodo 12 de red de radiocomunicaciones descrito en la Figura 1. Tal como se muestra, el nodo 600 de red de radiocomunicaciones incluye circuitería 610 de procesado y circuitería 620 de comunicaciones. La circuitería 620 de comunicaciones está configurada para transmitir y/o recibir información a y/o de otro u otros nodos, por ejemplo, a través de cualquier tecnología de comunicación. La circuitería 610 de procesado está configurada para realizar el procesado descrito anteriormente, por ejemplo, en la Figura 2A, 2B y/ó 2C, tal como mediante la ejecución de instrucciones almacenadas en la memoria 630. La circuitería 610 de procesado a este respecto puede implementar ciertos medios, unidades, o módulos funcionales.

La Figura 6B ilustra un nodo 700 de red de radiocomunicaciones implementado de acuerdo con otra u otras realizaciones. El nodo 700 de red de radiocomunicaciones se puede corresponder con el nodo 12 de red de radiocomunicaciones descrito en la Figura 1. Tal como se muestra, el nodo 700 de red de radiocomunicaciones implementa varios medios, unidades o módulos funcionales, por ejemplo, a través de la circuitería 610 de procesado de la Figura 6A y/o mediante código de *software*. Estos medios, unidades o módulos funcionales, por ejemplo, para implementar cualquiera de las etapas de la Figura 2A, incluyen, por ejemplo, una unidad o módulo 1010 de obtención para obtener una indicación 20A de activación que indica una decisión de la CN 10A sobre si el nodo 16 de RAN debe activar o no la seguridad 18S del plano de usuario en el AS, y una unidad o módulo 720 de obtención de indicaciones de permiso de desestimación para obtener una indicación 22 de permiso de desestimación que indica si al nodo de RAN se le permite o no (por ejemplo, por parte de la CN 10A) desestimar la decisión de la CN 10A. También se puede incluir una unidad o módulo 730 de control de seguridad para activar o desactivar la seguridad 18S del UP en el AS, dependiendo de la indicación 20A de activación y de la indicación 22 de permiso de desestimación. Además, se puede incluir una unidad o módulo 740 de acciones para realizar una o más acciones cuando la decisión de la CN 10A es que el nodo 16 de RAN debe activar la seguridad 18S del plano de usuario en el AS, cuando de acuerdo con la indicación 22 de permiso de desestimación, al nodo 16 de RAN no se le permite desestimar la decisión de la CN 10A, y cuando el nodo 16 de RAN no puede, o la CN 10A no está autorizada a, activar la seguridad 18S del plano de usuario en el AS.

La Figura 7A ilustra un dispositivo 14 de comunicaciones inalámbricas (por ejemplo, un UE) tal como se implementa de acuerdo con una o más realizaciones. Tal como se muestra, el dispositivo 14 de comunicaciones inalámbricas incluye circuitería 800 de procesado y circuitería 810 de comunicación. La circuitería 810 de comunicación (por ejemplo, circuitería de radiocomunicaciones) está configurada para transmitir y/o recibir información hacia y/o desde otro u otros nodos, por ejemplo, a través de cualquier tecnología de comunicación. Dicha comunicación puede producirse a través de una o más antenas que son o bien internas o bien externas con respecto al dispositivo 14 de comunicaciones inalámbricas. La circuitería 800 de procesado está configurada para realizar el procesado descrito anteriormente, tal como ejecutando instrucciones almacenadas en la memoria 820. La circuitería 800 de procesado a este respecto puede implementar ciertos medios, unidades o módulos funcionales.

La Figura 7B ilustra un diagrama de bloques esquemático del dispositivo 14 de comunicaciones inalámbricas según todavía otras realizaciones. Tal como se muestra, el dispositivo 14 de comunicaciones inalámbricas implementa varios medios, unidades o módulos funcionales, por ejemplo, a través de la circuitería 800 de procesado de la Figura 7A y/o mediante código de *software*. Estos medios, unidades o módulos funcionales, por ejemplo, para implementar el(los) método(s) de este documento, incluyen, por ejemplo, una unidad o módulo 900 de señalización para recibir señalización que orienta el dispositivo 14 de comunicaciones inalámbricas con el fin de establecer una sesión de plano de usuario con un nodo de RAN diferente. También se puede incluir una unidad o módulo 910 de orientación para intentar establecer una sesión de plano de usuario con el nodo de RAN diferente de acuerdo con la señalización recibida.

Aquellos versados en la materia también apreciarán que las realizaciones del presente documento incluyen además programas informáticos correspondientes.

Un programa informático comprende instrucciones que, cuando se ejecutan en al menos un procesador de un aparato configurado para su uso en un sistema de comunicaciones inalámbricas, hacen que el aparato lleve a cabo cualquier procesado de los respectivos descritos anteriormente. Un programa informático a este respecto puede comprender uno o más módulos de código correspondientes a los medios o unidades descritos anteriormente.

Realizaciones incluyen además un soporte que contiene dicho programa informático. Este soporte puede comprender uno de una señal electrónica, señal óptica, señal de radiocomunicaciones o soporte de almacenamiento legible por ordenador.

A este respecto, realizaciones del presente documento también incluyen un producto de programa informático almacenado en un soporte (de almacenamiento o grabación) no transitorio legible por ordenador y que comprende instrucciones que, cuando se ejecutan mediante un procesador de un aparato, consigue que el aparato funcione como se ha descrito anteriormente.

Realizaciones incluyen además un producto de programa informático que comprende fragmentos de código de programa para realizar las etapas de cualquiera de las realizaciones del presente documento cuando el producto de

programa informático es ejecutado por un aparato. Este producto de programa informático puede almacenarse en un soporte de grabación legible por ordenador.

Aunque realizaciones anteriores se han descrito con respecto a la seguridad del plano de usuario en el AS, las realizaciones pueden extenderse igualmente a otros tipos de seguridad en el AS, por ejemplo, AS del plano de control, en la medida en que los otros tipos de seguridad en el AS sean opcionales para requerir una decisión con respecto a su activación.

A continuación se describirán realizaciones adicionales. Al menos algunas de estas realizaciones pueden describirse como aplicables en ciertos contextos y/o tipos de redes inalámbricas (por ejemplo, 5G) con fines ilustrativos, pero las realizaciones son aplicables de manera similar en otros contextos y/o tipos de redes inalámbricas no descritos explícitamente. Por consiguiente, las siguientes realizaciones pueden ser ejemplos particulares de, y/o combinables de otra manera con, las realizaciones anteriores.

La 3GPP TS 23.501 describe la arquitectura de red 5G. En la Figura 8 se muestra una versión básica simplificada de una red 5G.

El UE (Equipo de Usuario) 40 es un dispositivo móvil utilizado por el usuario para acceder de forma inalámbrica a la red. El UE 40 puede representar, por ejemplo, el dispositivo inalámbrico 14 de la Figura 1 implementado para una red 5G. La función de red de acceso de radiocomunicaciones (RAN) o estación base denominada gNB (Nodo B de Próxima Generación) 42 es responsable de proporcionar radiocomunicaciones inalámbricas al UE y conectar el UE a la red central. El gNB 42 puede representar, por ejemplo, el nodo 12 de RAN de la Figura 1 implementado para una red 5G. La función de red central denominada AMF (Función de Gestión de Acceso y Movilidad) 44 es responsable de administrar la movilidad del UE, entre otras responsabilidades. Otra función de red central denominada SMF (Función de Gestión de Sesiones) 48 es responsable de administrar la orientación de las sesiones y del tráfico del UE, entre otras responsabilidades. La SMF 48 puede representar el nodo 16 de CN de la Figura 1 tal como se implementa para una red 5G. Todavía otra función de la red principal denominada UPF (Función de Plano de Usuario) 46 es responsable de la interconexión a la red de datos, del encaminamiento y reenvío de paquetes, entre otras responsabilidades.

El UE 40 interactúa con el gNB 42 por vía aérea utilizando la interfaz de radiocomunicaciones. El tráfico de la interfaz de radiocomunicaciones comprende tanto tráfico del plano de control como tráfico del plano de usuario. El plano de control de radiocomunicaciones también se denomina RRC (Control de Recursos de Radiocomunicaciones). El gNB 42 a su vez interactúa con la AMF 44 utilizando la interfaz denominada N2. La interfaz entre la AMF 44 y la SMF 48 se denomina N11. De modo similar, el gNB 42 y la UPF 46 interactúan usando la interfaz denominada N3. No existe una interfaz directa entre el gNB 42 y la SMF 48, con lo cual interactúan a través de la AMF 44.

Los aspectos lógicos entre el UE 40 y la AMF 44 se denominan NAS (estrato sin acceso) y al correspondiente entre el UE 40 y el gNB 42 se le hace referencia como AS (estrato de acceso). De manera correspondiente, la seguridad de la comunicación (plano de control y plano de usuario, si corresponde) se conoce como seguridad en el NAS y seguridad en el AS, respectivamente. La seguridad en el AS comprende la protección de la confidencialidad y la integridad del tráfico tanto del plano de control (es decir, el RRC) como del plano de usuario.

En el sistema LTE (Evolución a Largo Plazo, conocido popularmente como 4G), la seguridad en el AS es obligatoria tanto para el RRC como para el plano del usuario. Significa que tanto la confidencialidad como la protección de la integridad están activadas para el RRC y la confidencialidad está activada para el plano de usuario. No hay soporte para la protección de integridad del plano de usuario en LTE. Obsérvese que en LTE existen algoritmos de encriptación nula e integridad nula que no encriptan ni protegen en cuanto a integridad el tráfico de RRC o del plano de usuario en la práctica. Pero de acuerdo con algunas realizaciones, estos algoritmos nulos son solo otro tipo de algoritmo y, por lo tanto, se sigue diciendo que la seguridad en el AS está activada, es decir, activada usando algoritmos nulos.

En el sistema 5G, la seguridad en el AS es obligatoria para el RRC pero es probable que sea opcional para el plano del usuario. Significa que tanto la confidencialidad como la protección de integridad se activarán para el RRC; sin embargo, la confidencialidad y la protección de la integridad probablemente serán opcionales para el plano del usuario.

En el sistema LTE, dado que la activación de seguridad en el AS es obligatoria para el tráfico tanto del RRC como del plano de usuario, es suficiente con tener un solo procedimiento que active la seguridad en el AS tanto para el tráfico tanto del RRC como del plano de usuario. Ese procedimiento se conoce como procedimiento de orden de modo de seguridad en el AS (véase la Cláusula 7.2.4.5 en la 3GPP TS 33.401). Es probable que esto ya no sea así en el sistema 5G, porque la activación de seguridad en el AS es opcional para el tráfico del plano del usuario. No está claro si el procedimiento de orden de modo de seguridad en el AS es el procedimiento correcto o no para la activación de la seguridad del plano de usuario en el AS, y en caso negativo, cuál es el procedimiento correcto y qué nodo o función es responsable del mismo. Por lo tanto, la activación de la seguridad en el AS presenta un nuevo desafío para el sistema 5G.

Algunas realizaciones del presente documento proporcionan un mecanismo en el que la seguridad del plano de usuario en el AS (es decir, la protección de la confidencialidad y la integridad) se activa según lo previsto. Las realizaciones pueden proporcionar un mecanismo robusto para la activación de la seguridad del plano de usuario en el AS. La

robustez se introduce al ofrecer protección contra una situación en la que la seguridad del plano de usuario en el AS no se activa, aun cuando se haya tomado la decisión de activar la seguridad del plano de usuario en el AS.

De manera general, a continuación, realizaciones del presente documento pueden abordar un desafío por el que, cuando la CN envía una indicación a la RAN de que se debe activar la seguridad del plano de usuario en el AS, la RAN puede no ser capaz de cumplirla por motivos, tales como, por ejemplo, estar sobrecargada en ese momento o en modo de ahorro de energía y no puede activar la protección de integridad o la confidencialidad en aras de la eficiencia computacional o de la batería, etcétera. Algunas realizaciones proponen que la RAN pueda desestimar la decisión tomada por la CN sobre la activación de la seguridad del plano de usuario en el AS, solo si le está permitido hacerlo por la CN.

Los motivos de dichas realizaciones son los siguientes. La CN, y no la RAN, tiene acceso a las reglas de política de red o reglas de política de suscripción en función de las cuales la CN toma la decisión de activar o no la seguridad del plano de usuario en el AS. Por lo tanto, la RAN no está en condiciones de decidir por sí sola si la decisión de la CN puede desestimarse o no. Por ejemplo, si la CN ha decidido activar la seguridad del plano de usuario en el AS para UEs que pertenecen a los cuerpos de seguridad, sería devastador si la RAN, solo en función de su condición local, desestimase la decisión de la CN y no activase la seguridad del plano de usuario en el AS. Además, tampoco es suficiente con que la RAN informe a la CN de que la RAN desestimó su decisión. La CN obtendrá la información de que la activación de seguridad del plano de usuario en el AS no se activó, pero puede ser demasiado tarde antes de que la CN pueda adoptar alguna medida correctora, por ejemplo datos de enlace ascendente/enlace descendente ya enviados por vía aérea. En otras palabras, el daño podría producirse ya antes de que la CN tome otra decisión. Por lo tanto, algunas realizaciones solo consideran aceptable que la CN tenga la última palabra sobre si su decisión puede ser desestimada o no por la RAN. Esto podría llevarse a cabo de muchas maneras, por ejemplo, la CN envía una indicación (desestimación permitida o no) a la RAN junto con la decisión de activar la seguridad del plano de usuario en el AS, la CN envía una indicación (desestimación permitida o no) a la RAN en la configuración del contexto inicial de NGAP entre la RAN y la CN, preconfigurándose la RAN con una indicación (desestimación permitida o no para cierto tipo de sesiones o UEs), etcétera.

Por ejemplo, uno de los métodos llevado a cabo por un gNB 42 para configurar la seguridad del plano de usuario en un estrato de acceso (AS) puede comprender en algunas realizaciones: (i) Obtener una indicación donotOverrule de una SMF 48, que indica si al gNB 42 se le permite o no desestimar una primera indicación, es decir, la indicación de la SMF para la activación de la seguridad del plano de usuario en el AS; (ii) Obtener la primera indicación de la SMF 48, que es la indicación de la SMF para la activación de la seguridad del plano de usuario en el AS; y (iii) Determinar en función de la indicación donotOverrule si desestimar o no la primera indicación.

En algunas realizaciones, el método puede comprender además determinar que no se puede cumplir con la primera indicación.

De manera alternativa o adicional, la indicación donotOverrule y la primera indicación pueden obtenerse juntas. Por ejemplo, la indicación donotOverrule y la primera indicación pueden indicarse en conjunto mediante una indicación combinada que al mismo tiempo indica la indicación de la SMF para la activación de la seguridad del plano de usuario en el AS e indica si al gNB 42 se le permite desestimar o no la primera indicación.

En algunas realizaciones, el método puede comprender además adoptar medidas.

De forma más detallada, obsérvese que además del gNB 42, la RAN en 5G también constará de eNB de la próxima generación (ng-eNB), donde eNB (Nodo B E-UTRAN o Nodo B Evolucionado) significa estaciones base pertenecientes al LTE. Sin embargo, dicha distinción no es muy importante a efectos de esta exposición y, por lo tanto, la exposición se refiere solo al gNB 42. Esto es así para mayor claridad de la descripción y no para limitar realizaciones limitantes del presente documento. También obsérvese que la seguridad del plano de usuario en el AS comprende la confidencialidad del plano de usuario y la protección de integridad del plano de usuario. Sin embargo, dicha distinción no es muy importante a efectos de esta exposición y, por lo tanto, la exposición generalmente se referirá a la seguridad del plano del usuario en el AS, por motivos de claridad de la descripción y no para limitar realizaciones de este documento. Además, el término nodo puede designar un nodo físico o una función en la red.

Como se ha descrito anteriormente, en el sistema 5G, es probable que la activación de la seguridad del plano de usuario en el AS sea opcional. El primer desafío en la activación de la seguridad del plano de usuario en el AS es la decisión de qué nodo tiene el control de la activación. Dado que la seguridad del plano de usuario en el AS termina en el gNB 42, el gNB 42 controla la activación de acuerdo con algunas realizaciones. Sin embargo, el gNB 42 es un nodo de RAN y no tiene acceso a las reglas de política de red o reglas de política de suscripción que residen en la red central. Por lo tanto, el gNB 42 no puede ser el nodo que decide si la seguridad del plano de usuario en el AS para un UE 40 particular se debe activar o no. La SMF 48, por otro lado, es un nodo de red central y tiene acceso a las reglas de política. La SMF 48 también es el nodo responsable de la gestión de sesiones del plano de usuario. Por lo tanto, la SMF 48 según algunas realizaciones es el nodo que decide si la seguridad del plano de usuario en el AS para un UE 40 particular se debe activar o no. Aunque en las realizaciones descritas se hace referencia a la SMF 48, algún otro nodo de red central, por ejemplo, la AMF 46, puede decidir en su lugar la activación de seguridad del plano de usuario en el AS en otras realizaciones.

Según algunas realizaciones, la SMF 48 envía una primera indicación al gNB 42 (a través de la AMF 46) sobre la activación de la seguridad del plano de usuario en el AS. A continuación, el gNB 42 activa o no activa la seguridad del plano de usuario en el AS en función de la primera indicación recibida de la SMF 48. Las Figuras 9 y 10 ilustran adicionalmente los flujos de señalización, los procedimientos, los mensajes y los campos utilizados entre la SMF 48 y el gNB 42 para dicha primera indicación (por ejemplo, SMF_RUS_Pre). Obsérvese que las Figuras 9 y 10 solo describen la primera indicación; no describen ni explican ninguna indicación doNotOverrule, la cual se describirá después de las Figuras 9 y 10. En realidad las Figuras 9 y 10 ayudan, en cambio, a ilustrar un problema que surge al usar solo la primera indicación (por ejemplo, SMF_RUS_Pre).

En las Figuras 9 y 10, se supone que hay una capa de protección que admite integridad y encriptación (o cifrado) para el Plano de Usuario (UP) entre el UE y la RAN, es decir, el gNB. Cada vez que se menciona la encriptación o la integridad, esto significa, respectivamente, la encriptación o la característica de protección de integridad en esta capa de protección. Actualmente en el LTE esa capa de protección se materializa mediante el protocolo PDCP. Se espera que en Sistemas de Próxima Generación, la misma capa de protección se materialice también posiblemente mediante una versión mejorada del mismo protocolo, es decir, PDCP.

La red controla la protección del UP en la interfaz de radiocomunicaciones entre el UE y la RAN. Por control se entiende la activación o desactivación de cualquiera de entre la integridad o la encriptación. La granularidad de dicho control podría situarse en el nivel de los Segmentos de Red o incluso de las Sesiones de PDU. Es decir, la red aplica los controles de manera similar a todos los Portadores de Radiocomunicaciones que transportan el UP de manera específica para cada Segmento de Red o incluso posiblemente de manera específica para cada sesión de PDU.

Esta característica de control podría realizarse mediante un mecanismo de negociación entre la red y el UE donde el UE puede indicar su preferencia para activar o desactivar encriptación o la integridad en diferentes niveles de granularidad. Es decir, por Segmento de Red o por sesión de PDU.

Las preferencias del UE pueden almacenarse en la UDM, es decir, incluirse en la información de suscripción. También pueden estar preconfiguradas en el UE. La red doméstica puede ayudar en la toma de decisiones indicando a la red de servicio qué controles son preferibles y en qué nivel de granularidad.

La red visitada tiene que tomar una decisión de política sobre si se usará o no la terminación de encriptación y/o de integridad, según la indicación recibida de la red doméstica, la preferencia del UE y la política configurada para la red visitada (por ejemplo, en la SMF). La red central podría indicar al UE en la capa NAS el resultado de dicha decisión.

La red central tiene que informar a la RAN si se usará o no la encriptación y/o la integridad, por ID de Segmento o por Sesión de PDU. Esta información se envía sobre la interfaz N2 entre la red central y la RAN.

La RAN podría desestimar dicha decisión o tomar su propia decisión en función de la preferencia del UE recibida de la red central y posiblemente otra información.

Si no se cumplen las preferencias del UE, a continuación el UE puede realizar una acción como respuesta. La acción podría ser conectarse a otro gNB/eNB, o el UE podría abstenerse de usar una determinada aplicación.

Cuando el UE se mueve en la red y cambia el punto de conexión a la red (es decir, en eventos de movilidad, traspaso o conectividad dual), la información de preferencia del UE y de decisión de política de la red tiene que reenviarse en el lado de la red entre los nodos de red, por ejemplo entre dos estaciones base, o entre entidades de gestión de acceso. Ejemplos de dichas acciones son: (i) En caso de traspaso, la entidad de gestión de acceso (AMF) de origen informa a la AMF de destino; (ii) En un traspaso de Xn entre dos estaciones base, la estación base de origen tiene que informar a la estación base de destino si habilitar o deshabilitar la encriptación y/o la protección de integridad del UP posiblemente de manera específica para cada segmento/sesión de PDU. Esta información podría enviarse en la interfaz Xn desde el nodo de origen al nodo de destino; (iii) En la conectividad dual entre dos estaciones base, la estación base maestra tiene que informar a la estación base secundaria por DRB si habilitar o deshabilitar la encriptación y/o la protección de integridad de UP. Esta información podría enviarse sobre la interfaz Xn desde la estación base maestra a la estación base secundaria.

Considérese en primer lugar un establecimiento de sesión de PDU (una variante generalizada). En este caso, US_Pre indica la preferencia de seguridad del UP de la RAN, UE_RUS_Pre indica la preferencia del UE sobre la seguridad del UP de la RAN, SMF_RUS_Pre representa la preferencia de la entidad de gestión de sesiones sobre la seguridad del UP de la RAN, HN_Pre representa la preferencia de la red doméstica sobre la seguridad del UP (esta preferencia puede indicar la terminación de la seguridad del UP en la RAN o en la CN en la red de servicio), HN_Dec indica la decisión de la red doméstica sobre la seguridad del UP terminada en el hogar, SN_Policy indica las reglas de política de la red de servicio relacionadas con la negociación, y la política de seguridad del UP utilizada como valor por defecto en la RAN, RUS_Dec indica la decisión de seguridad del UP de la RAN tomada por la RAN y CUS_Dec indica la decisión de terminación de seguridad del UP de la CN.

A continuación, en referencia a la Figura 9, se muestra un Establecimiento de Sesión de PDU solicitado por un UE para seguimiento sin itinerancia e itinerante con desvío local. El procedimiento supone que el UE ya se ha registrado en la AMF, con lo cual la AMF ya ha recuperado los datos de suscripción de usuario del UDM.

Etapa 1: De UE a AMF: Solicitud de Establecimiento de Sesión de PDU (opcional: UE_RUS_Pre). El UE opcionalmente indica su preferencia de seguridad del plano de usuario de la RAN. La preferencia puede ser: Opcional: UE_RUS_Pre: usar/no usar encriptación de datos de UP que terminan en la RAN; y Opcional: UE_RUS_Pre: usar/no usar protección de integridad de datos de UP que terminan en la RAN. Por ejemplo, si el UE admite un tipo de segmento IoT, a continuación el UE podría indicar para ese tipo de segmento IoT su preferencia sobre si usar o no encriptación o protección de integridad, o las dos, de datos de UP que terminan en la RAN, para esta ID de Sesión de PDU particular. O si el UE está autorizado a acceder a la red de datos A (identificador de segmento), a continuación el UE podría indicar para ese identificador de segmento su preferencia de usar encriptación o protección de integridad o las dos para datos de UP terminados en la RAN. O si el UE es un UE de IoT, a continuación el UE podría indicar que se prefiere que todos los datos de UP utilicen tanto la encriptación como la protección de integridad para datos de UP terminados en la RAN.

Etapa 2: La AMF determina que el mensaje se corresponde con una solicitud de una nueva Sesión de PDU basada en el ID de Sesión de PDU que no se utiliza para ninguna Sesión de PDU existente(s) del UE. La AMF selecciona una SMF como se describe en la TS 23.501, cláusula 6.3.2.

Etapa 3: De AMF a SMF: Solicitud de SM con Solicitud de Establecimiento de Sesión de PDU (opcional: UE_RUS_Pre, opcional: SN_Policy). La AMF reenvía la preferencia del UE a la SMF. La AMF puede añadir información de política al mensaje: Opcional: SN_policy: la AMF podría indicar a la SMF la información de política si a la SMF se le permite solicitar un cambio en la seguridad de la RAN; y Opcional: SN_policy: la AMF también podría indicar los valores de la política de seguridad por defecto a la SMF (por ejemplo, se usa encriptación en la RAN, no se usa integridad en la RAN).

Etapa 4a: SMF a UDM: Solicitud de Datos de Suscripción (ID Permanente de Abonado, DNN). La SMF puede tener una política local común que se aplica a todos los UEs que acceden al segmento de red relacionado con la terminación de la seguridad del UP. En este caso, puede que no se requiera del UDM la información de política. Si no existe una política local común, y la SMF aún no ha recuperado los datos de suscripción relacionados con la SM para el UE relacionado con el DNN, la SMF solicita estos datos de suscripción.

Etapa 4b: UDM a SMF: Respuesta de Datos de Suscripción (opcional: HN_Pre, OR opcional: HN_Dec). El UDM puede indicar a la SMF la preferencia de la red doméstica relacionada con la seguridad del UP terminada en la RAN o la decisión sobre la seguridad del UP terminada en la red doméstica. La preferencia de la red doméstica (HN_Pre) puede ser específica de la seguridad del UP de la RAN, por ejemplo Opcional: el UDM indica en sus datos de suscripción si debe usarse o no la encriptación del UP que termina en la RAN, o si esto es indiferente. Opcional: el UDM indica en sus datos de suscripción si debe usarse o no la protección de integridad del UP que termina en la RAN, o si esto es indiferente. La preferencia de la red doméstica (HN_Pre) también puede ser específica de la terminación del UP en la CN, por ejemplo Opcional: El UDM indica que la encriptación del UP y/o la integridad del UP deben terminarse en la CN en la red de servicio. La decisión de la red doméstica (HN_Dec) es específica de la terminación de la seguridad del UP en la red doméstica, por ejemplo Opcional: El UDM indica que la encriptación del UP y/o la integridad del UP deben terminarse en la CN en la red doméstica.

Etapa 5: SMF a DN a través de UPF: Si la SMF tiene que autorizar/autenticar el establecimiento de la sesión de PDU como se describe en la cláusula 5.6.6 de la TS 23.501, la SMF selecciona una UPF como se describe en la TS 23.501 cláusula 6.3.3 y activa la autenticación/autorización del establecimiento de sesión de PDU. Si la autenticación/autorización de establecimiento de sesión de PDU falla, la SMF termina el procedimiento de establecimiento de sesión de PDU e indica un rechazo al UE.

Etapa 6a: Si se implementa un PCC dinámico, la SMF realiza la selección de la PCF.

Etapa 6b: La SMF puede iniciar el Establecimiento de Sesión de PDU-CAN hacia la PCF para obtener las Reglas de PCC por defecto para la Sesión de PDU.

Etapa 7: La SMF selecciona un modo de SSC para la Sesión de PDU.

Etapa 8: Si se implementa un PCC dinámico y el Establecimiento de Sesión de PDU-CAN no se realizó en la etapa 5, la SMF inicia el Establecimiento de Sesión de PDU-CAN hacia la PCF para obtener las Reglas de PCC por defecto para la Sesión de PDU.

Etapa 9: Si no se realizó la etapa 5, la SMF inicia un procedimiento de Establecimiento de Sesión N4 con la UPF seleccionada, de lo contrario, inicia un procedimiento de Modificación de Sesión N4 con la UPF seleccionada.

Etapa 9a: la SMF envía una Solicitud de Establecimiento/Modificación de Sesión N4 a la UPF y proporciona Reglas de notificación, fiscalización y detección de paquetes para su instalación en la UPF para esta sesión de PDU.

Etapa 9b: La UPF lo confirma enviando una Respuesta de Establecimiento/Modificación de Sesión N4.

Etapa 10: SMF a AMF: Ack de Solicitud de SM con opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec, (Aceptación de Establecimiento de Sesión de PDU (opcional: SMF_RUS_Pre OR opcional:

SMF_CUS_Dec OR opcional: HN_Dec)). Este mensaje puede incluir la solicitud de la SMF de seguridad del UP de la RAN (SMF_RUS_Pre), o la decisión de la SMF de seguridad del UP terminada en la CN en la red de servicio (SMF_CUS_Dec), o la decisión de la HN de seguridad del UP terminada en la CN en la red doméstica (HN_Dec).

Etapa 11: AMF a (R)AN: Solicitud de Sesión de PDU N2, opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec, (Aceptación de Establecim. de Sesión de PDU (opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec)). La información del mensaje 10 se reenvía a la RAN.

Etapa X: Esta es una etapa entre las etapas 11. y 12. La (R)AN toma la decisión de política relacionada con la seguridad para UP terminada en la RAN. La RAN considera toda la información que se le proporciona: La política local de RAN relacionada con la seguridad de UP terminada en la RAN; UE_RUS_Pre; SMF_RUS_Pre; SMF_CUS_Dec; y HN_Dec.

Etapa 12: (R)AN a UE: configuración de recursos específica de la AN (incluida la Aceptación de Establecimiento de Sesión de PDU (RUS_Dec)). La (R)AN indica la decisión de política al UE. Si la (R)AN activa la encriptación y/o la protección de integridad para esta ID de Sesión de PDU/ID de Segmento entre el UE y la (R)AN, entonces la (R)AN indicará los algoritmos seleccionados para la protección de integridad y/o la encriptación de datos de UP enviados en todos los portadores de radiocomunicaciones que prestan servicio a esta ID de Sesión de PDU en el mensaje de Reconfiguración de Conexión de RRC al UE. El mensaje de Reconfiguración de Conexión de RRC está protegido en cuanto a integridad. Opcional: El UE almacena la preferencia o indicación referente a si se utilizará o no la terminación de encriptación de UP en la RAN, recibida en el mensaje de Aceptación de Establecimiento de Sesión de PDU para esta ID de Sesión de PDU/ID de Segmento. Opcional. El UE almacena la preferencia o indicación con respecto a si la terminación de protección de integridad del UP se utilizará en la RAN o no, recibida en el mensaje de Aceptación de Establecimiento de Sesión de PDU para esta ID de sesión de PDU/ID de Segmento. Opcional. El UE puede activar la encriptación y/o la protección de integridad para esta ID de Sesión de PDU entre el UE y la (R)AN si la preferencia o las indicaciones recibidas en el mensaje de Aceptación de Establecimiento de Sesión de PDU así lo indican. Opcional. El UE utiliza los algoritmos seleccionados para la protección de la integridad y/o la encriptación recibidos en el mensaje de Reconfiguración de Conexión de RRC de la (R)AN. La (R)AN puede tener una preferencia diferente y no seguir la preferencia enviada en el mensaje de Aceptación de Establecimiento de Sesión de PDU al UE. Opcional. El UE ahora puede enviar datos de UP encriptados y/o protegidos en cuanto a integridad para esta ID de Sesión de PDU/ID de Segmento.

Etapa 13: (R)AN a AMF: Ack de Solicitud de Sesión de PDU N2 (RUS_Dec). La RAN indica la decisión de política a la AMF. La (R)AN indica a la AMF y la SMF si la terminación de encriptación de UP en la RAN se utiliza para esta ID de Sesión de PDU. La (R)AN indica a la AMF y la SMF si la terminación de protección de integridad del UP en la RAN se usa para esta ID de Sesión de PDU.

Etapa 14: AMF a SMF: Solicitud de SM (información de SM N2). La AMF reenvía la información de SM N2 recibida de la (R)AN a la SMF. Opcional; la AMF puede indicar la decisión de política a la AMF.

Etapa 15a: Si la sesión N4 para esta Sesión de PDU no se estableció ya, la SMF inicia un procedimiento de Establecimiento de Sesión N4 con la UPF.

Etapa 15b: la UPF proporciona una Respuesta de Establecimiento/Modificación de Sesión N4 a la SMF.

Etapa 16: Después de esta etapa, la AMF reenvía eventos relevantes a la SMF, por ejemplo en el traspaso donde cambia la Info de Túnel de (R)AN o se reubica la AMF.

Etapa 17: SMF a UE, a través de UPF: en el caso de un Tipo de PDU IPv6, la SMF genera un Aviso de Rúter IPv6 y lo envía al UE a través de la N4 y la UPF.

Considérese a continuación la Figura 10 que muestra una Solicitud de Servicio desencadenada por un UE en estado CM-IDLE. Hay dos opciones diferentes (Opción 1 y Opción 2) descritas donde la RAN indica al UE cómo establecer y configurar la seguridad del UP para portadores de radiocomunicaciones que prestan servicio a la misma ID de Sesión de PDU.

Etapa 1. UE a (R)AN: Solicitud de Servicio NAS de MM (ID(s) de sesión de PDU, parámetros de seguridad, estado de sesión de PDU, por ID de segmento/ID de sesión de PDU: opcional: UE_Rus_Pre). Opcional: por ID de Sesión de PDU: El UE indica su UE_Rus_Pre.

Etapa 2. (R)AN a AMF: Mensaje N2 (Solicitud de Servicio NAS de MM (ID(s) de sesión de PDU, parámetros de seguridad, estado de sesión de PDU, por ID de segmento/ID de sesión de PDU: opcional: UE_Rus_Pre), ID Temporal de 5G, Información de ubicación, tipo de RAT, motivo de establecimiento de RRC).

Etapa 3. Si la Solicitud de Servicio no se envió con protección de integridad o la protección de integridad se indica como fallida, la AMF iniciará el procedimiento de autenticación/seguridad NAS como se define en la cláusula 4.6 de la TS 23.502.

Etapa 4a [Condicional] AMF a SMF: Mensaje N11 (ID(s) de sesión de PDU). Si el mensaje de Solicitud de Servicio NAS de MM incluye ID(s) de sesión de PDU, o la SMF activa este procedimiento, pero las IDs de sesión de PDU del UE se correlacionan con otras SMFs que no son la que activa el procedimiento, la AMF envía un mensaje N11 a la(s) SMF(s) asociada(s) a la(s) ID(s) de sesión de PDU.

Etapa 4b [Condicional] SMF a AMF: mensaje N11 (por par de ID de Segmento/ID de Sesión de PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: HN_Dec, (información de SM N2 (perfil QoS, Info de Túnel de CN N3, por par de ID de Segmento/ID de Sesión de PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: HN_Dec)) a la AMF. Después de recibir el Mensaje N11 en 4a, cada SMF envía el Mensaje N11 a la AMF para establecer el(los) plano(s) de usuario para las sesiones de PDU. La información de SM N2 contiene información que la AMF proporcionará a la RAN Opcional: la SMF incluye la siguiente información por par de ID de Segmento/ID de Sesión de PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: HN_Dec.

Etapa 5a. AMF a (R)AN: Solicitud N2 (información de SM N2 recibida de la SMF, contexto de seguridad, ID de Conexión de Señalización de AMF, Lista de Restricciones de Traspaso, Aceptación de Servicio NAS de MM, lista de pares de ID de Segmento/ID de Sesión de PDU: por par de ID de Segmento/ID de Sesión de PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: HN_Dec). La AMF incluye la siguiente información para la RAN: lista de pares de ID de Segmento/ID de sesión de PDU, por cada par de ID de Segmento/ID de sesión de PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: HN_Dec.

Etapa 5b. RAN a UE: Orden de Modo de Seguridad en el AS (algoritmo de encriptación e integridad seleccionado para la protección de la señalización del CP, **Opción 1**: por ID de Segmento/ID de Sesión de PDU: algoritmos de encriptación y/o algoritmo de integridad seleccionados para la protección de datos de UP). Este mensaje está protegido en cuanto a integridad con la clave K-RRCint.

Tanto para la Opción 1 como para la Opción 2, <u>para todos los portadores de radiocomunicaciones que prestan servicio a la misma ID de Segmento/ID de Sesión de PDU,</u> la (R)AN almacena lo recibido: opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec para este ID de Segmento/ID de Sesión de PDU, recibidos en información de SM N2. La RAN puede tener una política diferente configurada que puede desestimar la preferencia recibida de la red central. La RAN decide y establece la política de seguridad del UP de la RAN en RUS_Dec. Si RUS_Dec indica que se usará la terminación de encriptación de UP en la RAN, entonces la RAN puede activar la encriptación para todos los portadores de radiocomunicaciones que prestan servicio a esta ID de Segmento/ID de Sesión de PDU entre el UE y la (R)AN. La (R)AN selecciona el algoritmo para la encriptación seleccionando un algoritmo común a partir de la capacidad 5G del UE (con algoritmos admitidos por el UE) recibida de la AMF y los algoritmos configurados con la prioridad más alta en la lista configurada en la (R)AN. Si RUS_Dec indica que en la RAN se utilizará la terminación de protección de integridad del UP, entonces la RAN puede activar la protección de integridad para todos los portadores de radiocomunicaciones que prestan servicio a este ID de Segmento/ID de Sesión de PDU entre el UE y la (R)AN. La (R)AN selecciona el algoritmo para la protección de la integridad seleccionando un algoritmo común a partir de la capacidad 5G del UE (con algoritmos admitidos por el UE) recibida de la AMF y los algoritmos configurados con la prioridad más alta en la lista configurada en la (R)AN. Si RUS_Dec indica que la terminación de encriptación de UP no se utilizará en la RAN, entonces la RAN puede no activar la encriptación para los portadores de radiocomunicaciones que prestan servicio a esta ID de Segmento/ID de Sesión de PDU entre el UE y la (R)AN. La RAN indica al UE que la encriptación del UP no se utilizará para todos los portadores de radiocomunicaciones que prestan servicio a esta ID de Segmento/ID de Sesión de PDU entre el UE y la (R)AN. Si RUS_Dec indica que la terminación de protección de integridad del UP no se utilizará en la RAN, entonces la RAN puede no activar la protección de integridad para los portadores de radiocomunicaciones que prestan servicio a esta ID de Segmento/ID de Sesión de PDU entre el UE y la (R)AN. La RAN indica al UE que la protección de integridad del UP no se utilizará para todos los portadores de radiocomunicaciones que prestan servicio a esta ID de Segmento/ID de Sesión de PDU entre el UE y la (R)AN.

Etapa 5c. UE a RAN: Orden de Modo de Seguridad en el AS Completada (). El UE utiliza los algoritmos de seguridad indicados para la protección de la señalización del CP. El UE utiliza los algoritmos de seguridad indicados para todos los portadores de radiocomunicaciones que prestan servicio a la misma ID de Segmento/Sesión de PDU para la protección de datos de UP.

Etapa 6. (R)AN a UE: Reconfiguración de Conexión de RRC (**Opción 2:** para portadores de radiocomunicaciones que prestan servicio a la misma ID de Segmento/ID de Sesión de PDU: algoritmos de encriptación y/o algoritmo de integridad seleccionados para la protección de datos de UP). La RAN realiza la Reconfiguración de Conexión de RRC con el UE dependiendo de la Información de QoS para todos los Flujos de QoS de las Sesiones de PDU activadas y los Portadores de Radiocomunicaciones de Datos. La seguridad del plano de usuario se establece en esta etapa, que se describe de forma detallada en las especificaciones de la RAN. **<u>Opción 2:</u>** <u>Véase el texto anterior de la etapa 5b.</u> La RAN reenvía la Aceptación de Servicio NAS de MM al UE. El UE elimina localmente el contexto de sesiones de PDU que no están disponibles en la CN 5G.

Etapa 7. Después de configurar los recursos de radiocomunicaciones del plano de usuario, los datos de enlace ascendente del UE ahora se pueden reenviar a la RAN. La RAN 5G envía los datos de enlace ascendente a la dirección de la UPF y la ID de Túnel proporcionadas en la etapa 4.

Existe otro desafío en la activación de la seguridad del plano de usuario en el AS, tal como se ha mencionado anteriormente, y que se describe a continuación. Es posible que el gNB no pueda cumplir con dicha primera indicación (por ejemplo, SMF_RUS_Pre) de la SMF. En otras palabras, el gNB puede no ser capaz de activar la seguridad del plano de usuario en el AS, aun cuando dicha primera indicación de la SMF significó la necesidad de activar la seguridad del plano de usuario en el AS. Podría haber varias razones para que el gNB no pueda cumplir con dicha primera indicación de la SMF, por ejemplo, el gNB está sobrecargado debido a que presta servicio a un gran número de UEs al mismo tiempo y, por lo tanto, el gNB está configurado para no usar ninguna operación criptográfica en aras de la eficiencia computacional, o el gNB está en modo de ahorro de energía y, por lo tanto, el gNB está configurado para no usar ninguna operación criptográfica en aras de la eficiencia de la batería, etcétera. En algunos escenarios, se supone un modelo en el que las partes que son propietarias de la RAN y la red central, y las explotan, son diferentes. En tales escenarios, varias redes centrales podrían compartir una sola RAN. Esto podría significar que una parte RAN que comercializa los servicios 5G de la RAN ha acordado diferentes políticas con cada una de las partes de red central que explotan las redes centrales 5G, y algunas partes de red central pueden no estar autorizadas a activar la seguridad del plano de usuario en el AS. La parte de red central que está dispuesta a pagar, por ejemplo por la integridad del plano de usuario, podría ser la única a la que se le permite activar la integridad del plano de usuario. En tales casos, el gNB prosigue adelante sin activar la seguridad del plano de usuario en el AS, aun cuando su activación esté indicada por la SMF. Sin embargo, la SMF debe al menos tener conocimiento de que el gNB no cumplió la primera indicación. De acuerdo con algunas realizaciones, a continuación, el gNB 42 envía una segunda indicación a la SMF 48 (a través de la AMF 46) para informar a la SMF 48 de si el gNB activó o no activó la seguridad del plano de usuario en el AS. Las Figuras 9 y 10 describen los flujos de señalización, los procedimientos, los mensajes y los campos utilizados entre la SMF 48 y el gNB 42 para dicha segunda indicación.

La primera indicación y dicha segunda indicación pueden no ser suficientes para la seguridad del tráfico del plano de usuario. Por lo tanto, algunas realizaciones proponen un nuevo mecanismo que proporciona un mecanismo robusto para la activación de la seguridad del plano de usuario en el AS.

En este sentido, obsérvese que la SMF 48 preparó la primera indicación sobre la base de alguna política, por ejemplo un tráfico importante del plano de usuario perteneciente al Presidente de una nación debe estar protegido tanto en cuanto a confidencialidad como en cuanto a integridad, o una ráfaga de datos corta perteneciente a un dispositivo IoT (Internet de las Cosas) debe estar protegida en cuanto a integridad, o un tráfico multimedia que pertenece a un servicio de vídeo debe estar protegido en cuanto a confidencialidad, etcétera. Dependiendo de la política o del caso de uso, puede ser inaceptable que el gNB 42 no cumpla con dicha primera indicación enviada por la SMF 48, por ejemplo, incluso si el gNB 42 está sobrecargado o funcionando en modo de ahorro de energía, puede ser un problema grave que el tráfico del plano de usuario perteneciente al Presidente de una nación no esté protegido en cuanto a confidencialidad e integridad por el gNB 42. Obsérvese que no es suficiente con que el gNB 42 envíe dicha segunda indicación a la SMF 48. La SMF 48 conoce el estado de activación de la seguridad del plano de usuario en el AS, pero puede ser demasiado tarde antes de que la SMF 48 tome medidas adicionales, por ejemplo algunos datos de enlace ascendente ya enviados por el UE 40 por vía aérea, o algunos datos de enlace descendente ya enviados por el gNB 42 por vía aérea. La SMF 48 tiene conocimiento, pero el daño ya está hecho.

La causa principal del problema mencionado anteriormente es que es la SMF 48 quien tiene la información correcta sobre la sensibilidad del tráfico del plano de usuario y la política correspondiente, mientras que es el gNB 42 quien desestima la primera indicación mencionada enviada por la SMF 48. Con esa observación, algunas realizaciones proponen que la SMF 48 (en términos generales, algún nodo 16 de red central de la Figura 1) indique al gNB 42 (en términos generales, algún nodo 12 de RAN de la Figura 1) si el gNB 42 puede desestimar o no la decisión de la SMF sobre la activación de la seguridad del plano de usuario en el AS. En otras palabras, el gNB 42 no desestima la decisión de la SMF a menos que la SMF 48 lo permita. El efecto nuevo de aplicar esto es que siempre es la SMF 48 la que toma la decisión final sobre la activación de la seguridad del plano de usuario en el AS y se evita una situación en la que el gNB 42 no activa la seguridad del plano de usuario en el AS, a pesar de la decisión de la SMF de activarlo.

La Figura 11 ilustra el concepto general de algunas realizaciones.

Etapa 1: Cualquier comunicación o acciones previas entre o en el gNB 42 y la SMF 48.

Etapa 2: La SMF 48 indica al gNB 42 un comportamiento permitido, designado con donotOverrule. Dicho donotOverrule indica al gNB 42 si al gNB 42 se le permite o no desestimar cualquier indicación de activación de la seguridad del plano de usuario en el AS proveniente de la SMF 48.

Etapa 3: Cualquier comunicación o acciones entre el gNB 42 y la SMF 48. Un ejemplo puede ser un mensaje del gNB 42 a la SMF 48 que indica un acuse de recibo en referencia a que ha recibido y acepta la indicación donotOverrule, o un mensaje de error que indica que el gNB 42 no puede aceptar la indicación donotOverrule. Otro ejemplo puede ser un mensaje de la SMF al gNB f42 o un establecimiento de sesión de plano de usuario y una indicación (designada como primera indicación antes) de la activación de la seguridad del plano de usuario en el AS.

Etapa 4: El gNB 42 tiene en cuenta el donotOverrule obtenido para decidir si desestima o no una indicación de la SMF. Por ejemplo - Debido a una sobrecarga o un modo de ahorro de energía, el gNB 42 puede determinar que no puede cumplir con la primera indicación de la SMF 48 que indica que el gNB 42 active la seguridad del plano de usuario en

el AS. Sin embargo, dicho donotOverrule no permite que el gNB 42 desestime la primera indicación. Por lo tanto, el gNB 42 no desestima la primera indicación de la SMF 48. En otras palabras, el gNB 42 no procede con el establecimiento de la sesión de plano de usuario sin la seguridad del plano de usuario en el AS.

Etapa 5: Cualquier comunicación o acciones entre el gNB 42 y la SMF 48. Un ejemplo puede ser un mensaje del gNB 42 a la SMF 48 con una indicación (designada como segunda indicación antes) sobre si el gNB 42 era capaz o no de cumplir con la primera indicación.

El gNB 42 solo puede enviar la segunda indicación cuando el gNB 42 no puede cumplir con la primera indicación. En otras palabras, cuando el gNB 42 puede cumplir con la primera indicación, entonces el gNB 42 procede con el establecimiento de la sesión de plano de usuario y no envía la segunda indicación a la SMF 48, entonces la SMF 48 sabe implícitamente que se cumplió con la primera indicación. Además, la segunda indicación del gNB 42 a la SMF 48 puede incluir información sobre por qué el gNB 42 no pudo cumplir con la primera indicación, por ejemplo, "no puede cumplir debido a una sobrecarga", "no puede cumplir debido al modo de ahorro de energía", "no puede cumplir porque la SMF 48 no está autorizada a activar la seguridad del plano de usuario en el AS", etcétera.

Dicha indicación donotOverrule puede transferirse directamente entre el gNB 42 y la SMF 48 ó podría haber nodos intermedios que finalmente reenvíen dicha indicación donotOverrule al gNB 42, por ejemplo, a través de la AMF 46 intermedia u otros gNB intermedios, lo cual significa que un nodo intermedio puede reenviar el donotOverrule recibido.

Dicha indicación donotOverrule puede implementarse de varias maneras, por ejemplo, aunque sin limitarse a lo siguiente. Una forma explícita de implementación podría ser, por ejemplo, un campo booleano donde VERDADERO indica que al gNB 42 no se le permite la desestimación y FALSO indica que al gNB 42 no se le permite la desestimación, o un campo de tipo cadena (*string*) donde "permitido" designa que al gNB 42 se le permite la desestimación y "no_permitido" indica que al gNB 42 no se le permite la desestimación. El donotOverrule también puede tener una política más granular que indica en qué condiciones se le permite la desestimación al gNB 42 y en qué condiciones no se le permite la desestimación al gNB 42 sin confirmación adicional de la SMF. Un ejemplo de política granular podría ser, por ejemplo, "desestimación permitida para confidencialidad", "desestimación no permitida para protección de integridad", "desestimación permitida durante los domingos", "desestimación permitida cuando el número de UEs conectados es superior a 10000", etcétera. Una forma implícita de implementación podría ser, por ejemplo, la ausencia de un campo significa que al gNB 42 se le permite la desestimación y la presencia de un campo designa que al gNB 42 no se le permite la desestimación, o viceversa.

Dicha indicación donotOverrule puede variar de diversas maneras, por ejemplo, aunque sin carácter limitativo: (i) Relativa al tipo de servicio: por ejemplo, donotOverrule es FALSO para el servicio de vídeo y VERDADERO para el servicio IoT; (ii) Relativa a la ubicación del gNB: por ejemplo, donotOverrule es FALSO para gNBs que están dentro de unas instalaciones aisladas físicamente, y VERDADERO para gNBs que están abiertos en áreas públicas; (iii) Relativa al tipo de abonado: por ejemplo, donotOverrule es FALSO para abonados públicos y VERDADERO para el Presidente de una nación; y/o (iv) Relativa al tiempo: por ejemplo, donotOverrule es FALSO durante los juegos olímpicos y VERDADERO durante elecciones nacionales. El gNB 42 puede obtener dicha indicación de donotOverrule de varias formas, por ejemplo, pero sin limitarse a lo siguiente. En una primera forma, la indicación donotOverrule puede obtenerse en un mismo mensaje que comprende una indicación de la SMF sobre la activación de la seguridad del plano de usuario en el AS (designada como primera indicación antes). En otras palabras, dicho donotOverrule y dicha primera indicación se envían en un mismo mensaje. Esto podría significar que donotOverrule se aplica solo a la primera indicación junto con la cual se obtiene el donotOverrule.

En una segunda forma, la indicación donotOverrule puede obtenerse durante un establecimiento de sesión de plano de usuario específico del UE entre el gNB y la red central, por ejemplo, donotOverrule se multiplexa con o se añade a un mensaje de aceptación de establecimiento de sesión de PDU desde la SMF 48 al gNB 42, el cual se reenvía al gNB 42 a través de la AMF 46 en un mensaje de Solicitud de Sesión N2-PDU.

En una tercera forma, la indicación donotOverrule no se envía como parte de la señalización para el establecimiento de la sesión de plano de usuario entre el gNB y la SMF 48, sino que el gNB 42 obtiene el donotOverrule a partir de una configuración, por ejemplo, leída de una base de datos de la red, recuperada de un archivo local, recuperada de un nodo de red, etcétera. El donotOverrule puede indicar si se permite o no una desestimación para todos los UEs que envían solicitudes de establecimiento de sesión de plano de usuario a una SMF particular o a un segmento de red.

En una cuarta forma, la indicación donotOverrule se obtiene durante una configuración de interfaz entre el gNB 42 y la red central, por ejemplo, N2/N11 (gNB-AMF-SMF) o N3/N4 (gNB-UPF-SMF).

En una quinta forma, la indicación donotOverrule se obtiene durante una configuración de contexto inicial específica del UE entre el gNB 42 y la red central.

En una sexta forma, la indicación donotOverrule se obtiene durante una fase de preparación de un traspaso específica del UE entre el gNB 42 y la red central.

En una séptima forma, la indicación donotOverrule se obtiene durante una fase de preparación de un traspaso específica del UE entre los gNBs.

Pueden producirse varias acciones del gNB 42 y la SMF 48, cuando el gNB 42 no puede cumplir con la primera indicación, por ejemplo, las siguientes, aunque sin carácter limitativo. Algunas acciones posibles podrían ser cancelar, rechazar o descartar cualquier sesión de plano de usuario en curso o establecimiento de sesión de plano de usuario en progreso. La SMF 48 también puede decidir cambiar temporalmente la política de seguridad del plano de usuario, por ejemplo para no activar la seguridad del plano de usuario en el AS para la sesión actual e indicar la misma al gNB. La SMF 48 puede desear hacer esto en casos en los que el daño debido a una potencial falta de comunicación sea mayor que el daño debido a una comunicación menos segura. La SMF puede indicar esto al gNB 42, por ejemplo, indicando que la seguridad del plano de usuario en el AS no se debe activar (por ejemplo, la primera indicación es FALSA), o indicando que la seguridad del plano de usuario en el AS se debe activar pero el gNB 42 puede desestimar la indicación de la SMF (por ejemplo, la primera indicación es VERDADERA y el donotOverrule es FALSO). La SMF 48 ó el gNB 42 también puede indicar al UE que seleccione un gNB diferente que pueda tener mejores posibilidades de cumplir con la primera indicación, por ejemplo, por no estar sobrecargado o no estar funcionando en modo de ahorro de energía. En el caso de una RAN virtualizada, puede ser posible que la SMF 48 aumente los recursos disponibles para el gNB 42 sobre la marcha y que, a continuación, vuelva a intentar el establecimiento de la sesión de plano de usuario.

Según se usa en este documento, nodo de red se refiere a equipos capaces, configurados, dispuestos y/u operativos para comunicarse directa o indirectamente con un dispositivo inalámbrico y/o con otros nodos o equipos de red de la red inalámbrica con el fin de habilitar y/o proporcionar acceso inalámbrico al dispositivo inalámbrico y/o para realizar otras funciones (por ejemplo, administración) en la red inalámbrica. Los ejemplos de nodos de red incluyen, aunque sin carácter limitativo, nodos de red de radiocomunicaciones, tales como puntos de acceso (AP) (por ejemplo, puntos de acceso de radiocomunicaciones), estaciones base (BSs) (por ejemplo, estaciones base de radiocomunicaciones, Nodos B, Nodos B evolucionados (eNBs)) y Nodos B de NR (gNBs)). Las estaciones base pueden clasificarse en función de la cantidad de cobertura que brindan (o, dicho de otra manera, su nivel de potencia de transmisión) y entonces también pueden denominarse femto-estaciones base, pico-estaciones base, micro-estaciones base o macro-estaciones base. Una estación base puede ser un nodo de retransmisión o un nodo donante de retransmisión que controla un retransmisor. Un nodo de red también puede incluir una o más partes (o la totalidad de ellas) de una estación base de radiocomunicaciones distribuida, tales como unidades digitales centralizadas y/o unidades de radiocomunicaciones remotas (RRUs), en ocasiones denominadas Cabeceras de Radiocomunicaciones Remotas (RRHs). En dichas unidades de radiocomunicaciones remotas puede integrarse o no una antena, como dispositivo de radiocomunicaciones con antena integrada. Las partes de una estación base de radiocomunicaciones distribuida también pueden denominarse nodos en un sistema de antenas distribuido (DAS). Aún otros ejemplos de nodos de red incluyen equipos de radiocomunicaciones multi-norma (MSR), tales como BSs MSR, controladores de red, tales como controladores de red de radiocomunicaciones (RNC) o controladores de estaciones base (BSC), estaciones transceptoras base (BTS), puntos de transmisión, nodos de transmisión, entidades de coordinación multicélula/multidifusión (MCEs), nodos de red central (por ejemplo, MSCs, MMEs), nodos de O&M, nodos de OSS, nodos de SON, nodos de posicionamiento (por ejemplo, E-SMLCs) y/o MDTs. Como ejemplo alternativo, un nodo de red puede ser un nodo de red virtual según se describe de forma más detallada posteriormente. Sin embargo, de forma más general, los nodos de red pueden representar cualquier dispositivo (o grupo de dispositivos) adecuado capaz, configurado, dispuesto y/u operativo para habilitar y/o proporcionar a un dispositivo inalámbrico acceso a la red inalámbrica o para proporcionar algún servicio a un dispositivo inalámbrico que haya accedido a la red inalámbrica.

Según se usa en este documento, dispositivo inalámbrico (WD) se refiere a un dispositivo capaz, configurado, dispuesto y/u operativo para comunicarse de forma inalámbrica con nodos de red y/u otros dispositivos inalámbricos. A menos que se indique lo contrario, el término WD puede usarse de manera intercambiable en la presente con equipo de usuario (UE). La comunicación inalámbrica puede implicar la transmisión y/o recepción de señales inalámbricas utilizando ondas electromagnéticas, ondas de radiocomunicaciones, ondas infrarrojas y/u otros tipos de señales adecuadas para transportar información por vía aérea. En algunas realizaciones, un WD puede configurarse para transmitir y/o recibir información sin interacción humana directa. Por ejemplo, un WD puede estar diseñado para transmitir información a una red con una planificación predeterminada, cuando se active por un evento interno o externo, o como respuesta a solicitudes de la red. Los ejemplos de WD incluyen, aunque sin carácter limitativo, un teléfono inteligente, un teléfono móvil, un teléfono celular, un teléfono de voz sobre IP (VoIP), un teléfono de bucle local inalámbrico, un ordenador de escritorio, un asistente personal digital (PDA), una cámara inalámbrica, una consola o dispositivo de juego, un dispositivo de almacenamiento de música, un aparato de reproducción, un dispositivo terminal ponible, un punto extremo inalámbrico, una estación móvil, una tableta, un ordenador portátil, un equipo integrado en ordenador portátil (LEE), un equipo montado en ordenador portátil (LME), un dispositivo inteligente, un equipo inalámbrico en las instalaciones del cliente (CPE), un dispositivo terminal inalámbrico montado en un vehículo, etcétera. Un WD puede admitir una comunicación de dispositivo-a-dispositivo (D2D), por ejemplo, implementando un estándar 3GPP para comunicación de enlace lateral, vehículo-a-vehículo (V2V), vehículo-a-infraestructura (V2I), vehículo-a-todo (V2X) y en este caso puede denominarse dispositivo de comunicación D2D. Todavía como ejemplo específico alternativo, en un escenario de Internet de las Cosas (IoT), un WD puede representar una máquina u otro dispositivo que realiza monitorizaciones y/o mediciones, y transmite los resultados de dichas monitorizaciones y/o mediciones a otro WD y/o Un nodo de red. En este caso, el WD puede ser un dispositivo de máquina-a-máquina

(M2M), que en un contexto 3GPP puede denominarse dispositivo MTC. Como ejemplo particular, el WD puede ser un UE que implementa el estándar 3GPP de banda estrecha de internet de las cosas (NB-IoT). Ejemplos particulares de tales máquinas o dispositivos son sensores, dispositivos de medición tales como medidores de potencia, maquinaria industrial o aparatos domésticos o personales (por ejemplo, neveras, televisores, etcétera), dispositivos ponibles personales (por ejemplo, relojes, rastreadores de actividad física, etcétera). En otros escenarios, un WD puede representar un vehículo u otro equipo que sea capaz de monitorizar y/o informar sobre su estado operativo u otras funciones asociadas a su funcionamientos. Un WD según se ha descrito anteriormente puede representar el punto extremo de una conexión inalámbrica, en cuyo caso el dispositivo puede ser denominado terminal inalámbrico. Además, un WD según se ha descrito anteriormente puede ser móvil, en cuyo caso también puede denominarse dispositivo móvil o terminal móvil.

La Figura 12 ilustra una red de telecomunicaciones conectada a través de una red intermedia a un ordenador anfitrión de acuerdo con algunas realizaciones. En particular, en referencia a la FIGURA 12, de acuerdo con una realización, un sistema de comunicaciones incluye una red 1210 de telecomunicaciones, tal como una red celular de tipo 3GPP, que comprende la red 1211 de acceso, tal como una red de acceso de radiocomunicaciones, y la red central 1214. La red 1211 de acceso comprende una pluralidad de estaciones base 1212a, 1212b, 1212c, tales como NBs, eNBs, gNBs u otros tipos de puntos de acceso inalámbrico, cada uno de los cuales define un área 1213a, 1213b, 1213c de cobertura correspondiente. Cada estación base 1212a, 1212b, 1212c se puede conectar a la red central 1214 a través de una conexión 1215 por cable o inalámbrica. Un primer UE 1291 ubicado en el área 1213c de cobertura está configurado para conectarse de forma inalámbrica a la estación base 1212c correspondiente, o ser localizado por esta. Un segundo UE 1292 en el área 1213a de cobertura se puede conectar de forma inalámbrica a la estación base correspondiente 1212a. Si bien se ilustra una pluralidad de UEs 1291, 1292 en este ejemplo, las realizaciones dadas a conocer son igualmente aplicables a una situación en la que un único UE está en el área de cobertura o en la que un único UE se conecta a la estación base 1212 correspondiente.

La propia red 1210 de telecomunicaciones está conectada al ordenador anfitrión 1230, que puede materializarse en el *hardware* y/o *software* de un servidor autónomo, un servidor implementado en la nube, un servidor distribuido o como recursos de procesado en una granja de servidores. El ordenador anfitrión 1230 puede estar bajo propiedad o control de un proveedor de servicios, o puede ser operado por el proveedor de servicios o en nombre del proveedor de servicios. Las conexiones 1221 y 1222 entre la red 1210 de telecomunicaciones y el ordenador anfitrión 1230 pueden discurrir directamente desde la red central 1214 al ordenador anfitrión 1230 ó pueden ir a través de una red intermedia opcional 1220. La red intermedia 1220 puede ser una, o una combinación de más de una, de una red pública, privada o alojada; la red intermedia 1220, si existe, puede ser una red troncal o Internet; en particular, la red intermedia 1220 puede comprender dos o más subredes (no mostradas).

El sistema de comunicaciones de la Figura 12 en su conjunto permite la conectividad entre los UEs conectados 1291, 1292 y el ordenador anfitrión 1230. La conectividad puede describirse como una conexión *over-the-top* (OTT) 1250. El ordenador anfitrión 1230 y los UEs conectados 1291, 1292 están configurados para comunicar datos y/o señalización a través de la conexión OTT 1250, utilizando la red 1211 de acceso, la red central 1214, cualquier red intermedia 1220 y una posible infraestructura adicional (no mostrada) como intermediarios. La conexión OTT 1250 puede ser transparente en el sentido de que los dispositivos de comunicación participantes a través de los cuales pasa la conexión OTT 1250 desconocen el encaminamiento de las comunicaciones de enlace ascendente y enlace descendente. Por ejemplo, la estación base 1212 puede no disponer, o no es necesario que disponga de, información sobre el encaminamiento pasado de una comunicación de enlace descendente entrante con datos que se originan en el ordenador anfitrión 1230 para su reenvío (por ejemplo, entrega) a un UE 1291 conectado. De manera similar, no es necesario que la estación base 1212 tenga conocimiento del encaminamiento futuro de una comunicación de enlace ascendente saliente que se origina en el UE 1291 hacia el ordenador anfitrión 1230.

A continuación se describirán, en referencia a la Figura 13, implementaciones de ejemplo, de acuerdo con una realización, del UE, la estación base y el ordenador anfitrión descritos en los párrafos anteriores. La Figura 13 ilustra el ordenador anfitrión que se comunica a través de una estación base con un equipo de usuario por medio de una conexión parcialmente inalámbrica de acuerdo con algunas realizaciones. En el sistema 1300 de comunicaciones, el ordenador anfitrión 1310 comprende *hardware* 1315 que incluye la interfaz 1316 de comunicaciones configurada para establecer y mantener una conexión por cable o inalámbrica con una interfaz de un dispositivo de comunicación diferente del sistema 1300 de comunicaciones. El ordenador anfitrión 1310 además comprende circuitería 1318 de procesado, que puede tener capacidades de almacenamiento y/o procesado. En particular, la circuitería 1318 de procesado puede comprender uno o más procesadores programables, circuitos integrados de aplicación específica, matrices de puertas programables in situ o combinaciones de estos (no mostradas) adaptadas para ejecutar instrucciones. El ordenador anfitrión 1310 comprende además *software* 1311, que está almacenado en o es accesible por el ordenador anfitrión 1310 y ejecutable por la circuitería 1318 de procesado. El *software* 1311 incluye la aplicación 1312 de anfitrión. La aplicación 1312 de anfitrión puede funcionar para proporcionar un servicio a un usuario remoto, tal como un UE 1330 que se conecta a través de la conexión OTT 1350 que termina en el UE 1330 y el ordenador anfitrión 1310. Al proporcionar el servicio al usuario remoto, la aplicación 1312 de anfitrión puede proporcionar datos de usuario que se transmiten usando la conexión OTT 1350.

El sistema 1300 de comunicaciones incluye además la estación base 1320 dispuesta en un sistema de telecomunicaciones y que comprende *hardware* 1325 que le permite comunicarse con el ordenador anfitrión 1310 y

con el UE 1330. El *hardware* 1325 puede incluir la interfaz 1326 de comunicaciones para establecer y mantener una conexión por cable o inalámbrica con una interfaz de un dispositivo de comunicación diferente del sistema 1300 de comunicaciones, así como la interfaz 1327 de radiocomunicaciones para establecer y mantener al menos una conexión inalámbrica 1370 con el UE 1330 ubicado en un área de cobertura (no mostrada en la Figura 13) a la que presta servicio la estación base 1320. La interfaz 1326 de comunicaciones puede configurarse para facilitar la conexión 1360 al ordenador anfitrión 1310. La conexión 1360 puede ser directa o puede pasar a través de una red central (no mostrada en la Figura 13) del sistema de telecomunicaciones y/o a través de una o más redes intermedias fuera del sistema de telecomunicaciones. En la realización mostrada, el *hardware* 1325 de la estación base 1320 incluye además circuitería 1328 de procesado, que puede comprender uno o más procesadores programables, circuitos integrados de aplicación específica, matrices de puertas programables in situ o combinaciones de estos (no mostradas) adaptadas para ejecutar instrucciones. La estación base 1320 tiene además el *software* 1321 almacenado internamente o accesible a través de una conexión externa.

El sistema 1300 de comunicaciones incluye además el UE 1330 ya mencionado. Su *hardware* 1335 puede incluir la interfaz 1337 de radiocomunicaciones configurada para establecer y mantener la conexión inalámbrica 1370 con una estación base que presta servicio a un área de cobertura en la que se encuentra ubicado en ese momento el UE 1330. El *hardware* 1335 del UE 1330 incluye además circuitería 1338 de procesado, que puede comprender uno o más procesadores programables, circuitos integrados de aplicación específica, matrices de puertas programables in situ o combinaciones de estos (no mostradas) adaptadas para ejecutar instrucciones. El UE 1330 comprende además el *software* 1331, que está almacenado en o es accesible por el UE 1330 y ejecutable por la circuitería 1338 de procesado. El *software* 1331 incluye la aplicación 1332 de cliente. La aplicación 1332 de cliente puede funcionar para proporcionar un servicio a un usuario humano o no humano a través del UE 1330, con el soporte del ordenador anfitrión 1310. En el ordenador anfitrión 1310, una aplicación 1312 de anfitrión en ejecución puede comunicarse con la aplicación 1332 de cliente en ejecución a través de la conexión OTT 1350 que termina en el UE 1330 y el ordenador anfitrión 1310. Al proporcionar el servicio al usuario, la aplicación 1332 de cliente puede recibir datos de solicitud de la aplicación 1312 de anfitrión y proporcionar datos de usuario como respuesta a los datos de solicitud. La conexión OTT 1350 puede transferir tanto los datos de solicitud como los datos de usuario. La aplicación 1332 de cliente puede interactuar con el usuario para generar los datos de usuario que proporciona.

Se observa que el ordenador anfitrión 1310, la estación base 1320 y el UE 1330 ilustrados en la Figura 13 pueden ser similares o idénticos al ordenador anfitrión 1230, una de las estaciones base 1212a, 1212b, 1212c y uno de los UE 1291, 1292 de la Figura 12, respectivamente. Es decir, el funcionamiento interno de estas entidades puede ser como el mostrado en la Figura 13 e independientemente, la topología de red circundante puede ser la de la Figura 12.

En la Figura 13, la conexión OTT 1350 se ha dibujado de manera abstracta para ilustrar la comunicación entre el ordenador anfitrión 1310 y el UE 1330 a través de la estación base 1320, sin referencia explícita a ningún dispositivo intermediario y al encaminamiento preciso de mensajes a través de estos dispositivos. La infraestructura de red puede determinar el encaminamiento, que se puede configurar para ocultarse del UE 1330 ó del proveedor de servicios que opera el ordenador anfitrión 1310, o de ambos. Mientras la conexión OTT 1350 está activa, la infraestructura de red puede además tomar decisiones mediante las cuales cambia dinámicamente el encaminamiento (por ejemplo, en función de la consideración del equilibrado de la carga o la reconfiguración de la red).

La conexión inalámbrica 1370 entre el UE 1330 y la estación base 1320 está de acuerdo con las enseñanzas de las realizaciones descritas a lo largo de esta exposición. Una o más de las diversas realizaciones mejoran el rendimiento de servicios OTT proporcionados al UE 1330 usando la conexión OTT 1350, en la que la conexión inalámbrica 1370 forma el último segmento. De manera más precisa, las enseñanzas de estas realizaciones pueden mejorar el equilibrado de la carga, la eficiencia de los recursos de radiocomunicaciones y la eficiencia energética en la red y, por lo tanto, proporcionar beneficios tales como un menor tiempo de espera del usuario, una restricción relajada sobre los tamaños de los archivos y una mejor capacidad de respuesta.

Se puede proporcionar un procedimiento de medición con el fin de monitorizar la velocidad de datos, la latencia y otros factores con respecto a los cuales mejoran una o más de las realizaciones. Además, puede haber una funcionalidad de red opcional para reconfigurar la conexión OTT 1350 entre el ordenador anfitrión 1310 y el UE 1330, como respuesta a variaciones en los resultados de la medición. El procedimiento de medición y/o la funcionalidad de red para reconfigurar la conexión OTT 1350 puede implementarse en el *software* 1311 y el *hardware* 1315 del ordenador anfitrión 1310 ó en el *software* 1331 y el *hardware* 1335 del UE 1330, o en ambos. En realizaciones, pueden desplegarse sensores (no mostrados) en o asociados a dispositivos de comunicación a través de los cuales pasa la conexión OTT 1350; los sensores pueden participar en el procedimiento de medición suministrando valores de las cantidades monitorizadas ejemplificadas anteriormente, o suministrando valores de otras cantidades físicas a partir de las cuales el *software* 1311, 1331 puede calcular o estimar las cantidades monitorizadas. La reconfiguración de la conexión OTT 1350 puede incluir formato de mensaje, ajustes de retransmisión, encaminamiento preferido, etcétera; no es necesario que la reconfiguración afecte a la estación base 1320, y puede ser desconocida o imperceptible para la estación base 1320. Tales procedimientos y funcionalidades pueden ser conocidos y haberse llevado a la práctica en la técnica. En ciertas realizaciones, las mediciones pueden implicar señalización del UE privativa que facilita las mediciones de rendimiento, tiempos de propagación, latencia y similares del ordenador anfitrión 1310. Las mediciones pueden implementarse en la medida en la que el *software* 1311 y 1331 hace que se transmitan mensajes, en particular

mensajes vacíos o "ficticios", utilizando la conexión OTT 1350 mientras monitoriza los tiempos de propagación, errores, etcétera.

La Figura 14 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización. El sistema de comunicaciones incluye un ordenador anfitrión, una estación base y un UE que pueden ser los descritos en referencia a las Figuras 12 y 13. Por simplicidad de la presente exposición, solo se incluirán en esta sección referencias de los dibujos a la Figura 14. En la etapa 1410, el ordenador anfitrión proporciona datos del usuario. En la subetapa 1411 (que puede ser opcional) de la etapa 1410, el ordenador anfitrión proporciona los datos del usuario ejecutando una aplicación de anfitrión. En la etapa 1420, el ordenador anfitrión inicia una transmisión que transporta los datos del usuario al UE. En la etapa 1430 (que puede ser opcional), la estación base transmite al UE los datos del usuario que se transportaron en la transmisión que inició el ordenador anfitrión, de acuerdo con las enseñanzas de las realizaciones descritas a lo largo de esta exposición. En la etapa 1440 (que también puede ser opcional), el UE ejecuta una aplicación de cliente asociada a la aplicación de anfitrión ejecutada por el ordenador anfitrión.

La Figura 15 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización. El sistema de comunicaciones incluye un ordenador anfitrión, una estación base y un UE que pueden ser los descritos en referencia a las Figuras 12 y 13. Por simplicidad de la presente exposición, solo se incluirán en esta sección referencias de los dibujos a la Figura 15. En la etapa 1510 del método, el ordenador anfitrión proporciona datos del usuario. En una subetapa opcional (no mostrada), el ordenador anfitrión proporciona los datos del usuario ejecutando una aplicación de anfitrión. En la etapa 1520, el ordenador anfitrión inicia una transmisión que transporta los datos del usuario al UE. La transmisión puede pasar a través de la estación base, de acuerdo con las enseñanzas de las realizaciones descritas a lo largo de esta exposición. En la etapa 1530 (que puede ser opcional), el UE recibe los datos del usuario transportados en la transmisión.

La Figura 16 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización. El sistema de comunicaciones incluye un ordenador anfitrión, una estación base y un UE que pueden ser los descritos en referencia a las Figuras 12 y 13. Por simplicidad de la presente exposición, solo se incluirán en esta sección referencias de los dibujos a la Figura 16. En la etapa 1610 (que puede ser opcional), el UE recibe datos de entrada proporcionados por el ordenador anfitrión. De manera adicional o alternativa, en la etapa 1620, el UE proporciona datos de usuario. En la subetapa 1621 (que puede ser opcional) de la etapa 1620, el UE proporciona los datos del usuario ejecutando una aplicación de cliente. En la subetapa 1611 (que puede ser opcional) de la etapa 1610, el UE ejecuta una aplicación de cliente que proporciona los datos del usuario como reacción a los datos de entrada recibidos proporcionados por el ordenador anfitrión. Al proporcionar los datos del usuario, la aplicación de cliente ejecutada puede considerar además la entrada del usuario recibida del usuario. Independientemente de la manera específica en la que se proporcionaron los datos de usuario, el UE inicia, en la subetapa 1630 (que puede ser opcional), la transmisión de los datos del usuario al ordenador anfitrión. En la etapa 1640 del método, el ordenador anfitrión recibe los datos del usuario transmitidos desde el UE, de acuerdo con las enseñanzas de las realizaciones descritas a lo largo de esta exposición.

La Figura 17 es un diagrama de flujo que ilustra un método implementado en un sistema de comunicaciones, de acuerdo con una realización. El sistema de comunicaciones incluye un ordenador anfitrión, una estación base y un UE que pueden ser los descritos en referencia a las Figuras 12 y 13. Por simplicidad de la presente exposición, solo se incluirán en esta sección referencias de los dibujos a la Figura 17. En la etapa 1710 (que puede ser opcional), de acuerdo con las enseñanzas de las realizaciones descritas a lo largo de esta exposición, la estación base recibe datos de usuario del UE. En la etapa 1720 (que puede ser opcional), la estación base inicia la transmisión de los datos de usuario recibidos al ordenador anfitrión. En la etapa 1730 (que puede ser opcional), el ordenador anfitrión recibe los datos de usuario transportados en la transmisión iniciada por la estación base.

Todas las etapas, métodos, características, funciones o ventajas apropiados dados a conocer en la presente se pueden materializar a través de una o más unidades o módulos funcionales de uno o más aparatos virtuales. Cada aparato virtual puede comprender varias de estas unidades funcionales. Estas unidades funcionales se pueden implementar a través de circuitería de procesado, que puede incluir uno o más microprocesadores o microcontroladores, así como otro *hardware* digital, que puede incluir procesadores de señales digitales (DSPs), lógica digital de propósito especial y similares. La circuitería de procesado puede configurarse para ejecutar código de programa almacenado en memoria, que puede incluir uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), memoria caché, dispositivos de memoria *flash*, dispositivos de almacenamiento óptico, etcétera. El código de programa almacenado en la memoria incluye instrucciones de programa para ejecutar uno o más protocolos de telecomunicaciones y/o de comunicaciones de datos, así como instrucciones para llevar a cabo una o más de las técnicas aquí descritas. En algunas implementaciones, la circuitería de procesado puede usarse para hacer que la unidad funcional respectiva realice funciones correspondientes de acuerdo con una o más realizaciones de la presente exposición.

En general, todos los términos utilizados en este documento deben interpretarse de acuerdo con su significado habitual en el campo técnico relevante, a menos que se dé claramente un significado diferente y/o el mismo esté implícito en el contexto en el que se use. Todas las referencias a un/una/el/la elemento, aparato, componente, medios, etapa,

etcétera, deben interpretarse abiertamente como relativas a por lo menos una instancia del elemento, aparato, componente, medios, etapa, etcétera, a no ser que se indique explícitamente lo contrario.

El término unidad puede tener un significado convencional en el campo de la electrónica, dispositivos eléctricos y/o dispositivos electrónicos, y puede incluir, por ejemplo, circuitería eléctrica y/o electrónica, dispositivos, módulos, procesadores, memorias, dispositivos lógicos de estado sólido y/o discretos, programas informáticos o instrucciones para materializar tareas, procedimientos, cálculos, salidas y/o funciones de visualización respectivos, y otros, tales como los que se describen en este documento.

REIVINDICACIONES

1. Un método para configurar la seguridad del plano de usuario en el estrato de acceso, AS, en un sistema (10) de comunicaciones inalámbricas que incluye una red de acceso de radiocomunicaciones, RAN, (10B) y una red central, CN, (10A), siendo llevado a cabo el método por un nodo (12) de RAN en la RAN (10B) y comprendiendo:

recibir (112), desde la CN (10A), señalización (20) que indica una decisión de la CN (10A) sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS y que indica si al nodo (12) de RAN se le permite o no desestimar la decisión de la CN (10A); y

activar o no activar (114) la seguridad del plano de usuario en el AS, dependiendo de la señalización (20).

2. El método de la reivindicación 1, que comprende activar o no activar la seguridad del plano de usuario en el AS, dependiendo además de información que indica la capacidad o conveniencia del nodo (12) de RAN para activar la seguridad del plano de usuario en el AS.

3. El método de cualquiera de las reivindicaciones 1-2, que comprende además determinar si se activa o no la seguridad del plano de usuario en el AS, sobre la base de uno o más de:

un nivel de carga del nodo (12) de RAN;

disponibilidad o eficiencia energética en el nodo (12) de RAN; y

autorización de la CN para activar la seguridad del plano de usuario en el AS; y

un modo del nodo (12) de RAN.

4. El método de cualquiera de las reivindicaciones 1-3, en el que la señalización (20) se aplica específicamente para una sesión de plano de usuario particular y se recibe durante un procedimiento para establecer la sesión de plano de usuario para un dispositivo de comunicaciones inalámbricas particular.

5. El método de cualquiera de las reivindicaciones 1-4, que comprende además realizar una o más acciones cuando la decisión de la CN (10A) es que el nodo (12) de RAN debe activar la seguridad del plano de usuario en el AS, al nodo (12) de RAN no se le permite desestimar la decisión de la CN (10A), y el nodo (12) de RAN no puede, o la CN (10A) no está autorizada a, activar la seguridad del plano de usuario en el AS, en donde la acción o acciones incluyen cancelar, rechazar, o descartar una sesión de plano de usuario o establecimiento de sesión de plano de usuario.

6. El método de cualquiera de las reivindicaciones 1-5, en el que la decisión de la CN (10A) es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la integridad del plano de usuario o es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la confidencialidad del plano de usuario.

7. El método de cualquiera de las reivindicaciones 1-5, en el que la decisión de la CN (10A) es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la integridad del plano de usuario y es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la confidencialidad del plano de usuario.

8. El método de cualquiera de las reivindicaciones 1-7, en el que la decisión la toma un nodo (16) de CN que realiza la gestión de sesiones del plano de usuario.

9. El método de cualquiera de las reivindicaciones 1-8, en el que el nodo (16) de CN es un nodo que implementa una función de gestión de sesiones, SMF.

10. El método de cualquiera de las reivindicaciones 1-9, en el que la señalización (20) indica si al nodo (12) de RAN se le permite o no desestimar la decisión de la CN (10A) al indicar si la decisión de la CN (10A) es una orden que el nodo (12) de RAN debe cumplir o una preferencia cuya desestimación le está permitida al nodo (12) de RAN.

11. Un método para configurar la seguridad del plano de usuario en el estrato de acceso, AS, en un sistema (10) de comunicaciones inalámbricas que incluye una red de acceso de radiocomunicaciones, RAN, (10B) y una red central, CN (10A), siendo llevado a cabo el método por un nodo (16) de CN en la CN (10A) y comprendiendo:

tomar (212) una decisión por parte de la CN sobre si un nodo (12) de RAN en la RAN (10B) debe activar o no la seguridad del plano de usuario en el AS; y

transmitir (214) señalización (20) que indica la decisión de la CN (10A) y que indica si al nodo (12) de RAN se le permite o no desestimar la decisión de la CN (10A).

12. El método de la reivindicación 11, que comprende además determinar si al nodo (12) de RAN se le permite o no desestimar la decisión, basándose en y/o específicamente para uno o más de:

un tipo particular de seguridad del plano de usuario en el AS;

un tipo o prioridad particular de servicio para el cual se debe comunicar tráfico del plano de usuario a través del AS del plano de usuario;

una ubicación o tipo de ubicación particular del nodo de RAN;

un nivel de carga particular del nodo de RAN;

un tipo o prioridad particular de abonado cuyo tráfico de plano de usuario debe ser una comunicación a través del AS del plano de usuario; y

un momento o evento particular.

13. El método de cualquiera de las reivindicaciones 11-12, en el que la señalización (20) se aplica específicamente para una sesión de plano de usuario particular y se transmite durante un procedimiento para establecer la sesión de plano de usuario para un dispositivo de comunicaciones inalámbricas particular.

14. El método de cualquiera de las reivindicaciones 11-13, en el que la decisión es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la integridad del plano de usuario o es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la confidencialidad del plano de usuario.

15. El método de cualquiera de las reivindicaciones 11-14, en el que la decisión es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la integridad del plano de usuario y es una decisión sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS en forma de protección de la confidencialidad del plano de usuario.

16. El método de cualquiera de las reivindicaciones 11-15, en el que el nodo (16) de CN está configurado para realizar la gestión de sesiones del plano de usuario.

17. El método de cualquiera de las reivindicaciones 11-16, en el que el nodo (16) de CN es un nodo que implementa una función de gestión de sesiones, SMF.

18.Un nodo (12) de red de acceso de radiocomunicaciones, RAN, para configurar la seguridad del plano de usuario en el estrato de acceso, AS, en un sistema (10) de comunicaciones inalámbricas que incluye una RAN (10B) y una red central, CN (10A), estando configurado el nodo (12) de RAN para:

recibir, desde la CN (10A), señalización (20) que indica una decisión de la CN (10A) sobre si el nodo (12) de RAN debe activar o no la seguridad del plano de usuario en el AS y que indica si al nodo (12) de RAN se le permite o no desestimar la decisión de la CN (10A); y

activar o no activar la seguridad del plano de usuario en el AS, según la señalización (20).

19. Un nodo (16) de red central, CN, para configurar la seguridad del plano de usuario en el estrato de acceso, AS, en un sistema (10) de comunicaciones inalámbricas que incluye una red de acceso de radiocomunicaciones, RAN, (10B) y una red central, CN (10A), estando configurado el nodo (16) de CN para:

tomar una decisión por parte de la CN (10A) sobre si un nodo (12) de RAN en la RAN debe activar o no la seguridad del plano de usuario en el AS; y

transmitir señalización (20) que indica la decisión de la CN (10a) y que indica si al nodo (12) de RAN se le permite o no desestimar la decisión de la CN (10a).

20. Un programa informático que comprende instrucciones el cual, cuando es ejecutado por al menos un procesador de un nodo (12) de red de acceso de radiocomunicaciones, RAN, configurado para su uso en un sistema (10) de comunicaciones inalámbricas, consigue que el nodo (12) de RAN lleve a cabo el método de cualquiera de las reivindicaciones 1-10.

21. Un programa informático que comprende instrucciones el cual, cuando es ejecutado por al menos un procesador de un nodo (16) de red central, CN, configurado para su uso en un sistema (10) de comunicaciones inalámbricas, consigue que el nodo (16) de CN lleve a cabo el método de cualquiera de las reivindicaciones 11-17.

22. Un soporte que contiene el programa informático de cualquiera de las reivindicaciones 20-21, en el que el soporte es uno de una señal electrónica, una señal óptica, una señal de radiocomunicaciones o un soporte de almacenamiento legible por ordenador.

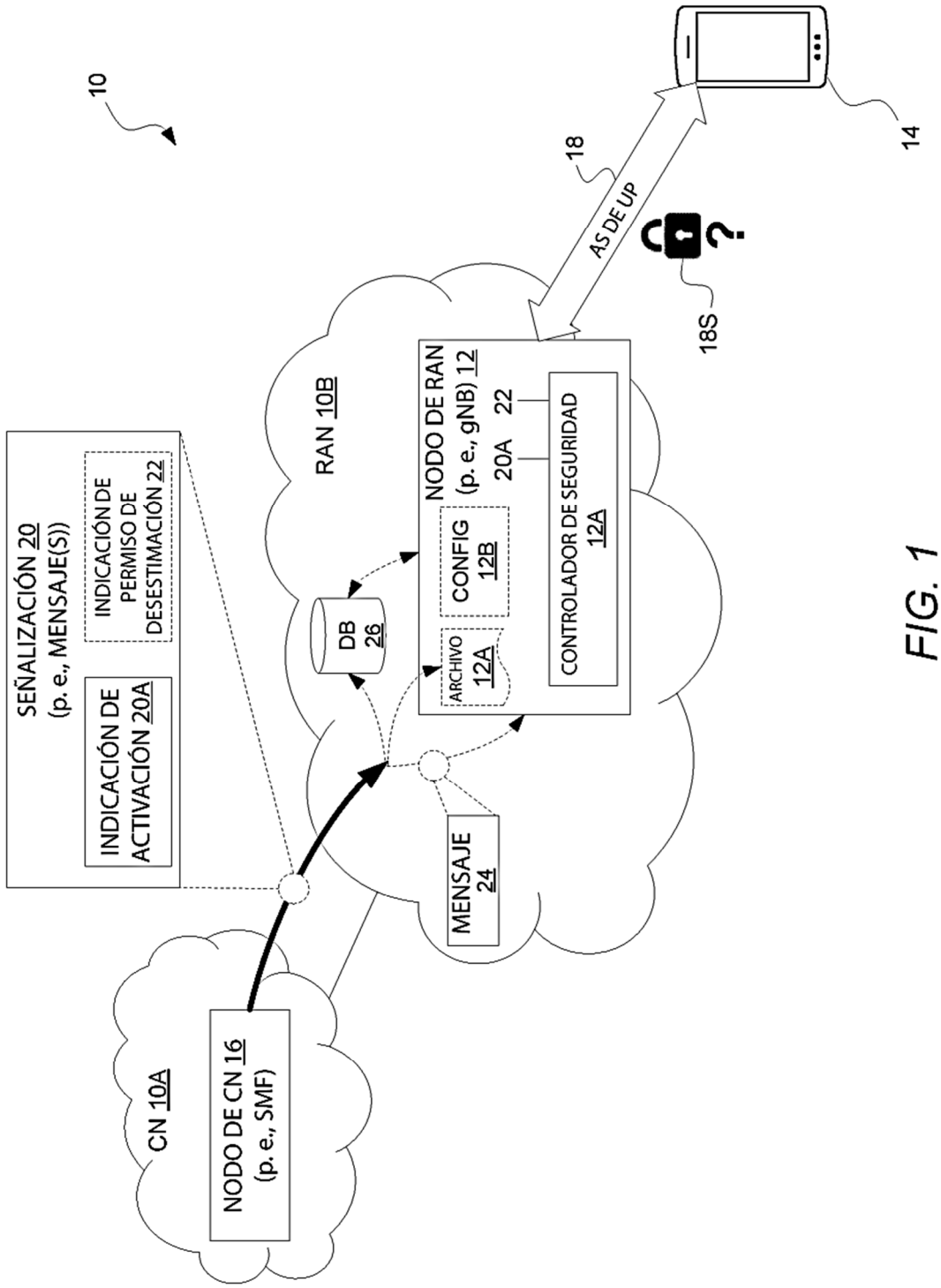
10
SEÑALIZACIÓN 20
(p. e., MENSAJE(S))
INDICACIÓN DE ACTIVACIÓN 20A
INDICACIÓN DE PERMISO DE DESESTIMACIÓN 22
CN 10A
NODO DE CN 16
(p. e., SMF)
RAN 10B
DB 26
MENSAJE 24
NODO DE RAN
(p. e., gNB) 12
ARCHIVO 12A
CONFIG 12B
20A
22
CONTROLADOR DE SEGURIDAD 12A
18
AS DE UP
18S
14

FIG. 1

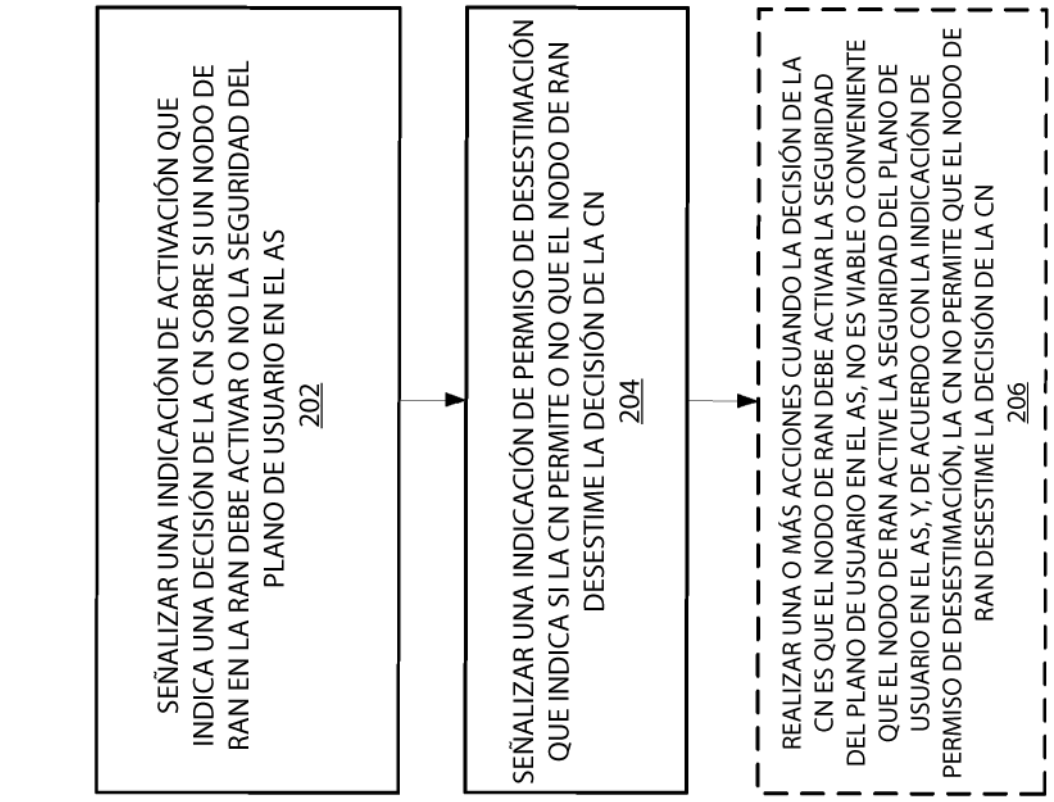

FIGURA 3A

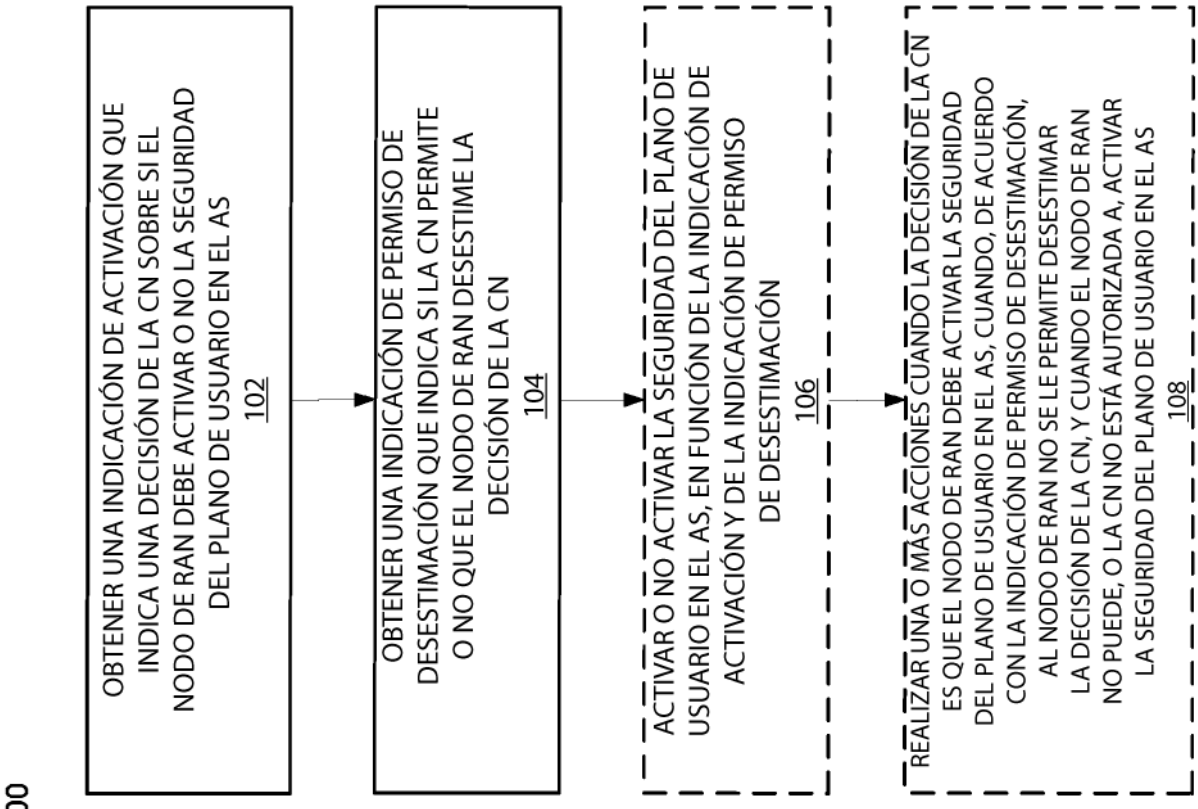

FIGURA 2A

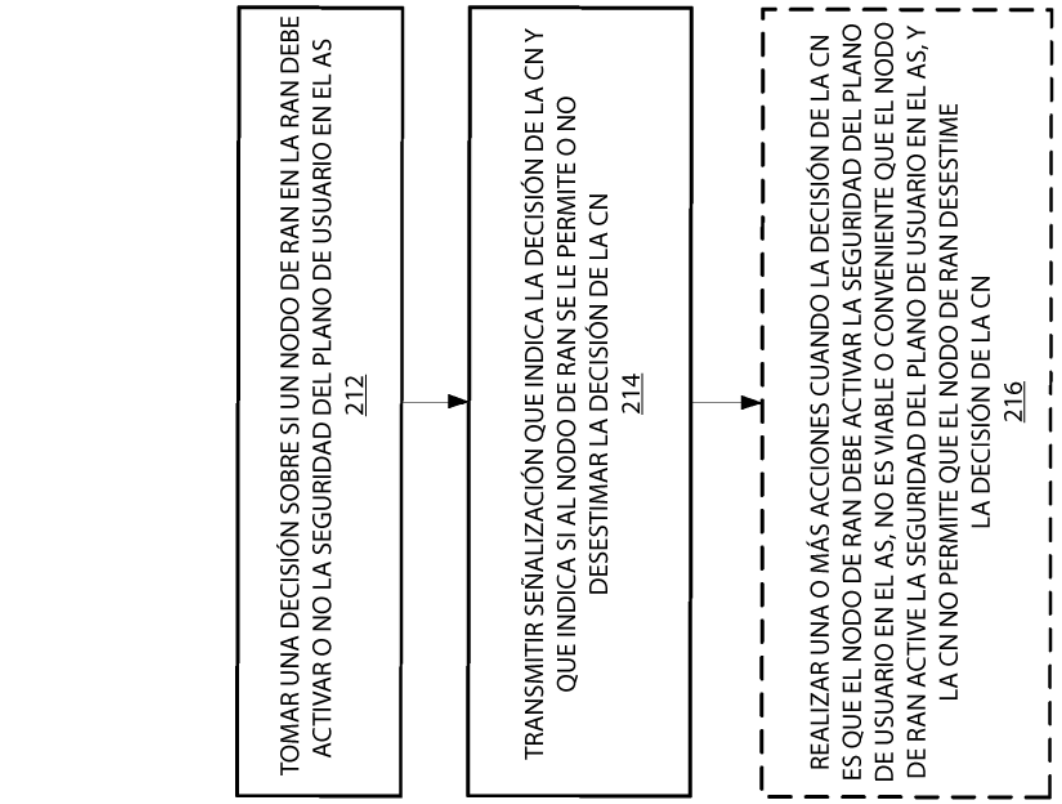

FIGURA 3B

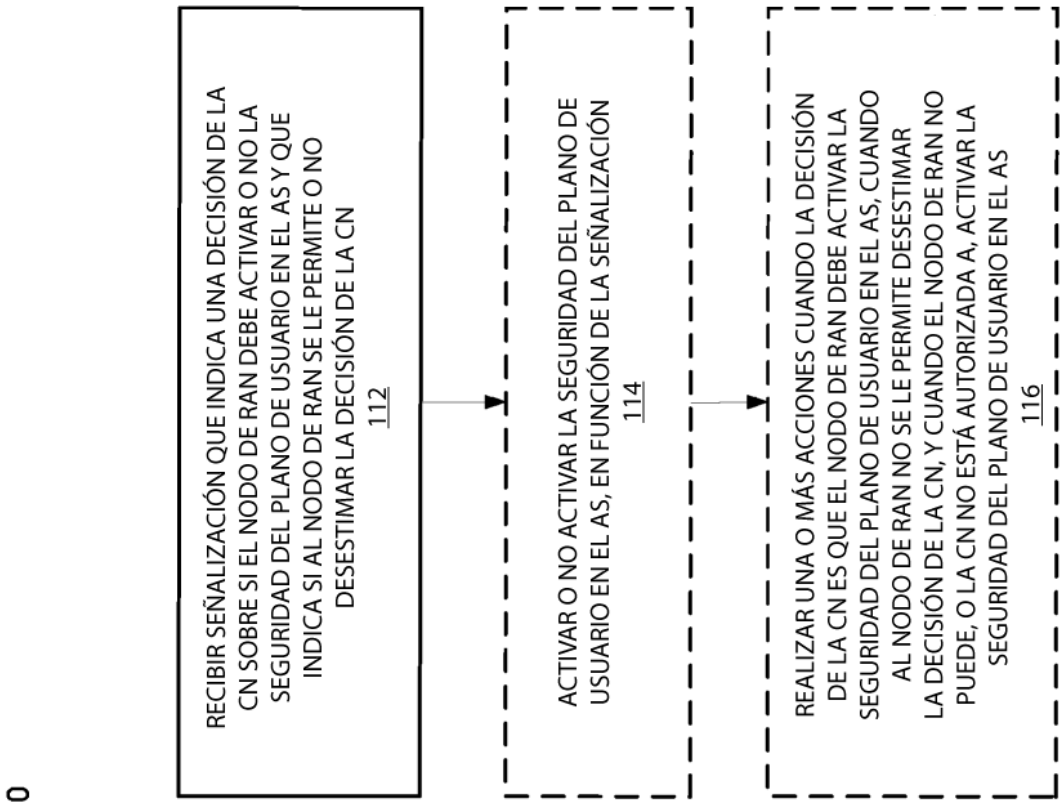

FIGURA 2B

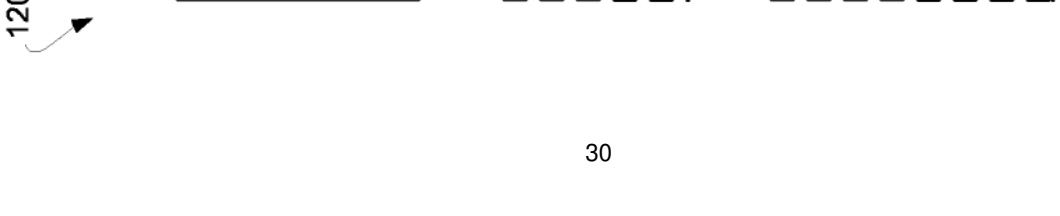

FIGURA 2C

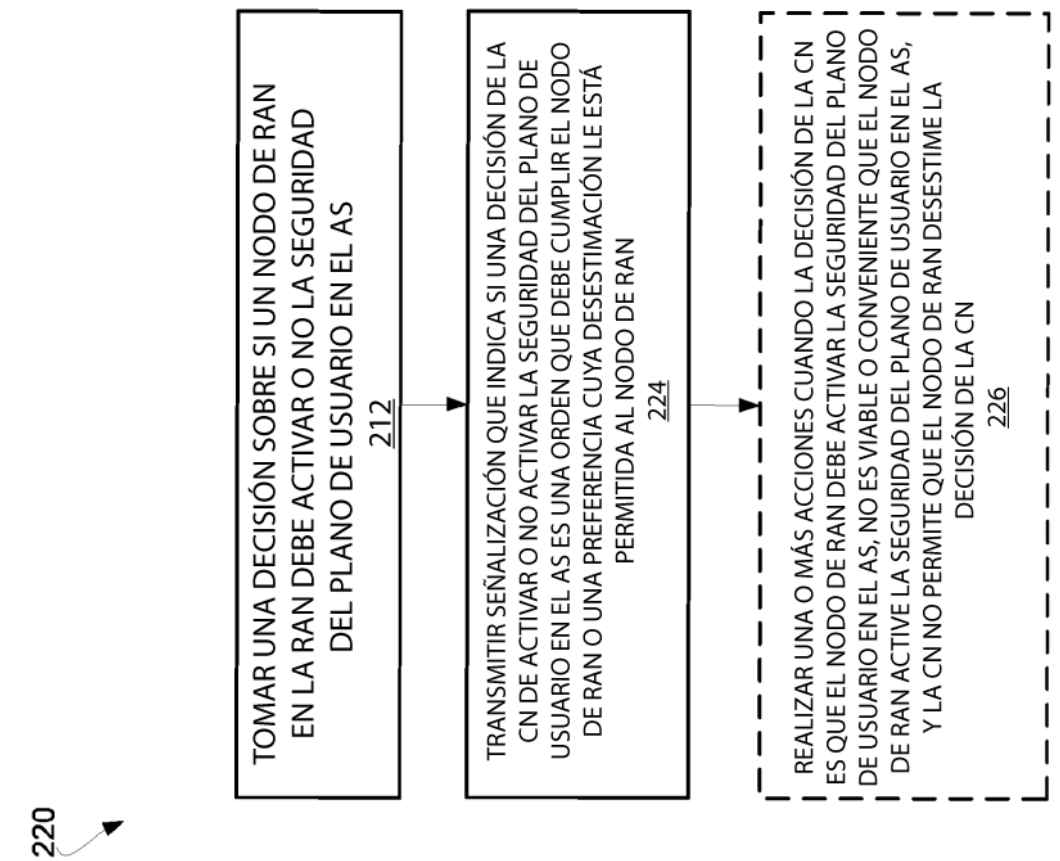

FIGURA 3C

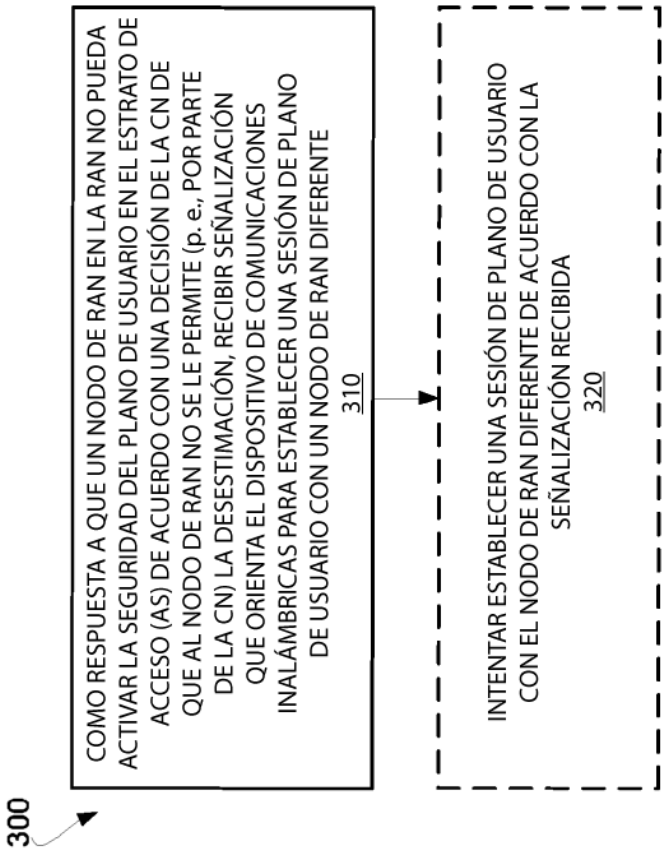
300
COMO RESPUESTA A QUE UN NODO DE RAN EN LA RAN NO PUEDA ACTIVAR LA SEGURIDAD DEL PLANO DE USUARIO EN EL ESTRATO DE ACCESO (AS) DE ACUERDO CON UNA DECISIÓN DE LA CN DE QUE AL NODO DE RAN NO SE LE PERMITE (p. e., POR PARTE DE LA CN) LA DESESTIMACIÓN, RECIBIR SEÑALIZACIÓN QUE ORIENTA EL DISPOSITIVO DE COMUNICACIONES INALÁMBRICAS PARA ESTABLECER UNA SESIÓN DE PLANO DE USUARIO CON UN NODO DE RAN DIFERENTE
310
INTENTAR ESTABLECER UNA SESIÓN DE PLANO DE USUARIO CON EL NODO DE RAN DIFERENTE DE ACUERDO CON LA SEÑALIZACIÓN RECIBIDA
320

FIGURA 4

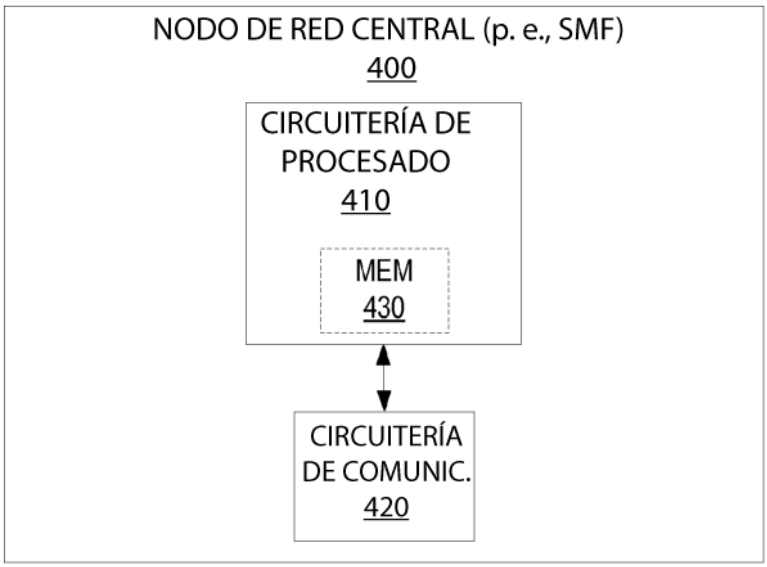

FIGURA 5A

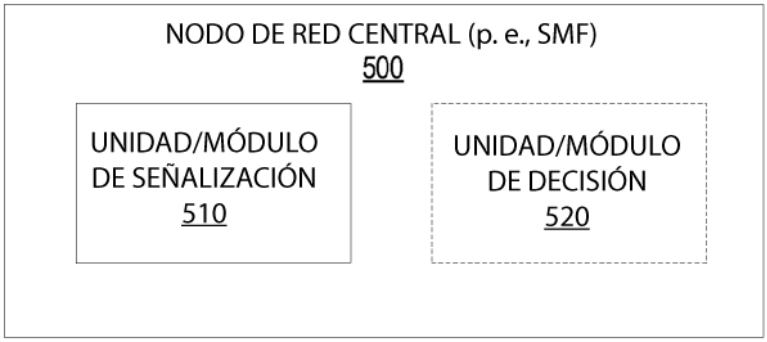

FIGURA 5B

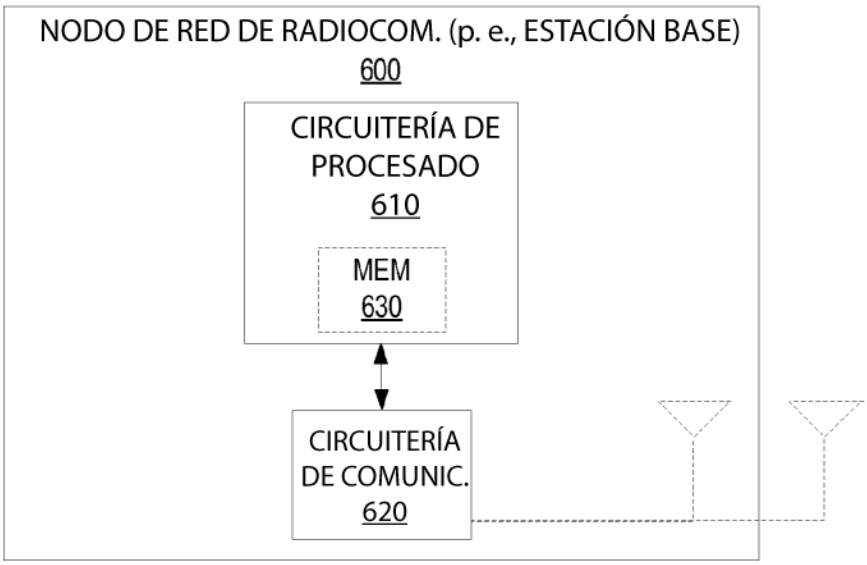

FIGURA 6A

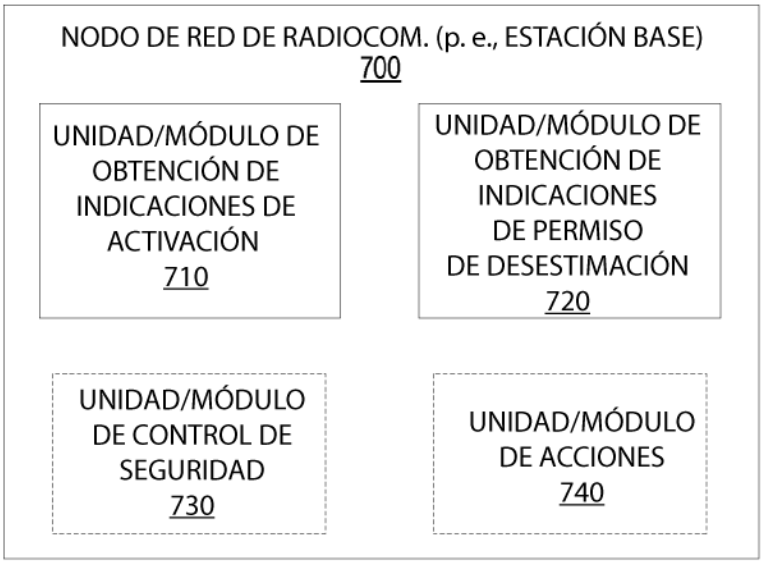

FIGURA 6B

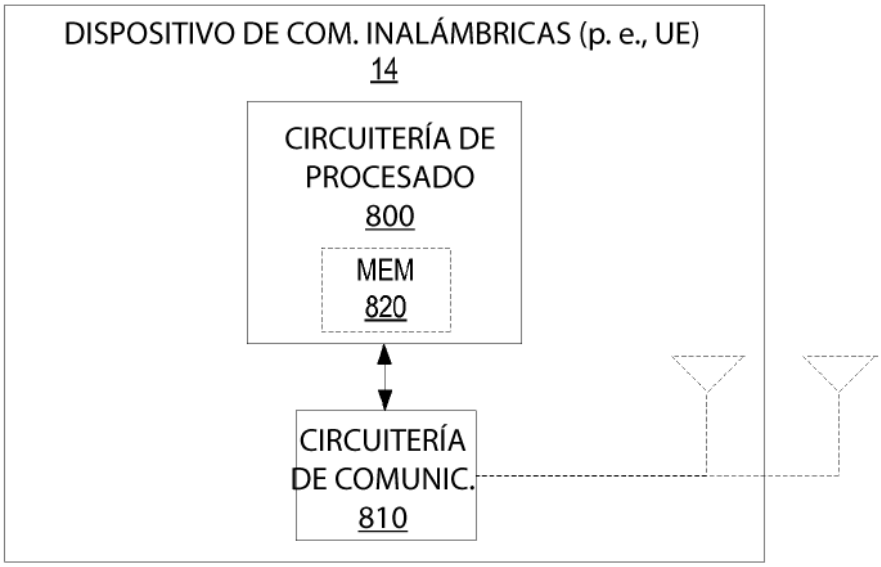

FIGURA 7A

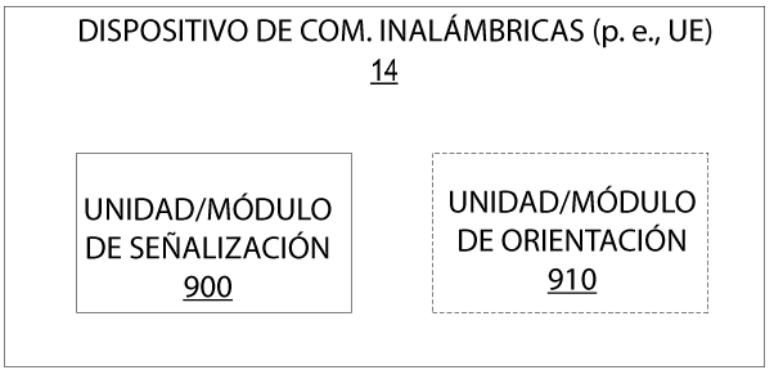

FIGURA 7B

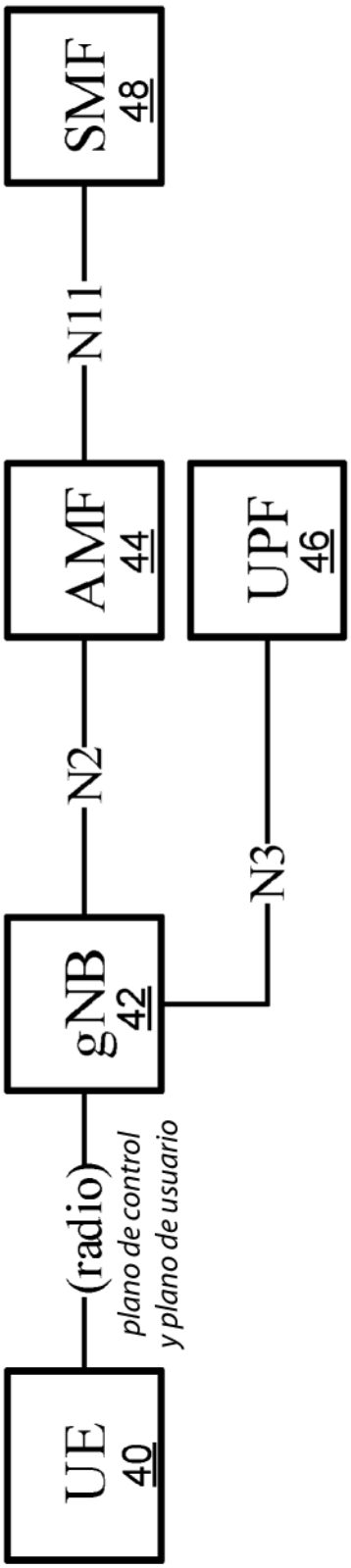
UE
40
(radio)
plano de control
y plano de usuario
gNB
42
N2
AMF
44
N11
SMF
48
N3
UPF
46

FIGURA 8

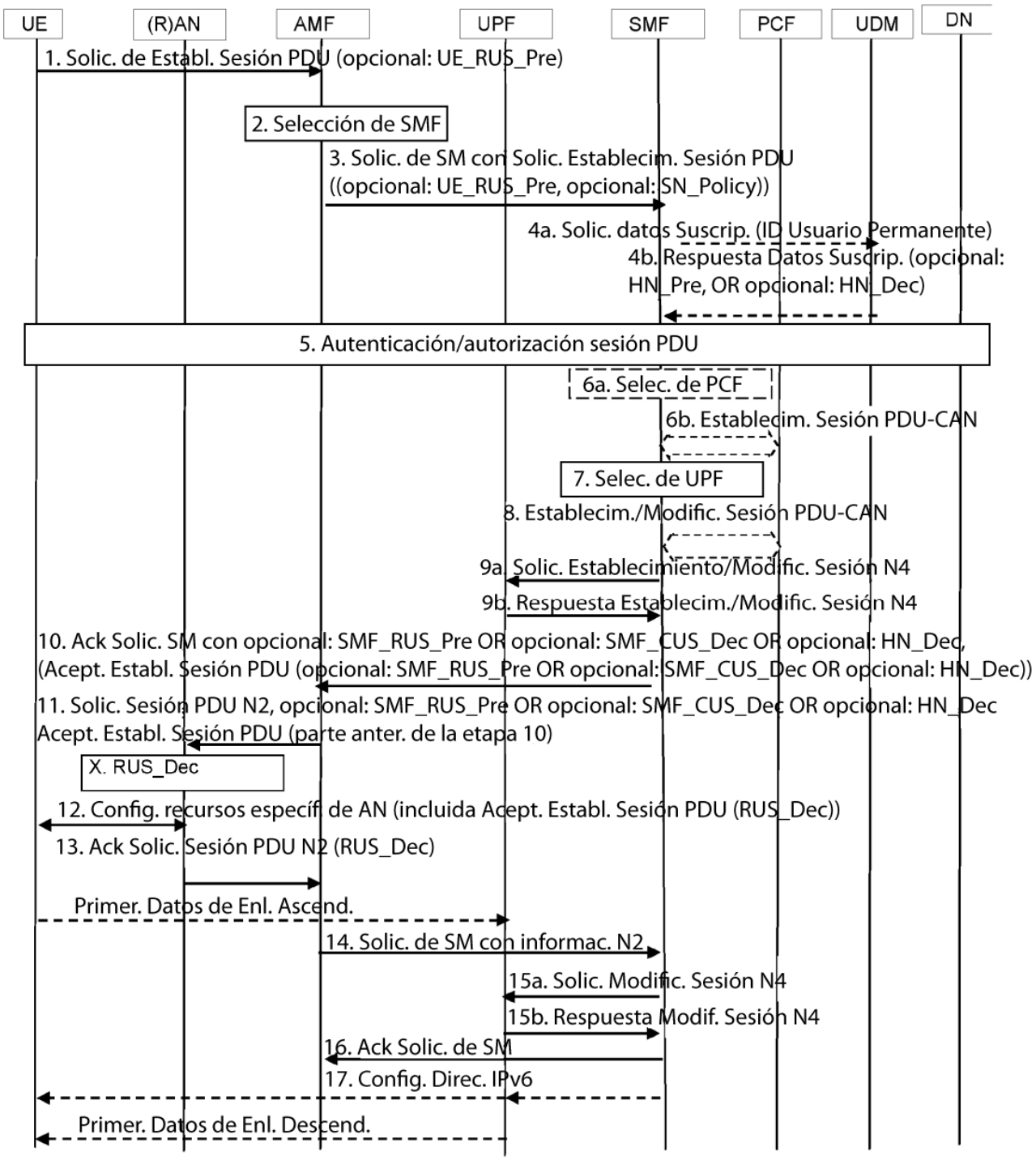
UE
(R)AN
AMF
UPF
SMF
PCF
UDM
DN
1. Solic. de Establ. Sesión PDU (opcional: UE_RUS_Pre)
2. Selección de SMF
3. Solic. de SM con Solic. Establecim. Sesión PDU ((opcional: UE_RUS_Pre, opcional: SN_Policy))
4a. Solic. datos Suscrip. (ID Usuario Permanente)
4b. Respuesta Datos Suscrip. (opcional: HN_Pre, OR opcional: HN_Dec)
5. Autenticación/autorización sesión PDU
6a. Selec. de PCF
6b. Establecim. Sesión PDU-CAN
7. Selec. de UPF
8. Establecim./Modific. Sesión PDU-CAN
9a. Solic. Establecimiento/Modific. Sesión N4
9b. Respuesta Establecim./Modific. Sesión N4
10. Ack Solic. SM con opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec, (Acept. Establ. Sesión PDU (opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec))
11. Solic. Sesión PDU N2, opcional: SMF_RUS_Pre OR opcional: SMF_CUS_Dec OR opcional: HN_Dec
Acept. Establ. Sesión PDU (parte anter. de la etapa 10)
X. RUS_Dec
12. Config. recursos específ. de AN (incluida Acept. Establ. Sesión PDU (RUS_Dec))
13. Ack Solic. Sesión PDU N2 (RUS_Dec)
Primer. Datos de Enl. Ascend.
14. Solic. de SM con informac. N2
15a. Solic. Modific. Sesión N4
15b. Respuesta Modif. Sesión N4
16. Ack Solic. de SM
17. Config. Direc. IPv6
Primer. Datos de Enl. Descend.

FIGURA 9

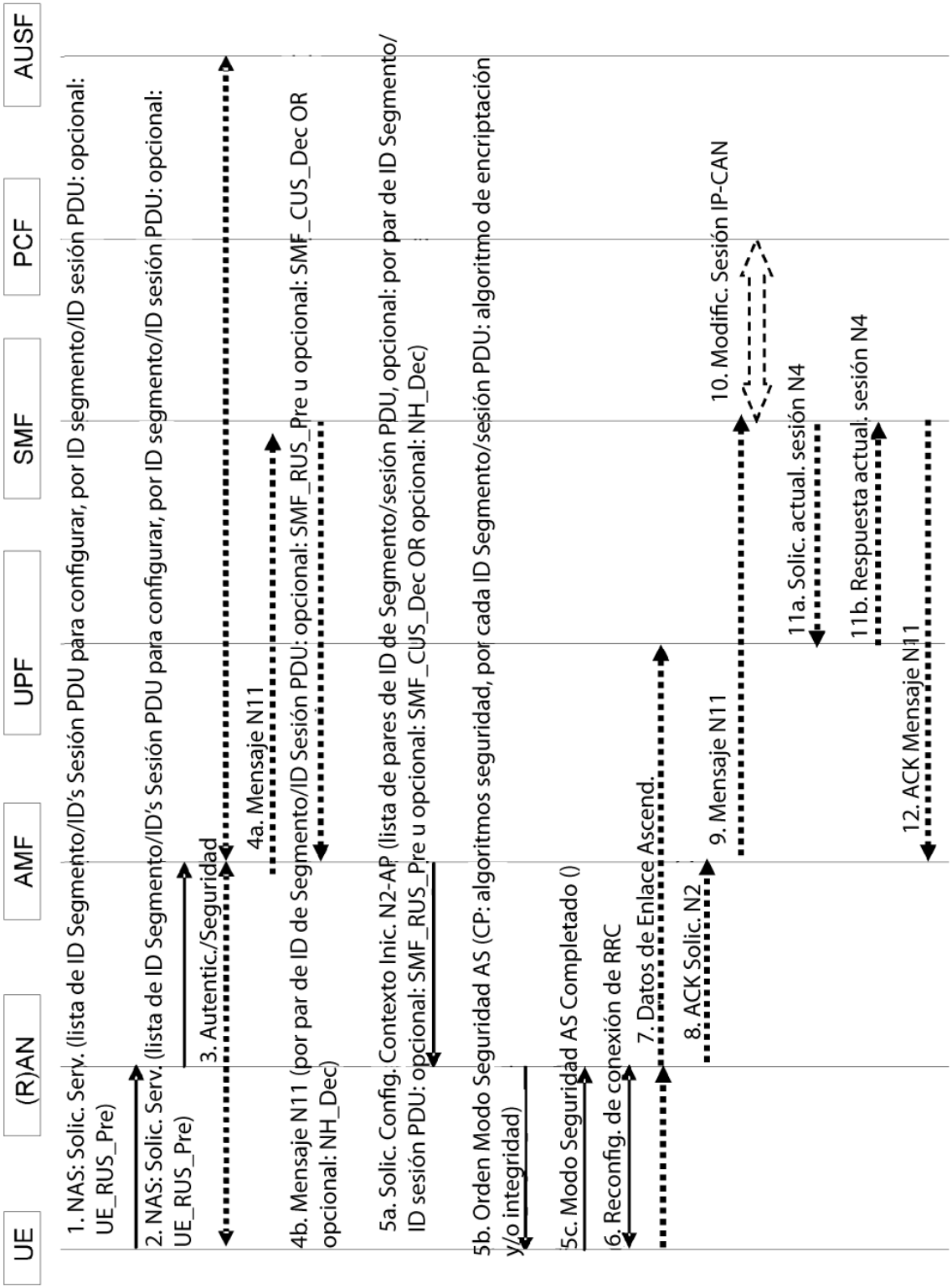
UE
(R)AN
AMF
UPF
SMF
PCF
AUSF
1. NAS: Solic. Serv. (lista de ID Segmento/ID's Sesión PDU para configurar, por ID segmento/ID sesión PDU: opcional: UE_RUS_Pre)
2. NAS: Solic. Serv. (lista de ID Segmento/ID's Sesión PDU para configurar, por ID segmento/ID sesión PDU: opcional: UE_RUS_Pre)
3. Autentic./Seguridad
4a. Mensaje N11
4b. Mensaje N11 (por par de ID de Segmento/ID Sesión PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: NH_Dec)
5a. Solic. Config. Contexto Inic. N2-AP (lista de pares de ID de Segmento/sesión PDU, opcional: por par de ID Segmento/ ID sesión PDU: opcional: SMF_RUS_Pre u opcional: SMF_CUS_Dec OR opcional: NH_Dec)
5b. Orden Modo Seguridad AS (CP: algoritmos seguridad, por cada ID Segmento/sesión PDU: algoritmo de encriptación y/o integridad)
5c. Modo Seguridad AS Completado ()
6. Reconfig. de conexión de RRC
7. Datos de Enlace Ascend.
8. ACK Solic. N2
9. Mensaje N11
10. Modific. Sesión IP-CAN
11a. Solic. actual. sesión N4
11b. Respuesta actual. sesión N4
12. ACK Mensaje N11

FIGURA 10

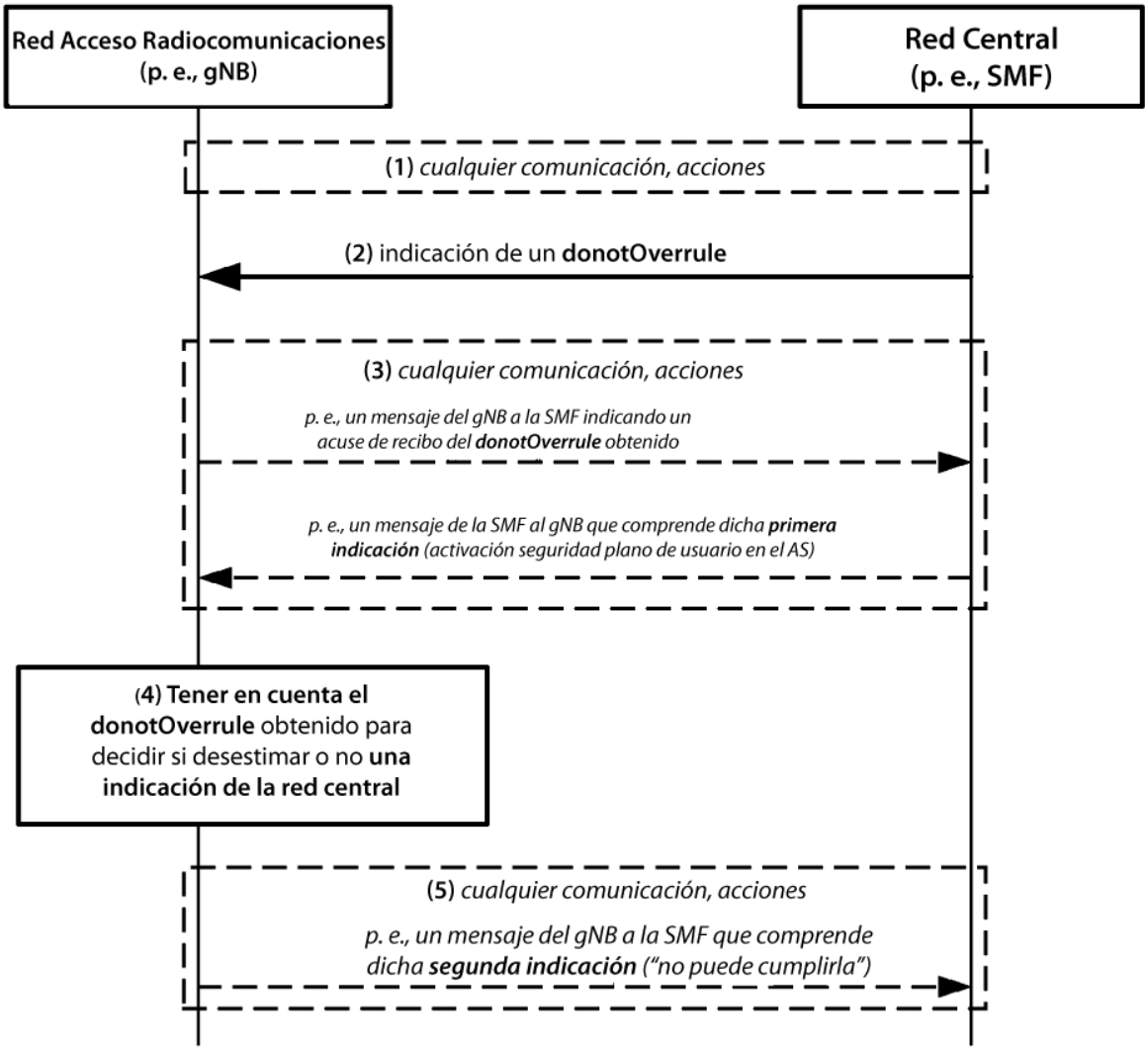
Red Acceso Radiocomunicaciones (p. e., gNB)
Red Central (p. e., SMF)
(1) cualquier comunicación, acciones
(2) indicación de un donotOverrule
(3) cualquier comunicación, acciones
p. e., un mensaje del gNB a la SMF indicando un acuse de recibo del donotOverrule obtenido
p. e., un mensaje de la SMF al gNB que comprende dicha primera indicación (activación seguridad plano de usuario en el AS)
(4) Tener en cuenta el donotOverrule obtenido para decidir si desestimar o no una indicación de la red central
(5) cualquier comunicación, acciones
p. e., un mensaje del gNB a la SMF que comprende dicha segunda indicación ("no puede cumplirla")

FIGURA 11

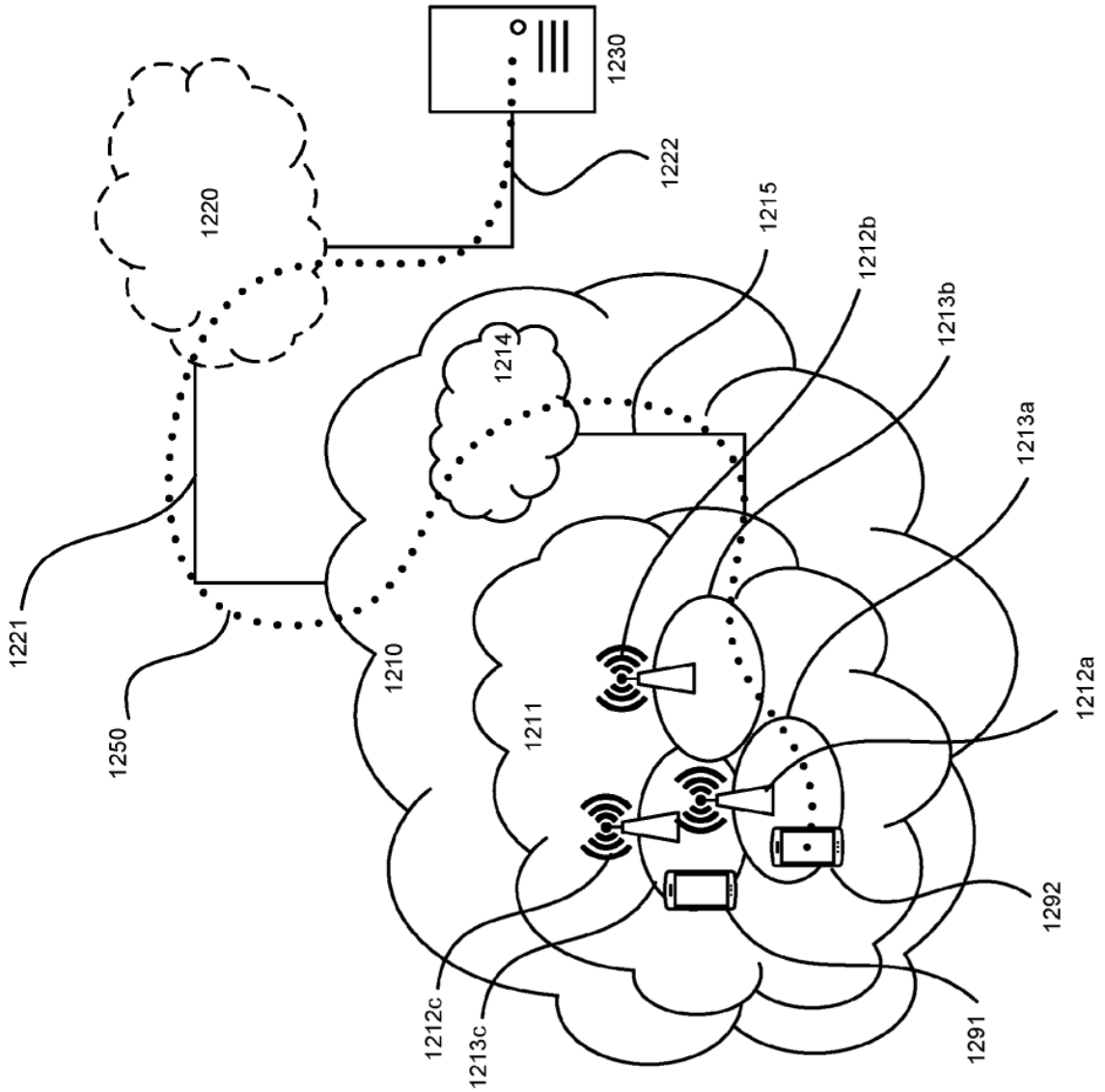
1230
1222
1220
1215
1212b
1213b
1214
1213a
1221
1210
1211
1212a
1250
1292
1212c
1213c
1291

FIGURA 12

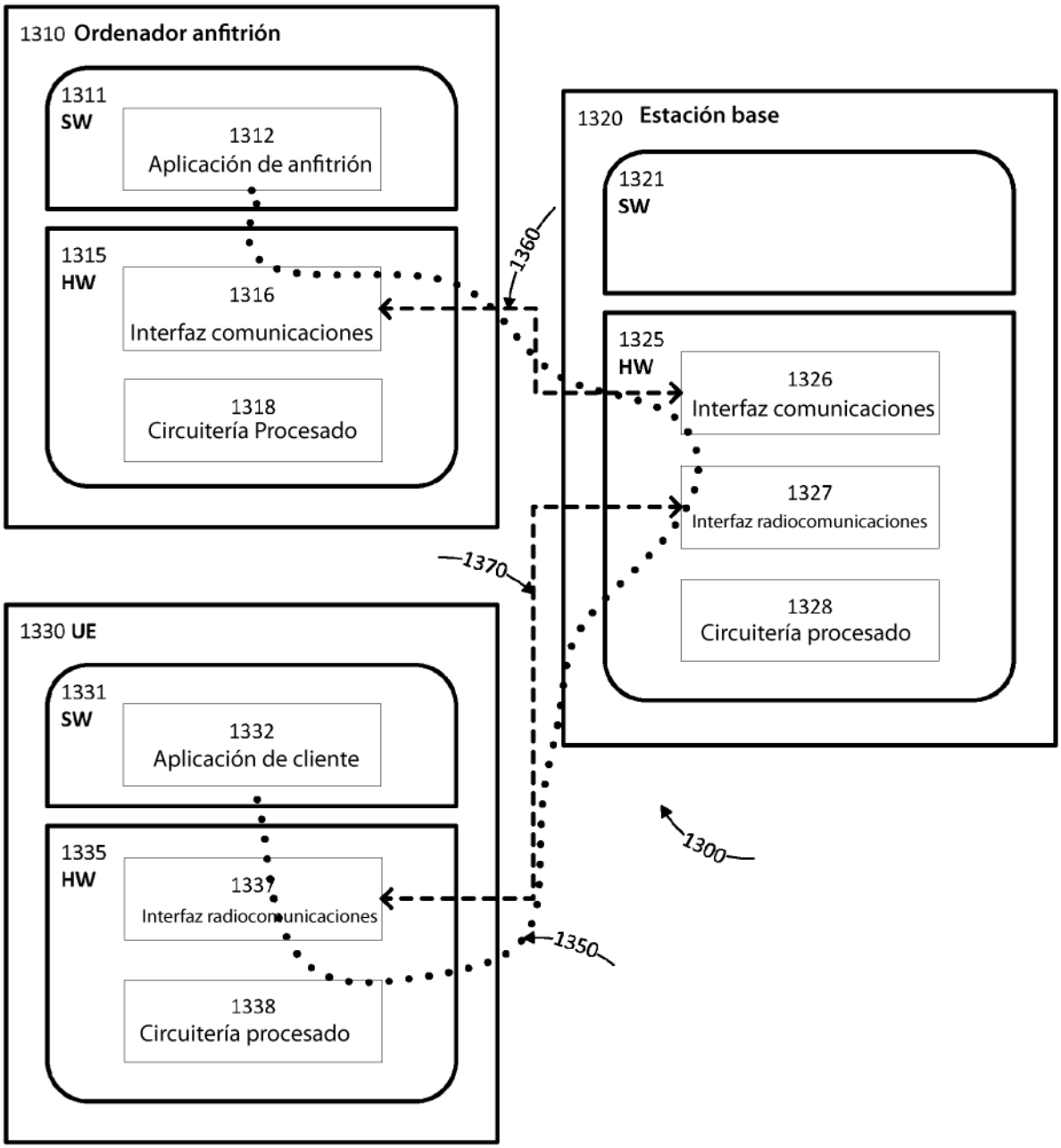
1310 Ordenador anfitrión
1311
SW
1312
Aplicación de anfitrión
1315
HW
1316
Interfaz comunicaciones
1318
Circuitería Procesado
1320 Estación base
1321
SW
1325
HW
1326
Interfaz comunicaciones
1327
Interfaz radiocomunicaciones
1328
Circuitería procesado
1330 UE
1331
SW
1332
Aplicación de cliente
1335
HW
1337
Interfaz radiocomunicaciones
1338
Circuitería procesado
1360
1370
1350
1300

FIGURA 13

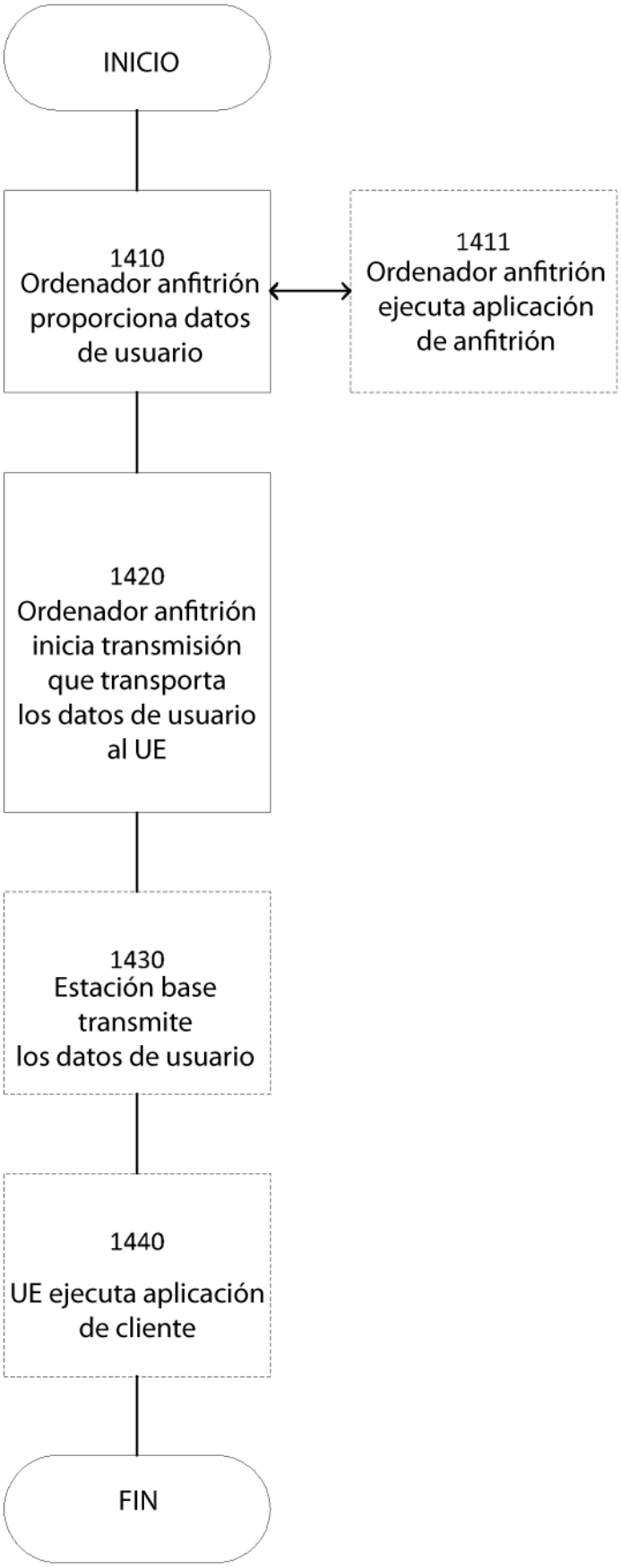
INICIO
1410
Ordenador anfitrión proporciona datos de usuario
1411
Ordenador anfitrión ejecuta aplicación de anfitrión
1420
Ordenador anfitrión inicia transmisión que transporta los datos de usuario al UE
1430
Estación base transmite los datos de usuario
1440
UE ejecuta aplicación de cliente
FIN

FIGURA 14


INICIO
1510
Ordenador anfitrión proporciona datos de usuario
1520
Ordenador anfitrión inicia transmisión que transporta los datos de usuario al UE
1530
UE recibe los datos de usuario
FIN

FIGURA 15

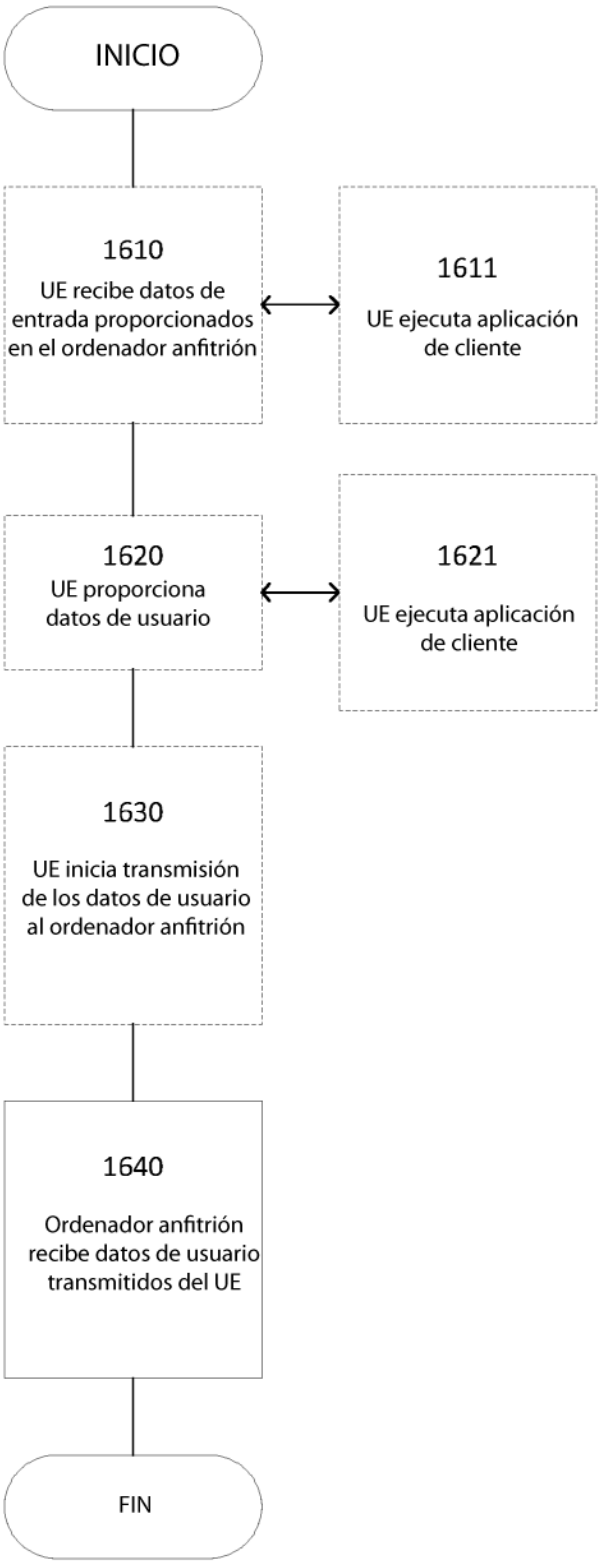
INICIO
1610
UE recibe datos de entrada proporcionados en el ordenador anfitrión
1611
UE ejecuta aplicación de cliente
1620
UE proporciona datos de usuario
1621
UE ejecuta aplicación de cliente
1630
UE inicia transmisión de los datos de usuario al ordenador anfitrión
1640
Ordenador anfitrión recibe datos de usuario transmitidos del UE
FIN

FIGURA 16

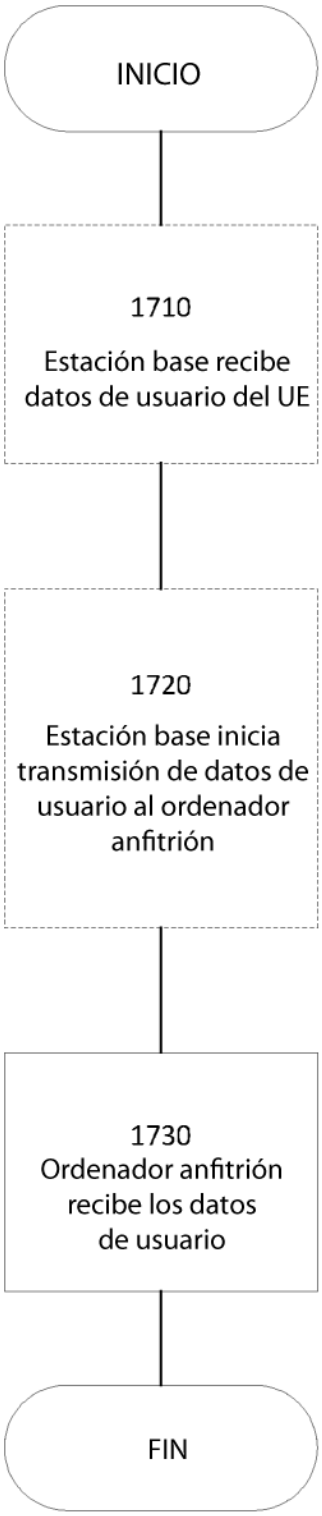
INICIO
1710
Estación base recibe datos de usuario del UE
1720
Estación base inicia transmisión de datos de usuario al ordenador anfitrión
1730
Ordenador anfitrión recibe los datos de usuario
FIN

FIGURA 17