(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 012 708**

(51) Int. CI.:

H04W 12/04 (2011.01)
H04W 88/06 (2009.01)
H04W 12/041 (2011.01)
H04W 8/04 (2009.01)
H04W 12/08 (2011.01)
H04W 12/106 (2011.01)
H04W 60/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.12.2015 E 22189016 (3)**

(97) Fecha y número de publicación de la concesión europea: **05.02.2025 EP 4102871**

(54) Título: **Configuración de seguridad multi-RAT**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.04.2025

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.00%)
164 83 Stockholm, SE

(72) Inventor/es:

YILMAZ, OSMAN NURI CAN;
WAGER, STEFAN;
DA SILVA, ICARO LEONARDO;
NORRMAN, KARL y
SCHLIWA-BERTLING, PAUL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Configuración de seguridad multi-RAT

Campo técnico

La presente divulgación se refiere en general al campo de la configuración del contexto de seguridad. Más específicamente, la presente divulgación se refiere a técnicas para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica.

Antecedentes

La seguridad es un aspecto crucial en los sistemas de comunicación móvil actuales. Por ejemplo, el diseño de seguridad de evolución a largo plazo (LTE) proporciona compartimentación. La compartimentación consiste principalmente en garantizar que si un atacante viola la seguridad de una función, solo esa función se ve comprometida. Por ejemplo, hay una clave utilizada para el cifrado del protocolo de control de recursos de radio (RRC) y otra clave utilizada para la protección de la integridad del protocolo RRC. RRC es un protocolo de señalización que utiliza capas inferiores para la segmentación y la entrega en orden confiable de los mensajes de señalización. RRC es adecuado para mensajes de cualquier tamaño que requieran una entrega confiable, tal como la configuración de equipo de usuario (UE). En LTE y LTE-advanced (LTE-a), RRC está involucrado en el intercambio de mensajes de estrato de no acceso (NAS) entre un UE y una entidad de gestión de la movilidad (MME), así como para proporcionar varias funciones del plano de control tanto en el UE como en el Nodo B evolucionado (eNodoB o, de manera abreviada, eNB).

La seguridad de estrato de acceso (AS) se compone de protección de la integridad del plano de control (es decir, señalización RRC) y el cifrado de los planos tanto de control como de usuario. Si un atacante viola la clave de cifrado RRC, el atacante puede descifrar y leer todos los mensajes RRC. Sin embargo, dado que la clave de integridad es diferente de la clave de cifrado, el atacante no puede modificar ni inyectar mensajes RRC. Un atacante que haya violado la clave de cifrado RRC tampoco puede utilizarla para interceptar las portadoras de radio de datos (DRB), dado que utilizan claves de cifrado separadas (y viceversa). Otra parte del diseño de compartimentación es que cada eNB utiliza un conjunto de claves separado. La razón es que esto garantiza que un atacante que irrumpa en un eNB no obtenga ninguna información sobre los datos transmitidos entre un UE y otro eNB físicamente diferente. Para mantener la propiedad de que irrumpir en un nodo físico de la red de acceso por radio (RAN), es decir, un eNB, no ayuda a atacar otro nodo de RAN, el eNB auxiliar debe usar su propio conjunto de claves separado del conjunto de claves utilizado en el eNB de anclaje, sin embargo, puede derivarse del eNB de anclaje como en la conectividad dual de LTE.

Típicamente, cuando se estandariza una nueva tecnología de acceso por radio (RAT), esto se hace introduciendo también una red central separada que atienda a esa RAT y 3GPP introduce mecanismos para pasar de una RAT a otra RAT con una interrupción mínima del servicio a través de la red central. Por lo tanto, en cualquier caso, pasar de una RAT a otra RAT significa establecer una conexión RRC hacia la RAT objetivo y eliminar la conexión RRC de la RAT de origen, y debido a que esas conexiones RRC terminan en diferentes nodos lógicos anclados en diferentes redes centrales (es decir, son conexiones de UE completamente separadas), no hay posibilidad de sinergia entre ellas.

El establecimiento de una portadora de señalización y/o portadora de datos y/o la recuperación de una portadora de señalización y/o portadora de datos requieren una serie de pasos de señalización, lo que da como resultado, por ejemplo, una sobrecarga de señalización y/o una larga duración de la señalización. Los procedimientos de señalización actuales para la configuración del contexto de seguridad no han sido diseñados o al menos optimizados para soportar una arquitectura RAN que esté compuesta por múltiples interfaces aéreas como en las redes multi-RAT. Este es el caso incluso cuando las conexiones de la primera y la segunda RAT del UE serían hacia el mismo, o en otras palabras, un nodo de radio compartido y/o nodo de red central.

Además, el contexto de seguridad puede ser diferente para diferentes RAT (a pesar de la integración estrecha) o versiones estándar o capacidades de UE o categorías de dispositivos. Por ejemplo, puede haber diferentes requisitos de longitud para las claves de seguridad de diferentes RAT o la terminación de la red puede estar en nodos separados, lo que requiere conjuntos de claves separados.

La técnica anterior relevante está representada por la literatura de patentes EP 2 648 437 A1 y US 2013/044709 A1.

Compendio

Por consiguiente, existe la necesidad de una técnica mejorada para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica multi-RAT. La invención está definida por las reivindicaciones independientes adjuntas.

Según un primer aspecto, se proporciona un método para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El método comprende iniciar, por un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica, la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común.

De esta manera, se reduce la señalización para la configuración del contexto de seguridad de AS para la primera y la segunda RAT, es decir, un entorno multi-RAT. Como consecuencia, puede simplificarse la configuración del contexto de seguridad multi-RAT.

El término tecnología de acceso por radio (RAT) puede entenderse como la técnica de conexión física subyacente para una red de comunicación basada en radio. El elemento de red de acceso por radio puede comprender o configurarse como una estación base de una red de acceso por radio.

El procedimiento de señalización común puede comprender el intercambio de uno o más mensajes relacionados tanto con la primera RAT como con la segunda RAT.

El método puede comprender recibir, por el elemento de RAN, un primer material de clave de RAN desde un elemento de red central (CN) de la red de comunicación inalámbrica. El primer material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la primera RAT. El método comprende además recibir, por el elemento de RAN, un segundo material de clave de RAN desde el elemento de CN de la red de comunicación inalámbrica. El segundo material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la segunda RAT.

En este caso, pueden señalizarse dos materiales de clave separados a la RAN, uno para la primera RAT y otro para la segunda RAT. El material de clave puede utilizarse para configurar el contexto de seguridad. El material de clave recibido desde la CN puede, pero no tiene por qué, utilizarse directamente en la configuración del contexto de seguridad; por ejemplo, puede utilizarse más adelante.

El método puede comprender recibir, por el elemento de RAN, un primer material de clave de RAN de un elemento de CN de la red de comunicación inalámbrica. El primer material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la primera RAT. El método puede comprender además derivar, por el elemento de RAN, un segundo material de clave de RAN a partir del primer material de clave de RAN recibido. El segundo material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la segunda RAT.

En este caso, el primer material de clave de RAN para la primera RAT puede utilizarse para derivar el material de clave para la segunda RAT. El material de clave puede utilizarse entonces para configurar el contexto de seguridad.

El paso de iniciar la configuración del contexto de seguridad de AS puede incluir utilizar directamente el primer material de clave de RAN recibido para iniciar la configuración del contexto de seguridad de AS para la primera RAT. Alternativamente, el paso de iniciar la configuración del contexto de seguridad de AS puede incluir derivar un tercer material de clave de RAN a partir del primer material de clave de RAN recibido y utilizar el tercer material de clave de RAN derivado para iniciar la configuración del contexto de seguridad de AS para la primera RAT. Por ejemplo, el primer material de clave de RAN recibido desde la CN puede, pero no tiene por qué, utilizarse directamente en la configuración del contexto de seguridad, por ejemplo, puede utilizarse más adelante. Por ejemplo, un tercer material de clave de RAN puede derivarse a partir del primer material de clave de RAN y el tercer material de clave de RAN puede utilizarse para configurar el contexto de seguridad para la primera RAT. Como el segundo material de clave de RAN se deriva a partir del primer material de clave de RAN recibido, la señalización para la configuración de seguridad de AS para la primera y la segunda RAT, es decir, un entorno multi-RAT, se reduce aún más. Como consecuencia, la configuración del contexto de seguridad multi-RAT puede simplificarse aún más.

En una o más realizaciones, el paso de iniciar la configuración del contexto de seguridad de AS puede comprender transmitir, por el elemento de RAN, un mensaje de comando de modo de seguridad de AS común para la primera RAT y la segunda RAT a un dispositivo de comunicación inalámbrica de la red de comunicación inalámbrica.

El método puede comprender recibir, por el elemento de RAN, un mensaje de modo de seguridad de AS completo que informa al elemento de RAN de la finalización de la configuración del contexto de seguridad de AS para la primera RAT y la segunda RAT.

El elemento de RAN puede corresponder al elemento de RAN que implementa la primera RAT. Además, el elemento de RAN puede corresponder al elemento de RAN que implementa la segunda RAT o puede ser diferente del mismo.

Según un segundo aspecto, se proporciona un método para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El método comprende informar, por un elemento de red central (CN) de la red de comunicación inalámbrica, a un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica, que inicie la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común.

El método puede comprender recibir, por el elemento de CN desde un dispositivo de comunicación inalámbrica, información sobre las capacidades de seguridad del dispositivo de comunicación inalámbrica con respecto a la primera RAT y la segunda RAT.

El método puede comprender iniciar, por el elemento de CN, la configuración del contexto de seguridad de estrato de

no acceso (NAS) para la primera RAT y la segunda RAT en un procedimiento de señalización común.

De esta manera, se reduce la señalización para la configuración del contexto de seguridad de NAS para la primera y la segunda RAT, es decir, un entorno multi-RAT. Como consecuencia, la configuración del contexto de seguridad multi-RAT puede simplificarse aún más.

El procedimiento de señalización común puede comprender el intercambio de uno o más mensajes relacionados tanto con la primera RAT como con la segunda RAT.

El paso de iniciar la configuración del contexto de seguridad de NAS puede comprender solicitar, por el elemento de CN, a un dispositivo de comunicación inalámbrica que realice la autenticación hacia el elemento de CN.

El método puede comprender derivar, por el elemento de CN, material de clave de CN que permita a un dispositivo de comunicación inalámbrica realizar la autenticación para la primera RAT y que permita al dispositivo de comunicación inalámbrica realizar la autenticación para la segunda RAT.

El método puede comprender transmitir, por el elemento de CN, el material de clave de CN al dispositivo de comunicación inalámbrica.

El método puede comprender recibir, por el elemento de CN, un mensaje de respuesta de autenticación desde el dispositivo de comunicación inalámbrica.

El método puede comprender derivar, por el elemento de CN, material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS.

El método puede comprender transmitir, por el elemento de CN, de un mensaje de comando de modo de seguridad de NAS para la primera RAT y la segunda RAT al dispositivo de comunicación inalámbrica. El mensaje de comando de modo de seguridad de NAS permite al dispositivo de comunicación inalámbrica derivar el material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS.

El método puede comprender recibir, por el elemento de CN, un mensaje de modo de seguridad de NAS completo para la primera RAT y la segunda RAT desde el dispositivo de comunicación inalámbrica.

Según un tercer aspecto, se proporciona un método para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El método comprende recibir, por un dispositivo de comunicación inalámbrica de la red de comunicación inalámbrica desde un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica en un procedimiento de señalización común, información que permite a la comunicación inalámbrica configurar un contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT. El método comprende además configurar, por el dispositivo de comunicación inalámbrica, el contexto de seguridad de AS para la primera RAT y la segunda RAT.

El método puede comprender recibir, por el dispositivo de comunicación inalámbrica desde el elemento de RAN de la red de comunicación inalámbrica, un mensaje de comando de modo de seguridad de AS común para la primera RAT y la segunda RAT.

El método puede comprender transmitir, por el dispositivo de comunicación inalámbrica, un mensaje de modo de seguridad de AS completo al elemento de RAN. El mensaje de finalización del modo de seguridad de AS puede informar al elemento de RAN de la finalización de la configuración del contexto de seguridad de AS para la primera RAT y la segunda RAT.

El método puede comprender transmitir, por el dispositivo de comunicación inalámbrica a un elemento de red central (CN) de la red de comunicación inalámbrica, información sobre las capacidades de seguridad del dispositivo de comunicación inalámbrica con respecto a la primera RAT y la segunda RAT.

El método puede comprender recibir, por el dispositivo de comunicación inalámbrica desde un elemento de CN, una solicitud para realizar una autenticación hacia el elemento de CN.

El método puede comprender transmitir, por el dispositivo de comunicación inalámbrica, un mensaje de respuesta de autenticación al elemento de CN.

El método puede comprender recibir, por el dispositivo de comunicación inalámbrica, un mensaje de comando de modo de seguridad de NAS para la primera RAT y la segunda RAT desde el elemento de CN. El método puede comprender además derivar, por el dispositivo de comunicación inalámbrica, material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS para la primera RAT y la segunda RAT a partir del mensaje de comando de modo de seguridad de NAS recibido.

El método puede comprender transmitir, por el dispositivo de comunicación inalámbrica, un mensaje de modo de seguridad de NAS completo para la primera RAT y la segunda RAT al elemento de CN.

Según un cuarto aspecto, se proporciona un programa informático. El programa informático comprende partes de código de programa para hacer que se realicen los pasos de cualquiera de los aspectos del método descritos en la presente memoria, cuando el programa informático se ejecuta en un sistema informático o en uno o más dispositivos informáticos. El programa informático puede almacenarse en un medio de registro legible por ordenador o puede ser descargable como una señal.

Según un quinto aspecto, se proporciona un elemento de red de acceso por radio (RAN) para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El elemento de RAN comprende un componente de iniciación configurado para iniciar la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común.

El elemento de RAN puede ser o comprender al menos uno del elemento de red de acceso por radio que implementa la primera RAT y el elemento de red de acceso por radio que implementa la segunda RAT.

El elemento de RAN puede configurarse para realizar el método de cualquiera de los pasos del método descritos en la presente memoria con respecto al primer aspecto. El elemento de RAN puede comprender o configurarse como o ser parte de una estación base de radio, un controlador de red de radio (RNC), un nodoB, un eNodoB, un controlador de unidad de radio de 5G o una estación base de 5G.

Según un sexto aspecto, se proporciona un elemento de red central (CN) para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El elemento de CN comprende un componente de información configurado para informar a un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica que inicie la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común.

El elemento de CN puede configurarse para realizar el método de cualquiera de los pasos del método descritos en la presente memoria con respecto al segundo aspecto.

Según un séptimo aspecto, se proporciona un dispositivo de comunicación inalámbrica para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El dispositivo de comunicación inalámbrica comprende un componente de recepción y un componente de configuración. El componente de recepción está configurado para recibir, desde un elemento de red de acceso por radio (RAN) en un procedimiento de señalización común, información que permite al dispositivo de comunicación inalámbrica configurar un contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT. El componente de configuración se configura para configurar el contexto de seguridad de AS para la primera RAT y la segunda RAT.

El dispositivo de comunicación inalámbrica puede configurarse para realizar el método de cualquiera de los pasos del método descritos en la presente memoria con respecto al tercer aspecto. El dispositivo de comunicación inalámbrica puede comprender o configurarse como o ser parte de un equipo de usuario (UE).

Según un octavo aspecto, se proporciona un sistema de comunicación inalámbrica. El sistema de comunicación inalámbrica comprende el elemento de RAN como se describe en la presente memoria, el elemento de CN como se describe en la presente memoria y uno o más dispositivos de comunicación inalámbrica, tales como equipos de usuario (UE). El sistema de comunicación inalámbrica puede configurarse para realizar los pasos de cualquiera de los aspectos del método como se describe en la presente memoria.

En general, los pasos de cualquiera de los aspectos del método descritos en la presente memoria pueden realizarse igualmente en uno o más componentes, dispositivos o unidades adecuados, por ejemplo, en componentes adecuados del elemento de RAN, el elemento de CN, el dispositivo de comunicación inalámbrica y/o el sistema de comunicación inalámbrica.

Breve descripción de los dibujos

A continuación, se describirá con más detalle la presente divulgación con referencia a las realizaciones ejemplares ilustradas en las Figuras, en las que:

la Figura 1 es un diagrama de flujo que ilustra los pasos de señalización relacionados con la configuración de seguridad de LTE;

la Figura 2 es una ilustración esquemática de una realización de un sistema que comprende una realización de dispositivo de un dispositivo de comunicación inalámbrica, una realización de dispositivo de un elemento de red de acceso por radio y una realización de dispositivo de un elemento de red central;

la Figura 3 es un diagrama de flujo que ilustra una realización de un método realizada en el sistema de la Figura 2;

la Figura 4 es una ilustración esquemática de las interfaces entre nodos para la RAN de 5G;

la Figura 5 es una ilustración esquemática de una arquitectura de protocolo para la interfaz aérea en la RAN de 5G;

la Figura 6 un diagrama de flujo que ilustra un procedimiento de conexión combinado a través de una única RAT que puede realizarse en el sistema de la Figura 2;

la Figura 7 es un diagrama de bloques que ilustra esquemáticamente una realización de un elemento de red de acceso por radio o un dispositivo de comunicación inalámbrica o un elemento de red central;

la Figura 8 es un diagrama de bloques que ilustra esquemáticamente una realización adicional de un elemento de red de acceso por radio;

la Figura 9 es un diagrama de bloques que ilustra esquemáticamente una realización adicional de un elemento de red central; y

la Figura 10 es un diagrama de bloques que ilustra esquemáticamente una realización adicional de un dispositivo de comunicación inalámbrica.

Descripción detallada

En la siguiente descripción, con fines explicativos y no limitativos, se exponen detalles específicos, tales como topologías de red específicas que incluyen nodos de red particulares, con el fin de proporcionar una comprensión completa de la presente divulgación. Será evidente para los expertos en la técnica que la presente divulgación puede ponerse en práctica en otras realizaciones que se apartan de estos detalles específicos. Por ejemplo, aunque la presente divulgación se describe principalmente con referencia a la evolución a largo plazo (LTE) como un ejemplo específico para una tecnología utilizada en una red de comunicación inalámbrica, la presente divulgación puede ponerse en práctica en cualquier red a la que puedan conectarse usuarios móviles o estacionarios que utilicen un equipo de usuario (UE) correspondiente. Por ejemplo, la presente divulgación es aplicable a otras redes celulares tales como redes del sistema global para las comunicaciones móviles (GSM), redes del sistema universal de telecomunicaciones móviles (UMTS), redes de LTE-Advanced (LTE-A), redes de 5G, redes WiFi o a la red de área local inalámbrica (WLAN) o redes inalámbricas similares y una combinación de las mismas.

Los expertos en la materia apreciarán además que las funciones explicadas a continuación en la presente memoria pueden implementarse utilizando circuitos de hardware individuales, utilizando software que funcione en conjunto con un microprocesador programado o un ordenador de propósito general, utilizando un circuito integrado de aplicación específica (ASIC) y/o utilizando uno o más procesadores de señales digitales (DSP). También se apreciará que cuando la presente divulgación se describe como un método, también puede realizarse en un procesador informático y una memoria acoplada a un procesador, en donde la memoria está codificada con uno o más programas para hacer que el procesador realice los métodos divulgados en la presente memoria cuando son ejecutados por el procesador.

Antes de explicar las realizaciones en detalle a continuación, se proporciona información general con respecto al contexto de UE y la configuración de seguridad.

El contexto de UE es un término general para referirse a un conjunto de parámetros y/o información de una asociación de UE y/o conexión de UE dada hacia un nodo de red dado. En el caso de LTE, por ejemplo, existen varios tipos de asociaciones de UE necesarias en el eNB, como se especifica en TS 36.401 V12.2.0 (2015-03). En ese caso, el "contexto de UE de eNB " puede utilizarse para almacenar toda la información necesaria para un UE en estado conectado y las asociaciones entre el UE y las conexiones lógicas S1 y X2 utilizadas para los mensajes asociados al UE de S1/X2-AP.

Más específicamente, el contexto de UE de eNB puede entenderse en el sentido de 3GPP TS 36.401 V12.2.0 (2015-03) como un bloque de información en un eNB asociado a un UE activo, por ejemplo en estado RRC_CONECTADO. El bloque de información puede contener la información necesaria requerida para mantener los servicios de E-UTRAN hacia el UE activo. Por ejemplo, una o más de la información de estado del UE, información de seguridad (por ejemplo, algoritmos, claves de seguridad y parámetros), información de capacidad del UE (por ejemplo, soporte de portadora, MIMO, formato de transmisión, etc.), identidades del UE (por ejemplo, C-RNTI, S-TMSI) y las identidades de la conexión S1 lógica asociada al UE pueden incluirse en el contexto de UE de eNB. El establecimiento del contexto de UE de eNB puede considerarse completado cuando se completa la transición al estado activo para un UE o en el eNB objetivo después de la finalización de la asignación de recursos de traspaso durante la preparación del traspaso, por ejemplo, la finalización del traspaso a E-UTRAN. En LTE, cuando no existe una conexión dedicada entre la E-UTRAN y el UE, no se almacena información de contexto de UE en E-UTRAN. Eso básicamente significa que el contexto de UE de eNB se descarta cuando el UE pasa del estado RRC_CONECTADO al estado RRC_INACTIVO.

Se crea un contexto de UE de MME cuando un UE se enciende y se conecta a la red. La MME asigna al UE una identidad temporal corta única denominada identidad temporal de abonado móvil SAE (S-TMSI) que identifica el contexto de UE en la MME. Este contexto de UE contiene información de suscripción del usuario descargada desde el servidor de abonado doméstico (HSS). El almacenamiento local de datos de suscripción en la MME permite una ejecución más rápida de procedimientos como el establecimiento de portadora, dado que elimina la necesidad de consultar el HSS cada vez. Además, el contexto de UE también contiene información dinámica tal como la lista de portadoras que están establecidas y las capacidades del terminal.

Para reducir la sobrecarga en la E-UTRAN y el procesamiento en el UE, toda la información relacionada con el UE en la red de acceso puede liberarse durante largos períodos de inactividad de datos. El UE se encuentra entonces en el estado ECM-INACTIVO. La MME conserva el contexto de UE y la información sobre las portadoras establecidas durante estos períodos de inactividad. Para permitir que la red contacte con un UE de ECM-INACTIVO, el UE actualiza la red en cuanto a su nueva ubicación cada vez que se mueve fuera de su área de seguimiento (TA) actual; este procedimiento se denomina "actualización de área de seguimiento". La MME es responsable de realizar el seguimiento de la ubicación del usuario mientras el UE está en ECM-INACTIVO. En ese sentido, se podría decir que la ubicación del UE en un nivel de TA es parte del contexto de UE en la MME.

Cuando existe la necesidad de entregar datos de enlace descendente a un UE de ECM-INACTIVO, la MME envía un mensaje de radiolocalización a todos los eNB en su TA actual, y los eNB localizan al UE a través de la interfaz de radio. Al recibir un mensaje de radiolocalización, el UE realiza un procedimiento de solicitud de servicio que da como resultado que el UE pase al estado ECM-CONECTADO. De este modo, se crea información relacionada con el UE en la E-UTRAN y se restablecen las portadoras.

La MME es responsable del restablecimiento de las portadoras de radio y de la actualización del contexto de UE en el eNodoB. Esta transición entre los estados del UE se denomina "transición de inactivo a activo".

La MME es responsable de establecer la seguridad para la señalización de control entre el UE y la red central. Cuando un UE se conecta a la red, se realiza una autenticación mutua del UE y la red entre el UE y la MME/HSS. Esta función de autenticación también establece la clave de seguridad K_{ASME}, que es la base para todas las claves posteriores derivadas para su uso en la RAN.

El diseño de seguridad de LTE proporciona compartimentación. La compartimentación consiste principalmente en garantizar que si un atacante viola la seguridad de una función, solo esa función se ve comprometida. Por ejemplo, como se explica en el análisis de amenazas, hay una clave utilizada para el cifrado del protocolo RRC y otra clave utilizada para la protección de la integridad del protocolo RRC.

La seguridad de estrato de acceso (AS) está compuesta por la protección de la integridad del plano de control (es decir, la señalización RRC) y el cifrado tanto del plano de control como de usuario. El algoritmo de protección de la integridad se aplica a las portadoras de radio de señalización (SRB) (por ejemplo, dos portadoras de radio de señalización SRB1 y SRB2). El algoritmo de cifrado se aplica a las portadoras de radio (por ejemplo, dos portadoras de radio de señalización SRB1 y SRB2, así como a las portadoras de radio de datos DRB). Por otro lado, no se aplica ni la protección de la integridad ni el cifrado a otra portadora de radio de señalización (por ejemplo, portadora de radio de señalización SRB0).

Si un atacante viola la clave de cifrado de control de recursos de radio (RRC), el atacante puede descifrar y leer todos los mensajes RRC. Sin embargo, dado que la clave de integridad es diferente de la clave de cifrado, el atacante no puede modificar o inyectar mensajes RRC. Un atacante que haya violado la clave de cifrado RRC tampoco puede utilizarla para interceptar los DRB, dado que utilizan claves de cifrado separadas (y viceversa).

Otra parte del diseño de compartimentación es que cada eNB utiliza un conjunto de claves separado. La razón es que esto garantiza que un atacante que irrumpa en un eNB no obtenga ninguna información sobre los datos transmitidos entre un UE y otro eNB físicamente diferente. Para mantener la propiedad de que irrumpir en un nodo de RAN físico, es decir, un eNB, no ayuda a atacar a otro nodo de RAN, el eNB auxiliar debe utilizar su propio conjunto de claves separado del conjunto de claves utilizado en el eNB de anclaje, sin embargo, puede derivarse a partir del eNB de anclaje como en la conectividad dual de LTE.

Para explicarlo con más detalle, las claves de seguridad en LTE pueden ordenarse en una jerarquía donde las claves en niveles inferiores en la jerarquía se derivan de claves en el mismo nivel o en niveles superiores. La clave de nivel superior es K, y tiene un valor permanente almacenado en el módulo de identidad de abonado universal (USIM) y HSS (centro de autenticación, AuC). A partir de esta K, se derivan la clave de cifrado (CK) y la clave de integridad (IK) durante el procedimiento de autenticación que se ejecuta entre el UE y el HSS/MME. A partir de la CK/IK, el UE y el HSS derivan una clave denominada K_{ASME}. El HSS reenvía K_{ASME} a MME. Las claves de NAS (entre MME y UE) (K_{NASint}, K_{NASenc}) y K_{eNB} se derivan a partir de K_{ASME} en MME. Las claves de seguridad de AS (entre eNB y UE) (K_{RRCint}, K_{RRCenc}, K_{UPenc}) se derivan a partir de K_{eNB}, que es reenviada por la MME a eNB, en eNB.

A continuación se describen con respecto a la Figura 1 detalles adicionales de los principios de diseño de seguridad. Es decir, a continuación, se describen y se muestran en la Figura 1 los diferentes pasos para la configuración de seguridad en EPC.

En el paso 1, el UE se conecta a la MME para los servicios de LTE. Para este propósito, la MME recibe una solicitud de conexión (capacidad de red del UE que indica los algoritmos de seguridad de LTE soportados, IMSI) desde el UE para obtener el acceso inicial a la red.

En el paso 2, la MME autentica el UE y deriva K_{ASME}. Para este propósito, al MME solicita el vector de autenticación (AV) relacionado con la identidad de abonado móvil internacional (IMSI) enviando la solicitud de datos de autenticación a AuC/HSS. Después de la derivación de un valor aleatorio (RAND), la respuesta esperada (XRES), K_{ASME} (derivada

a partir de CK, IK y PLMN ID) y el token de autenticación (AUTN), el AuC los combina como un vector de autenticación (AV = RAND || XRES || KASME || AUTN) y lo envía a la MME adjunto dentro de la respuesta de datos de autenticación.

Luego, MME recupera K_{ASME}, el valor aleatorio (RAND), la respuesta esperada (XRES), y el AUTN del AV. La MME envía AUTN y RAND con la solicitud de autenticación al UE. El UE autentica la red comprobando el AUTN recibido. Luego deriva IK, CK (y K_{ASME} a partir de CK/IK), RES, AUTN y RAND. Envía la respuesta (RES) junto con la respuesta de autenticación. Después de recibir la RES, la MME la compara con XRES y si coincide, entonces la autenticación se considera exitosa (de lo contrario, la MME envía un fallo de autenticación al UE). A continuación, la MME deriva K_{NASint}, K_{NASenc}. La entrada a las derivaciones de clave son los algoritmos de cifrado e integridad de NAS particulares que son seleccionados por la MME en base a la información de capacidad de red del UE incluida en el mensaje de solicitud de conexión recibido. Finalmente, la MME establece en cero el contador NAS de enlace descendente utilizado para los mensajes NAS protegidos con las claves derivadas a partir de este K_{ASME} particular y envía el comando de modo de seguridad de NAS (que incluye el identificador de K_{ASME} (KSI_{ASME}), el algoritmo de integridad, el algoritmo de cifrado, la capacidad de seguridad de UE, MAC de NAS) en un mensaje no cifrado. Aquí, se genera el MAC de NAS (código de autenticación de mensajes para NAS) para la protección de la integridad de todo el mensaje utilizando K_{NASint} y el algoritmo de integridad seleccionado. Después de recibir el comando de modo de seguridad de NAS, el UE establece el identificador de K_{ASME} (KSI_{ASME}) en el mensaje como su KSI_{ASME} y lo utiliza como un identificador de la K_{ASME} actual; calcula K_{ASME}, K_{eNB}, K_{NASint} K_{NASenc}; y verifica la integridad del mensaje de comando de modo de seguridad con MAC de XNAS. A continuación, el UE envía a la MME el modo de seguridad de NAS completo dentro de un mensaje de integridad protegida, de manera similar a un MAC de NAS.

La MME deriva K_{eNB} a partir de K_{ASME} y envía K_{eNB} al eNB. El UE deriva K_{eNB} a partir de K_{ASME} para calcular otras claves de seguridad y activar la seguridad.

En el paso 3, después de recibir el modo de seguridad de NAS completo del UE, la MME calcula la K_{eNB} y lo envía al eNB con la solicitud de configuración del contexto inicial de S1AP adjuntando la capacidad de seguridad de UE y K_{eNB}. Después de recibir K_{eNB}, eNB calcula K_{RRCint}, K_{RRCenc}, K_{UPenc} a partir de ello. Luego envía el comando de modo de seguridad de AS que incluye algoritmos de cifrado e integridad de AS, así como MAC-I (código de autenticación de mensaje para la integridad) que se genera utilizando K_{RRCint}. Aquí, el mensaje está protegido en cuanto a integridad, pero no cifrado. Después de recibir el comando de modo de seguridad de AS, el UE identifica los algoritmos de seguridad; calcula K_{RRCint}, K_{RRCenc}, K_{UPenc}; y verifica la integridad del mensaje de comando de modo de seguridad con XMAC-I. Finalmente, el UE enviará el modo de seguridad de AS completo al eNB con protección de la integridad con MAC-I.

Cabe señalar que después de los pasos dados anteriormente, la mayoría de los mensajes NAS y AS estarán protegidos en cuanto a integridad y cifrados, excepto los datos de usuario, que solo estarán cifrados.

Ahora se describirá la configuración RRC para las claves de seguridad de AS. RRC configura todas las entidades PDCP con las que está asociado. En particular, RRC configura las entidades PDCP con claves criptográficas y datos de configuración, tales como qué algoritmos de seguridad aplicar. El conjunto de claves en un eNB consta de la K_{eNB} y K_{UPenc}, K_{RRCenc} y K_{RRCint} como se discutió anteriormente. RRC configura cada entidad PDCP para el tráfico del plano de usuario (DRB) con una clave de cifrado K_{UPenc} y cada entidad PDCP para el tráfico del plano de control (SRB) con una clave de cifrado K_{RRCenc} y una clave de protección de la integridad K_{RRCint}. Para los DRB utilizados para proteger los datos entre un eNB donante y un nodo de retransmisión, RRC también configura el DRB con una clave de protección de la integridad K_{UPint}.

La activación de la seguridad de AS puede describirse de la siguiente manera. El procedimiento de comando de modo de seguridad de AS inicia la seguridad para las portadoras de radio (RB) entre el eNB y el UE. Después de este procedimiento, la seguridad está activa hasta que el UE o el eNB terminen la conexión RRC. Esto implica que cuando el eNB establece un nuevo DRB a través de un procedimiento de reconfiguración RRC, la seguridad ya está activa y el eNB y el UE cifrarán los paquetes PDCP en las DRB desde el inicio.

Como se describió anteriormente con respecto a la Figura 1, los procedimientos de señalización actuales no se han diseñado o al menos optimizado para soportar una arquitectura RAN que esté compuesta por múltiples interfaces aéreas donde estas interfaces aéreas pueden tener algunos aspectos diferentes en su contexto de UE.

Un ejemplo puede comprender un contexto de seguridad que sea diferente para diferentes RAT (a pesar de la integración estrecha) o versiones estándar o capacidades de UE o categorías de dispositivos. Por ejemplo, puede haber diferentes requisitos de longitud para las claves de seguridad de diferentes RAT o la terminación de la red puede estar en nodos separados, lo que requiere conjuntos de claves separados.

El establecimiento de portadora de señalización y/o el establecimiento de portadora de datos y/o la recuperación de portadora de señalización y/o portadora de datos requiere una serie de pasos de señalización como se explicó anteriormente con respecto a la Figura 1, lo que da como resultado, por ejemplo, una sobrecarga de señalización y/o una larga duración de la señalización, especialmente cuando se supone la integración estrecha de múltiples interfaces aéreas. Esto es así incluso en el caso donde las conexiones de la primera RAT y la segunda RAT del UE serían hacia al mismo, o en otras palabras, un nodo de radio compartido y/o nodo de red central.

La Figura 2 muestra una realización de un sistema de comunicación inalámbrica 20 que comprende una realización

de un dispositivo de comunicación inalámbrica 100, una realización de un elemento de red de acceso por radio (RAN) 200 y una realización de un elemento de red central (CN) 300.

El dispositivo de comunicación inalámbrica 100 está adaptado para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El dispositivo de comunicación inalámbrica 100 puede ser, comprender o ser parte de un equipo de usuario (UE) operable de acuerdo con LTE o LTE-A.

El dispositivo de comunicación inalámbrica 100 comprende un componente de recepción 120 y un componente de configuración 140. El dispositivo de comunicación inalámbrica 100 puede comprender además un componente de transmisión 160. El componente de recepción 120 está configurado para recibir, desde un elemento de RAN, por ejemplo, el elemento de RAN 200, en un procedimiento de señalización común, información que permite al dispositivo de comunicación inalámbrica 100 configurar un contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT. El componente de configuración 140 está configurado para configurar el contexto de seguridad de AS para la primera RAT y la segunda RAT. El componente de recepción 120 puede configurarse para recibir información adicional desde un elemento de RAN, por ejemplo, el elemento de RAN 200, y/o un elemento de CN, por ejemplo, el elemento de CN 300. El componente de transmisión 160 puede configurarse para transmitir información a un elemento de RAN, por ejemplo, el elemento de RAN 200 y/o un elemento de CN, por ejemplo, el elemento de CN 300.

El elemento de RAN 200 está adaptado para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El elemento de RAN 200 puede ser, comprender o ser parte de un eNodoB en el caso de LTE o LTE-A.

El elemento de RAN 200 comprende un componente de iniciación 220. El elemento de RAN 200 puede comprender además un componente de recepción 240 y/o un componente de derivación 260. El componente de iniciación 220 está configurado para iniciar la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común. El componente de recepción 240 puede configurarse para recibir información desde un dispositivo de comunicación inalámbrica, por ejemplo, desde el dispositivo de comunicación inalámbrica 100, o de un elemento de CN, por ejemplo, el elemento de CN 300. El componente de derivación 260 puede configurarse para derivar cierta información a partir de la información recibida, por ejemplo.

El elemento de CN 300 está adaptado para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El elemento de CN 300 puede ser, comprender o ser parte de una entidad de gestión de la movilidad (MME) en el caso de LTE o LTE-A.

El elemento de CN 300 comprende un componente de información 320. El elemento de CN 300 puede comprender además un componente de recepción 340 y un componente de derivación 360. El componente de información 320 está configurado para informar a un elemento de RAN, por ejemplo, el elemento de RAN 200, de la red de comunicación inalámbrica que inicie la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común. El componente de recepción 240 puede configurarse para recibir información desde un dispositivo de comunicación inalámbrica, por ejemplo, del dispositivo de comunicación inalámbrica 100, o de un elemento de RAN, por ejemplo, el elemento de RAN 200. El componente de derivación 360 puede configurarse para derivar cierta información a partir de la información recibida, por ejemplo.

El dispositivo de comunicación inalámbrica 100, el elemento de RAN 200 y el elemento de CN 300 se describirán con más detalle a continuación con respecto a la Figura 3.

La Figura 3 muestra una realización de un método que puede implementarse en el sistema de comunicación inalámbrica 20 de la Figura 2. En más detalle, el primer paso S302 de la Figura 3 muestra una realización de un método que puede implementarse en el elemento de CN 300 de la Figura 2, el segundo paso S304 de la Figura 3 muestra una realización de un método que puede implementarse en el elemento de RAN 200 de la Figura 2 y el tercer paso S306 y el cuarto paso S308 de la Figura 3 muestran una realización de un método que puede implementarse en el dispositivo de comunicación inalámbrica 100 de la Figura 2.

El método de la Figura 3 soporta la configuración del contexto de seguridad en una red de comunicación inalámbrica, comprendiendo el método informar.

En el paso S302, el elemento de CN, por ejemplo, el elemento de CN 300, de la red de comunicación inalámbrica informa a un elemento de RAN, por ejemplo, el elemento de RAN 200, de la red de comunicación inalámbrica, que inicie la configuración del contexto de seguridad de AS para una primera RAT y una segunda RAT en un procedimiento de señalización común. Por ejemplo, el componente de información 320 del elemento de CN 300 informa en el paso S302 a un elemento de RAN, por ejemplo, el elemento de RAN 200, de la red de comunicación inalámbrica, que inicie la configuración del contexto de seguridad de AS para una primera RAT y una segunda RAT en un procedimiento de señalización común.

En el paso S304, el elemento de RAN, por ejemplo, el elemento de RAN 200, de la red de comunicación inalámbrica

inicia la configuración del contexto de seguridad de AS para una primera RAT y una segunda RAT en un procedimiento de señalización común. Por ejemplo, el componente de iniciación 220 del elemento de RAN 200 inicia, en el paso S304, la configuración del contexto de seguridad de AS para una primera RAT y una segunda RAT en un procedimiento de señalización común.

En el paso S306, un dispositivo de comunicación inalámbrica, por ejemplo, el dispositivo de comunicación inalámbrica 100, de la red de comunicación inalámbrica recibe, desde un elemento de RAN, por ejemplo, el elemento de RAN 200, de la red de comunicación inalámbrica en un procedimiento de señalización común, información que permite a la comunicación inalámbrica, por ejemplo, el dispositivo de comunicación inalámbrica 100, configurar un contexto de seguridad de AS para una primera RAT y una segunda RAT. Por ejemplo, el componente de recepción 120 del dispositivo de comunicación inalámbrica 100 recibe, desde un elemento de RAN, por ejemplo, el elemento de RAN 200, de la red de comunicación inalámbrica en un procedimiento de señalización común, información que permite a la comunicación inalámbrica, por ejemplo, el UE 100, configurar un contexto de seguridad de AS para una primera RAT y una segunda RAT en el paso S306. En el paso S308, el dispositivo de comunicación inalámbrica, por ejemplo, el dispositivo de comunicación inalámbrica 100, configura el contexto de seguridad de AS para la primera RAT y la segunda RAT. Por ejemplo, el componente de configuración 140 del dispositivo de comunicación inalámbrica 100 configura el contexto de seguridad de AS para la primera RAT y la segunda RAT en el paso S308.

La presente divulgación se describe a continuación principalmente dentro el contexto de LTE. Debe entenderse que los problemas y soluciones descritos en la presente memoria son igualmente aplicables a redes de acceso inalámbrico y equipos de usuario (UE) que implementan otras tecnologías y estándares de acceso. Por lo tanto, LTE se utiliza como una tecnología de ejemplo donde la técnica propuesta es adecuada y, por lo tanto, el uso de LTE en lo sucesivo es útil para entender la técnica descrita en la presente memoria. Por lo tanto, en lo sucesivo, a modo de explicación y no de limitación, el elemento de red de acceso por radio 200 se denominará eNB 200 para ilustrar, a modo de ejemplo, que el elemento de red de acceso por radio 200 puede configurarse como una estación base y que la técnica propuesta en la presente memoria puede utilizarse e implementarse en LTE. De manera similar, el dispositivo de comunicación inalámbrica 100 se denominará UE 100 para ilustrar, a modo de ejemplo, que la técnica propuesta en la presente memoria puede utilizarse e implementarse en LTE. De manera similar, el elemento de CN 300 se denominará MME 300 para ilustrar, a modo de ejemplo, que el elemento de CN 300 puede configurarse como una entidad de gestión de la movilidad y que la técnica propuesta en la presente memoria puede utilizarse e implementarse en LTE.

De manera similar, la información de contexto se denominará contexto de UE de eNB. El contexto de UE de eNB puede entenderse en el sentido de 3GPP TS 36.401 como un bloque de información en un eNB asociado a un UE activo. El bloque de información puede contener la información necesaria requerida para mantener los servicios de E-UTRAN hacia el UE activo. Por ejemplo, una o más de la información de estado del UE, información de seguridad, información de capacidad del UE y las identidades de la conexión S1 lógica asociada al UE pueden incluirse en el contexto de UE de eNB. El establecimiento del contexto de UE de eNB puede considerarse completado cuando se completa la transición al estado activo para un UE o en el eNB objetivo después de la finalización del traspaso a E-UTRAN.

A continuación se describen detalles ejemplares adicionales relativos al UE 100, el eNB 200, la MME 300 y el sistema 20 que comprende el UE 100, el eNB 200 y la MME 300, y los métodos realizados en los mismos con respecto a las Figuras 6 a 10. Antes de explicar estos detalles, se explica brevemente información general sobre el concepto de arquitectura RAN de 5G con referencia a las Figuras 4 y 5.

Con el fin de cumplir con los requisitos de 5G en términos de tasas de datos y latencia, se necesita una nueva interfaz aérea diseñada para operar en frecuencias superiores (por ejemplo, por encima de 6 GHz). En comparación con las bandas de frecuencia actuales asignadas a LTE, existen condiciones de propagación mucho más desafiantes, de modo que la cobertura de la nueva interfaz aérea puede ser más irregular. El uso extensivo de la formación de haces, en particular en el lado de la red, es una parte esencial del acceso inalámbrico de alta frecuencia para superar los desafíos de propagación destacados anteriormente. A pesar de las posibles ganancias en el presupuesto del enlace, la fiabilidad de un sistema que dependa exclusivamente de la formación de haces y que opere en frecuencias superiores puede ser un desafío (la cobertura puede ser más sensible a las variaciones de tiempo y/o espacio).

Con el fin de soportar aplicaciones que requieren latencias muy bajas (del orden de 1 ms), tal como algunos casos de uso de comunicación de tipo máquina ultra confiable, es probable que se defina para la nueva interfaz aérea de 5G una nueva estructura de dominio del tiempo en base a intervalos de tiempo de transmisión (TTI) más cortos y un ancho de banda más amplio para bloques de recursos de radio en comparación con el especificado para LTE.

En paralelo con las actividades de investigación de 5G, el 3GPP está añadiendo continuamente nuevas características a LTE y es probable que, en el momento en que 5G llegue al mercado, LTE sea capaz de abordar muchos de los requisitos de 5G. Además de esto, también se espera que LTE se despliegue de manera masiva y, el hecho de que opere en bandas de frecuencia con mejores propiedades de propagación hace que la integración estrecha de LTE y la nueva interfaz aérea que opera en bandas de frecuencia superiores resulte muy atractiva.

Con respecto a la arquitectura RAN de 5G, actualmente hay un debate en curso entre las diferentes partes involucradas sobre alternativas de arquitectura para lograr una integración tan estrecha. En algunas de las discusiones, tal como en el proyecto METIS-II de UE, se supone que habrá funcionalidades comunes en la pila de

protocolos RAN en contraste con el interfuncionamiento actual entre los diferentes accesos de red. En el sistema actual, a diferencia de esa suposición, el interfuncionamiento depende de interfaces entre nodos, tanto para el plano de usuario (UP) como para el plano de control (CP). Por ejemplo, en el caso del interfuncionamiento de E-UTRAN y UTRAN, la MME y la S-GW están interconectadas a través de la interfaz S11. Dicha arquitectura básicamente permite la continuidad de la cobertura y el balanceo de carga solo a través de traspasos duros (que siempre involucran señalización de la red central) y una gestión de recursos semiindependiente para las múltiples interfaces aéreas. Los detalles sobre el interfuncionamiento entre E-UTRAN y UTRAN pueden encontrarse en TS 36.300 V13.1.0 (2015-09), por ejemplo, u otras versiones del mismo.

Con el fin de lograr la integración estrecha de LTE y la nueva interfaz aérea de 5G, se propone en (véase "Tigh integration of new 5G air interface and LTE to fulfill 5G requirements", VTC Primavera de 2015 - primer taller internacional sobre Arquitectura de 5G, Glasgow, Escocia) una arquitectura lógica que depende de capas de protocolo RRC/PDCP comunes, como se muestra en la Figura 5. "AI" denota interfaz aérea, que en lo sucesivo a veces se denomina NX, NX de 5G o, de manera abreviada, 5G.

En la Figura 4 se muestra una posible realización para interfaces entre nodos comunes.

En la Figura 6 se explican ahora detalles adicionales de las realizaciones de las Figuras 2 y 3. Con más detalle, como se ilustra en la Figura 6, lo siguiente puede ser realizado por el UE 100 y/o el eNB 200 y/o la MME 300. A modo de ilustración y no de limitación, una primera RAT (RAT1) y una segunda RAT (RAT2) son soportadas por el mismo eNB, es decir, el eNB 200, en la Figura 6. Sin embargo, esto no debe entenderse como limitativo. En su lugar, la RAT1 y la RAT2 pueden ser soportadas por diferentes eNB, por ejemplo, la RAT1 por el eNB 200 y la RAT2 por un eNB diferente. Por lo tanto, la presente divulgación es igualmente aplicable independientemente de si una BS implementa ambas RAT o si las dos RATS se implementan por separado en diferentes BS. Se supone que solo hay una conexión RAN-CN por UE para ambas RAT. La primera RAT y la segunda RAT pueden combinarse en una BS o pueden distribuirse en dos BS separadas. En el caso de BS separadas para la primera y la segunda RAT, la BS de la primera RAT es informada por la BS de la segunda RAT sobre las capacidades de seguridad de la BS para la segunda RAT antes del método a continuación. Además, como se mencionó anteriormente, en el caso de BS separadas para la primera y la segunda RAT, la BS de la segunda RAT no necesita una conexión a la CN.

A continuación, se explica cómo manejar el contexto de UE para la seguridad a través de un procedimiento común (suponiendo un escenario con una integración estrecha de múltiples interfaces aéreas tales como LTE y otra RAT) para permitir el establecimiento de una conexión rápida, eficiente y segura para multi-RAT (por ejemplo, 4G y 5G) independientemente de qué tecnología de acceso se utilice inicialmente (por ejemplo, para el procedimiento de conexión). Aquí, 5G puede referirse a la evolución de LTE u otra RAT que pueda suponerse como 5G.

El contexto de seguridad puede incluir capacidades de seguridad, claves, algoritmos y parámetros disponibles. Para algunos procedimientos, un subconjunto del contexto de seguridad multi-RAT (por ejemplo, claves de seguridad, parámetros o algoritmos) puede ser idéntico (para diferentes RAT), lo que minimiza la sobrecarga del contexto y la cantidad de procesamiento. Sin embargo, este puede no ser siempre el caso, incluso si los procedimientos relacionados son los mismos o similares para diferentes RAT. Por ejemplo, si las RAT no están coubicadas en un nodo físico seguro, puede ser necesaria la transformación del contexto con el fin de no violar el principio de compartimentación mencionado en la sección de antecedentes, incluso si puede reutilizarse el mismo tipo de material de clave y los procedimientos relacionados.

De acuerdo con esto, el UE 100 podría conectarse para "solo LTE" o "solo 5G" o para "LTE y 5G combinados". En el caso de una conexión combinada de 5G y LTE (por ejemplo, a través de RAT de 5G), el método comprendido en la presente memoria incluye uno o más de los pasos que se explican a continuación con respecto a la Figura 6.

Con respecto a la Figura 6, en un primer paso paso1, el UE 100 se conecta a la CN para servicios tanto 5G como LTE. Para este propósito, el UE 100 envía a la CN 300 (que hace referencia a una función lógica de CN y/o un elemento de red de CN que maneja solicitudes de conexión, por ejemplo, la MME 300) su información de contexto sobre las capacidades de seguridad tanto para RAT1 como para RAT2 (por ejemplo, algoritmos de seguridad soportados a través de la información de capacidad de red de UE disponible en la solicitud de conexión) cuando se conecta a través de RAT1 (por ejemplo, en el mensaje de conexión) (paso S602). Por consiguiente, el UE 100 se indica como un UE de LTE+5G dentro de la solicitud de conexión. En otras palabras, el UE 100 informa a la CN 300 (en lo sucesivo, a veces se la denominará MME 300 generalmente como elemento de la CN o, de manera abreviada, simplemente CN 300) sobre sus capacidades de seguridad con respecto a la primera RAT y la segunda RAT cuando envía un mensaje L3 inicial a la CN 300 (por ejemplo, SOLICITUD DE UNIÓN para el propósito de conexión de CN; solicitud de actualización de área de seguimiento (TAU) para informar a la CN sobre un evento de movilidad en modo INACTIVO a través de la primera RAT).

Como se indicó anteriormente, el UE 100 puede incluir un indicador para LTE así como para para servicios de 5G. Por lo tanto, la CN 300 puede activar el elemento de RAN 200 para la activación combinada como se describe en la presente memoria. Para completar la descripción de la configuración de seguridad, el UE 100 puede incluir sus capacidades de seguridad de LTE. Estos son los algoritmos de cifrado e integridad soportados para diferentes tipos de acceso. La indicación del tipo de conexión podría estar implícita a partir de qué capacidades incluye el UE en el

mensaje de conexión. En general, puede ser beneficioso mantener las capacidades de seguridad del UE para todas las RAT que el UE soporta en la CN para futuros traspasos entre RAT.

Después de informar a la CN 300 sobre las capacidades de seguridad del UE 100, se realiza la configuración de seguridad para NAS (CN de UE para señalización) en el paso 2 paso2. Para este propósito, la CN 300 solicita la autenticación del UE 100 en un mensaje de solicitud de autenticación NAS (paso S606) y deriva el material de clave de CN (común para ambas RAT o separado para cada RAT). El UE verifica la autenticidad de la solicitud de autenticación y responde con un mensaje de respuesta de autenticación (paso S608) y deriva el material de clave de CN correspondiente. En otras palabras, la CN 300 autentica al UE 100 tanto para los servicios de 5G como de LTE y deriva una clave de nivel de CN (por ejemplo, K_{ASME}). En más detalle, la CN 300, por ejemplo, la MME 300, solicita el vector de autenticación (AV) relacionado con la identidad de abonado móvil internacional (IMSI) enviando la solicitud de datos de autenticación a AuC /HSS 400 (paso S604). Aquí, el AV podría ser un vector dual relacionado tanto con 5G como con LTE. Además, AuC 400 reconoce que UE 100 es un UE 100 de RAT dual. La CN recupera claves de seguridad y parámetros del AV dual relacionado tanto con 5G como con LTE. La CN 300 envía la solicitud de autenticación, que es válida tanto para 5G como para LTE, al UE 100 en el paso S606. El UE 100 autentica la CN 300 comprobando los parámetros de seguridad recibidos, derivando las claves de seguridad y otros parámetros. La derivación se realiza tanto para NX como para LTE. De esta manera, el UE 100 ejecutará un(os) algoritmo(s) de autenticación común(es) o separado(s) al mismo tiempo y preparará un único mensaje (por ejemplo, respuesta de autenticación) en el paso S608.

Cuando el UE 100 envía el mensaje de respuesta de autenticación y cuando la CN 300 recibe el mensaje de respuesta de autenticación, el UE 100 y la CN 300 consideran la autenticación completada para ambas RAT. La CN 300 deriva material de clave de CN adicional para la protección de la integridad y el cifrado de la comunicación de NAS y envía información que permite al UE 100 derivar el material de clave de CN adicional al UE 100 en un mensaje de comando de modo de seguridad de NAS (paso S610). Esta información puede corresponder a información a partir de la que puede derivarse el material de clave de CN, un material de clave de RAN o ambos. El mensaje puede comprender una indicación de que el material de clave de CN y/o RAN es para la primera RAT, la segunda RAT o para ambas. El UE 100 deriva el material de clave de CN y RAN adicional y responde a la CN 300 en un mensaje de comando de modo de seguridad de NAS completo (paso S612) para confirmar a la CN 300 que el procedimiento se ha completado exitosamente en el UE 100. En este sentido, la derivación de un material de clave no necesariamente debe realizarse inmediatamente, sino que normalmente se deriva cuando debe utilizarse por primera vez (el remitente no necesita calcular una clave de cifrado hasta que se cifra el primer mensaje).

Para explicarlo con más detalle, la CN 300 verifica la autenticación tanto para 5G como para LTE y deriva claves y parámetros adicionales en base a los algoritmos de seguridad seleccionados, que podrían ser comunes o separados para ambas RAT. A continuación, la CN 300 envía el comando de seguridad de NAS en el paso S610, con los parámetros de seguridad, las capacidades y la protección de la integridad pertinentes, tanto para LTE como para 5G. Después de recibir el comando de modo de seguridad de NAS, que es válido para ambas RAT, el UE 100 puede derivar claves y parámetros de seguridad adicionales; y verificar la integridad del mensaje de comando de modo de seguridad. A continuación, el UE 100 envía a la CN 300 el modo de seguridad de NAS completo con los parámetros de seguridad, las capacidades y la protección de la integridad pertinentes, tanto para LTE como para 5G en el paso S612.

Después de que se haya derivado el material de clave de CN, se realiza la configuración de seguridad para AS (RAN de UE para señalización y plano de usuario) en el paso 3 paso3. Para este propósito, la CN 300 deriva a partir del material de clave de CN el material de clave de RAN (común para ambas RAT o separado para cada RAT) y envía, en el paso S614, el material de clave de RAN al elemento de RAN 200 (también denominado a veces eNB 200 en lo sucesivo), por ejemplo, en un mensaje de configuración del contexto inicial de UE de S1AP (en el nivel de NAS). Si eNB 200 no ha recibido el material de clave de RAN para la segunda RAT, eNB 200 deriva este material de clave de RAN a partir del material de clave de RAN para la primera RAT. Luego, eNB 200 envía al UE 100 información que permite al UE 100 derivar el material de clave de RAN y activar la seguridad de AS para ambas RAT, por ejemplo, en un mensaje de comando de modo de seguridad de AS (paso S616). El UE 100 deriva este material de clave de RAN e informa al eNB 200 de la primera RAT o al eNB 200 de la segunda RAT (por ejemplo, incluido en un mensaje RRC) en un mensaje de modo de seguridad de AS completo del mismo. En caso de que el mensaje se envíe a una estación base de la segunda RAT, la estación base de la segunda RAT envía una indicación de X2AP a la estación base de la primera RAT. Esta indicación indica a la estación base de la primera RAT que la seguridad está establecida para ambas RAT.

Para explicarlo con más detalle, la CN 300 deriva un material de clave de nivel de RAN común (por ejemplo, K_{eNB}) o separado para las seguridades tanto de 5G como de LTE a partir de un material de clave de nivel de CN común (por ejemplo, K_{ASME}) o separado, y envía el material de clave de nivel de RAN derivado al elemento de RAN 200 (paso S614). El UE 100 también deriva el mismo material de clave de nivel de RAN (por ejemplo, K_{eNB} de K_{ASME}) para calcular otras claves de seguridad y activar la seguridad de extremo a extremo tanto para los servicios de 5G como de LTE. Después de recibir el modo de seguridad de NAS completo desde el UE 100 en el paso S612, la CN envía material de clave de nivel de RAN (por ejemplo, un K_{eNB} común) tanto para LTE como para 5G al elemento de RAN 200 en el paso S614 con la solicitud de configuración del contexto inicial de S1AP adjuntando la capacidad de seguridad de UE y las claves de LTE y 5G o un material de clave de nivel de RAN común tanto para LTE como para 5G. De esta manera, la CN 300 proporciona un contexto de seguridad dual al elemento de RAN 200. Después de recibir el material

de clave de nivel de RAN, el elemento de RAN realiza la comprobación de integridad y calcula las claves y parámetros de AS requeridos tanto para LTE como para 5G a partir de ello. Luego, envía un comando de modo de seguridad de AS común en el paso S616 con los parámetros de seguridad necesarios tanto para LTE como para 5G con protección de la integridad. De esta manera, se habilita una activación combinada. Después de recibir el comando de modo de seguridad de AS, el UE 100 identifica los algoritmos de seguridad y calcula las claves de seguridad de AS tanto para LTE como para 5G; y verifica la integridad del mensaje de comando de modo de seguridad. Finalmente, el UE 100 envía un comando de modo de seguridad de AS completo común al elemento de RAN con protección de la integridad en el paso S618.

El elemento de RAN 200 deriva una clave NX a partir de K_{eNB} y utiliza la clave de 5G como base para cualquier clave de cifrado e integridad que deba utilizarse en 5G. Puede ser posible que se produzcan algunas variaciones en los pasos dados anteriormente. Por ejemplo, en lugar del caso donde la MME 300 deriva las claves de 5G y LTE o una K_{eNB} común (por ejemplo, a partir de la K_{ASME} común) directamente y las proporciona al elemento de RAN 200, el elemento de RAN 200 también puede derivar una clave de 5G a partir de K_{eNB} y puede utilizar la clave de 5G como base para cualquier clave de cifrado e integridad que deba utilizarse en 5G. Esto puede ser obligatorio especialmente cuando las RAT de 5G y LTE no están coubicadas (debido al principio de compartimentación).

Cabe señalar que una opción es enviar información a partir de la cual puede derivarse la clave RAN del elemento de CN 300 al UE 100. Otra opción es enviar dicha información desde el elemento de RAN 200 al UE 100. También es posible que se envíen ambas piezas de información y que la clave RAN se derive a partir de ambas.

Como se indicó anteriormente, la CN puede necesitar indicar explícitamente a la RAN qué hacer si algunos pasos se consideran transparentes para la RAN, por ejemplo, especialmente cuando se utilizan algoritmos y material de clave común para configurar múltiples seguridades de RAT. De manera similar, el UE 100 puede que necesite que se le reconozca explícitamente sobre qué seguridades de RAT han de activarse, por ejemplo, a través del comando de modo de seguridad. La decisión de crear y activar el contexto de seguridad de AS puede tomarse en el nivel de RAN o de CN. A pesar de la indicación de capacidades de seguridad de RAT duales del UE 100, el elemento de RAN 200 o la CN 300 pueden rechazar la configuración de seguridad para una RAT específica. En este caso, la MME 300 o el eNB 200 pueden reconocer implícitamente el rechazo de una configuración de seguridad (por ejemplo, seguridad de RAT2) respondiendo solo para una RAT (por ejemplo, seguridad de RAT1) como se muestra en la Figura 6. Alternativamente, cualquier mensaje de rechazo o fallo puede señalizarse dentro de un procedimiento de señalización dedicado.

En una variación de la Figura 6, aunque MME 300 puede autenticar con éxito el UE 100 para ambas RAT y crear el contexto requerido, la activación de seguridad para una determinada RAT y seguridad (por ejemplo, seguridad de AS para la RAT2) puede posponerse. Esto podría ser, por ejemplo, debido a la movilidad, carga de tráfico, política de seguridad o cualquier otro motivo.

Como se explica en la presente memoria, el contexto multi-RAT para la seguridad se maneja a través de un procedimiento común para permitir el establecimiento de una conexión rápida, eficiente y segura para multi-RAT. De acuerdo con esto, el UE puede solicitar una configuración de seguridad multi-RAT y la red (NW) puede ejecutar un único procedimiento (por ejemplo, comando de modo de seguridad) para activar la seguridad tanto para LTE como para 5G. Para poder hacer eso, la NW puede necesitar obtener la información requerida de otro elemento de red relacionado tanto con LTE como con 5G para este UE.

En la presente memoria, se describe un mecanismo para la señalización simultánea relacionada con la configuración de la seguridad entre un UE y una red para dos o más RAT, por ejemplo, LTE, 5G. La activación de la seguridad puede o no realizarse simultáneamente para ambas RAN. La seguridad se activa para dos estratos. El primero es entre el UE y un nodo de CN, y el segundo es entre el UE y un nodo de RAN. El mecanismo comprende la autenticación mutua entre el UE y la CN por medio de un primer procedimiento de NAS único. Además, un segundo nodo de CN informa al UE de si debe activarse la seguridad para dos o más RAT simultáneamente en un único procedimiento para el primer estrato de NAS. El primer y el segundo nodo de CN pueden ser el mismo. La información también puede indicar si se activará la seguridad para el segundo estrato (el AS para dos o más RAT). Si la información no se aplicó al AS, un nodo de RAN activa la seguridad para el AS utilizando un procedimiento de AS.

Sin el procedimiento descrito en la presente memoria, puede haber una configuración de seguridad entre el UE y la CN para cada conexión de UE a CN, y para LTE puede haber además una configuración de seguridad de AS separada. Por ejemplo, para LTE y 3G tendrían que ejecutarse dos procedimientos separados correspondientes a la señalización de los pasos paso2 y paso3 de la Figura 6.

En un escenario donde el UE está conectado a una RAT de 3GPP y luego es traspasado a una segunda RAT, el UE y los nodos de CN primero deben ejecutar una señalización para establecer la seguridad para la primera RAT y luego, durante el traspaso, necesitan realizar una señalización adicional para establecer la seguridad para la segunda RAT. En un escenario donde un UE realiza un traspaso de LTE a 3G, el UE no realiza un establecimiento de seguridad para 3G, sino que confía en los mismos parámetros de seguridad utilizados en LTE. En otras palabras, no hay ninguna configuración de seguridad para 3G.

Mediante el procedimiento descrito en la presente memoria, puede manejarse una configuración del contexto de

seguridad para un UE capaz de emplear dos RAT para las dos RAT al mismo tiempo en un único procedimiento por estrato para reducir la sobrecarga de señalización. Además, la configuración del contexto de seguridad puede incluir un procedimiento de autenticación, un procedimiento de activación (de UE de CN) de NAS y un procedimiento de activación de AS (UE de RAN), en donde cada procedimiento puede utilizar un procedimiento común para ambas RAT. Además, puede activarse una única solicitud de comando de modo de seguridad de AS desde la BS al UE para ambas RAT en la seguridad del UE para dos RAT. Además, puede activarse una única solicitud de comando de modo de seguridad de NAS desde la CN al UE para ambas RAT en la seguridad del UE para la clave de CN para las dos RAT, y posiblemente informa al UE de si el comando de modo de seguridad de AS debe aplicarse a una o ambas RAT.

En la presente memoria, se describen métodos para manejar el contexto de seguridad del UE a través de un procedimiento común que supone un escenario con una integración estrecha de múltiples interfaces aéreas (tales como LTE y 5G). El método puede resumirse de la siguiente manera:

1. El UE se conecta a la CN tanto para los servicios de 5G como de LTE.

2. La CN autentica el UE tanto para los servicios de 5G como de LTE y deriva una clave de nivel de CN (por ejemplo, K_{ASME}).

3. a. La CN deriva un material de clave de nivel de RAN común (por ejemplo, K_{eNB}) o separado tanto para 5G como para LTE a partir de un material de clave de nivel de CN común (por ejemplo, K_{ASME}) o separado; y envía el material de clave de nivel de RAN derivado al elemento de RAN. El UE también deriva de manera similar el mismo material de clave (por ejemplo, K_{eNB} de K_{ASME}) para calcular otras claves de seguridad y activar la seguridad de extremo a extremo tanto para servicios de NX/5G como de LTE.

b. El elemento de RAN deriva una clave de NX/5G a partir de K_{eNB} y utiliza la clave de 5G como base para cualquier clave de cifrado e integridad que deba utilizarse en 5G.

Aquí, CN se refiere a una función de CN lógica y/o un elemento de red de CN, por ejemplo, que maneja solicitudes de conexión, y el elemento de RAN denota un nodo de RAN o una función lógica donde la conexión multi-RAT (como una entidad RRC común) termina en el lado de la red.

Como consecuencia, se reduce la señalización para la seguridad de la segunda RAT, por ejemplo, al mínimo. Puede garantizarse la compartimentación del material de clave de RAN en el mismo nivel de seguridad que la conectividad dual de LTE. Es decir, un atacante que obtenga el material de clave para la segunda RAT no tendrá acceso al material de clave para la primera RAT, pero un atacante que obtenga el material de clave para la primera RAT podrá derivar el material de clave para la segunda RAT.

Por medio de la técnica descrita en la presente memoria, se proporciona una forma más eficiente de manejar el contexto de seguridad para múltiples RAT y los procedimientos de seguridad relacionados. En consecuencia, puede reducirse la sobrecarga de señalización y el consumo de energía de la misma. La reducción de la señalización se produce cuando el UE configura una conectividad dual o múltiple entre las RAT duales o múltiples, respectivamente, de modo que el contexto de seguridad de la segunda RAT ya esté preparado. Los parámetros de seguridad para la segunda RAT pueden proporcionarse incorporados en los procedimientos de seguridad aplicados para la primera RAT.

Crear el contexto de seguridad por adelantado para RAT duales/múltiples también significa que el plano de usuario puede habilitarse más rápido al cambiar de una RAT a otra.

Los detalles explicados anteriormente con respecto a las Figuras 2 a 6 pueden resumirse con respecto a la Figura 7. La Figura 7 es un diagrama de bloques que ilustra esquemáticamente una realización de dispositivo de un elemento de red 2 que soporta la configuración del contexto de seguridad en una red de comunicación inalámbrica.

A modo de ejemplo, se describe el elemento de red 2 para implementar las funcionalidades del elemento de red de acceso por radio 200 según la realización de la Figura 2. El elemento de red de acceso por radio 2 comprende una memoria 4 y un procesador 6 acoplados entre sí. El elemento de red de acceso por radio puede comprender además una interfaz opcional acoplada al procesador 6. La memoria 4 contiene instrucciones de control ejecutables por el procesador 6.

El procesador 6 está configurado para iniciar la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común. La interfaz puede configurarse para llevar a cabo cualquier comunicación con otros componentes de la red de comunicación. Por ejemplo, la interfaz puede transmitir información a otros componentes de la red de comunicación y/o puede recibir información de otros componentes de la red de comunicación.

Alternativamente, el elemento de red 2 se describe para implementar las funcionalidades del elemento de red central 300 según la realización de la Figura 2. El elemento de red de acceso por radio 2 comprende una memoria 4 y un procesador 6 acoplados entre sí. El elemento de red de acceso por radio puede comprender además una interfaz opcional acoplada al procesador 6. La memoria 4 contiene instrucciones de control ejecutables por el procesador 6. El procesador 6 está configurado para informar a un elemento de red de acceso por radio (RAN) de la red de

comunicación inalámbrica, que inicie la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común. La interfaz puede configurarse para llevar a cabo cualquier comunicación con otros componentes de la red de comunicación. Por ejemplo, la interfaz puede transmitir información a otros componentes de la red de comunicación y/o puede recibir información de otros componentes de la red de comunicación.

Alternativamente, se describe el elemento de red 2 para implementar las funcionalidades del dispositivo de comunicación inalámbrica 100 según la realización de la Figura 1. El elemento de red de acceso por radio 2 comprende una memoria 4 y un procesador 6 acoplados entre sí. El elemento de red de acceso por radio puede comprender además una interfaz opcional acoplada al procesador 6. La memoria 4 contiene instrucciones de control ejecutables por el procesador 6. El procesador 6 está configurado para recibir, desde un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica en un procedimiento de señalización común, información que permite al dispositivo de comunicación inalámbrica configurar un contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT. El procesador está configurado además para configurar el contexto de seguridad de AS para la primera RAT y la segunda RAT.

La Figura 8 muestra un diagrama de bloques funcional de un elemento de red de acceso por radio 20 configurado según los principios de la divulgación como se describió anteriormente. Los bloques funcionales del elemento de red 20 pueden implementarse mediante hardware, software o una combinación de hardware y software para llevar a cabo los principios de la divulgación. Un experto en la técnica entenderá que los bloques funcionales descritos en la Figura 8 pueden combinarse en uno o más bloques o separarse en subbloques para implementar los principios de la divulgación como se describió anteriormente. Por lo tanto, la descripción de la presente memoria puede admitir cualquier posible combinación o separación o definición adicional de los bloques funcionales descritos en la presente memoria.

El elemento de red de acceso por radio 20 de la Figura 8 es para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica. El elemento de red 20 comprende un módulo de iniciación 22 para iniciar la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común.

El elemento de red 20 puede comprender un módulo de recepción 24. El módulo de recepción es para recibir, por el elemento de RAN, un primer material de clave de RAN desde de un elemento de red central (CN) de la red de comunicación inalámbrica. El primer material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la primera RAT. El módulo de recepción es además para recibir, por el elemento de RAN, un segundo material de clave de RAN desde el elemento de CN de la red de comunicación inalámbrica. El segundo material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la segunda RAT.

El módulo de recepción puede ser para recibir, por el elemento de RAN, un primer material de clave de RAN desde un elemento de CN de la red de comunicación inalámbrica. El primer material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la primera RAT. El elemento de red 20 puede comprender además un módulo de derivación para derivar, por el elemento de RAN, un segundo material de clave de RAN a partir del primer material de clave de RAN recibido. El segundo material de clave de RAN permite al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la segunda RAT.

El elemento de red 20 puede comprender además un módulo de transmisión 26 para transmitir, por el elemento de RAN, un mensaje de comando de modo de seguridad de AS común para la primera RAT y la segunda RAT a un dispositivo de comunicación inalámbrica de la red de comunicación inalámbrica.

El módulo de recepción puede además ser para recibir, por el elemento de RAN, un mensaje de modo de seguridad de AS completo que informa al elemento de RAN de la finalización de la configuración del contexto de seguridad de AS para la primera RAT y la segunda RAT.

El elemento de red 20 puede corresponder al elemento de RAN que implementa la primera RAT y puede corresponder o ser diferente del elemento de RAN que implementa la segunda RAT.

La Figura 9 muestra un diagrama de bloques funcional de un elemento de red central 40 configurado de acuerdo con los principios de la divulgación como se describió anteriormente. Los bloques funcionales del elemento de red 40 pueden implementarse mediante hardware, software o una combinación de hardware y software para llevar a cabo los principios de la divulgación. Un experto en la técnica entenderá que los bloques funcionales descritos en la Figura 9 pueden combinarse en uno o más bloques o separarse en subbloques para implementar los principios de la divulgación como se describió anteriormente. Por lo tanto, la descripción de la presente memoria puede admitir cualquier posible combinación o separación o definición adicional de los bloques funcionales descritos en la presente memoria.

El elemento de red central 40 de la Figura 9 soporta la configuración del contexto de seguridad en una red de comunicación inalámbrica. El elemento de red central 40 comprende un módulo de información 42 para informar a un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica, que inicie la configuración del contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT en un procedimiento de señalización común.

El elemento de red central 40 puede comprender un módulo de recepción 44 para recibir, por el elemento de CN desde un dispositivo de comunicación inalámbrica, información sobre las capacidades de seguridad del dispositivo de comunicación inalámbrica con respecto a la primera RAT y la segunda RAT.

El elemento de red central 40 puede comprender un módulo de iniciación 46 para iniciar, por el elemento de CN, la configuración del contexto de seguridad de estrato de no acceso (NAS) para la primera RAT y la segunda RAT en un procedimiento de señalización común.

El módulo de iniciación puede ser además para iniciar la configuración del contexto de seguridad de NAS, lo que comprende solicitar, por el elemento de CN, a un dispositivo de comunicación inalámbrica que realice la autenticación hacia el elemento de CN.

El elemento de red central 40 puede comprender un módulo de derivación 48 para derivar, por el elemento de CN, material de clave de CN que permite a un dispositivo de comunicación inalámbrica realizar la autenticación para la primera RAT y permite al dispositivo de comunicación inalámbrica realizar la autenticación para la segunda RAT.

El elemento de red central 40 puede comprender un módulo de transmisión 50 para transmitir, por el elemento de CN, el material de clave de CN al dispositivo de comunicación inalámbrica.

El módulo de recepción puede ser además para recibir, por el elemento de CN, un mensaje de respuesta de autenticación desde el dispositivo de comunicación inalámbrica.

El módulo de derivación puede ser además para derivar, por el elemento de CN, material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS.

El módulo de transmisión puede ser además para transmitir, por el elemento de CN, un mensaje de comando de modo de seguridad de NAS para la primera RAT y la segunda RAT al dispositivo de comunicación inalámbrica, permitiendo el mensaje de comando de modo de seguridad de NAS al dispositivo de comunicación inalámbrica derivar el material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS.

El módulo de recepción puede ser además para recibir, por el elemento de CN, un mensaje de modo de seguridad de NAS completo para la primera RAT y la segunda RAT desde el dispositivo de comunicación inalámbrica.

La Figura 10 muestra un diagrama de bloques funcional de un dispositivo de comunicación inalámbrica 60 configurado de acuerdo con los principios de la divulgación como se describió anteriormente. Los bloques funcionales del dispositivo de comunicación inalámbrica 6 pueden implementarse mediante hardware, software o una combinación de hardware y software para llevar a cabo los principios de la divulgación. Un experto en la técnica entenderá que los bloques funcionales descritos en la Figura 10 pueden combinarse en uno o más bloques o separarse en subbloques para implementar los principios de la divulgación como se describió anteriormente. Por lo tanto, la descripción de la presente memoria puede admitir cualquier posible combinación o separación o definición adicional de los bloques funcionales descritos en la presente memoria.

El dispositivo de comunicación inalámbrica 60 de la Figura 10 soporta la configuración del contexto de seguridad en una red de comunicación inalámbrica. El dispositivo de comunicación inalámbrica 60 comprende un módulo de recepción 62 para recibir, desde un elemento de red de acceso por radio (RAN) de la red de comunicación inalámbrica en un procedimiento de señalización común, información que permite a la comunicación inalámbrica configurar un contexto de seguridad de estrato de acceso (AS) para una primera tecnología de acceso por radio (RAT) y una segunda RAT. El dispositivo de comunicación inalámbrica 60 comprende además un módulo de configuración 64 para configurar el contexto de seguridad de AS para la primera RAT y la segunda RAT.

El módulo de recepción puede ser además para recibir, por el dispositivo de comunicación inalámbrica desde el elemento de RAN de la red de comunicación inalámbrica, un mensaje de comando de modo de seguridad de AS común para la primera RAT y la segunda RAT.

El dispositivo de comunicación inalámbrica 60 puede comprender además un módulo de transmisión 66 para transmitir, por el dispositivo de comunicación inalámbrica, un mensaje de modo de seguridad de AS completo al elemento de RAN, informando el mensaje de modo de seguridad de AS completo al elemento de RAN de la finalización de la configuración del contexto de seguridad de AS para la primera RAT y la segunda RAT.

El módulo de transmisión puede ser además para transmitir, por el dispositivo de comunicación inalámbrica a un elemento de red central, CN, de la red de comunicación inalámbrica, información sobre las capacidades de seguridad del dispositivo de comunicación inalámbrica con respecto a la primera RAT y la segunda RAT.

El módulo de recepción puede ser además para recibir, por el dispositivo de comunicación inalámbrica desde un elemento de CN, una solicitud para realizar una autenticación hacia el elemento de CN.

El módulo de transmisión puede ser además para transmitir, por el dispositivo de comunicación inalámbrica, un mensaje de respuesta de autenticación al elemento de CN.

El módulo de recepción puede ser además para recibir, por el dispositivo de comunicación inalámbrica, un mensaje de comando de modo de seguridad de NAS para la primera RAT y la segunda RAT desde el elemento de CN y derivar, por el dispositivo de comunicación inalámbrica, material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS para la primera RAT y la segunda RAT a partir del mensaje de comando de modo de seguridad de NAS recibido.

El módulo de transmisión puede ser además para transmitir, por el dispositivo de comunicación inalámbrica, un mensaje de modo de seguridad de NAS completo para la primera RAT y la segunda RAT al elemento de CN.

Muchas ventajas de la presente divulgación se entenderán plenamente a partir de la descripción anterior, y será evidente que pueden realizarse varios cambios en la forma, construcción y disposición de las unidades y dispositivos sin apartarse del alcance de la presente divulgación y/o sin sacrificar todas sus ventajas.

REIVINDICACIONES

1. Un método para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica, comprendiendo el método iniciar (S304), por un elemento (200) de red de acceso por radio, RAN, de la red de comunicación inalámbrica, la configuración del contexto de seguridad de estrato de acceso, AS, para una primera tecnología de acceso por radio, RAT, y una segunda RAT en un procedimiento de señalización común, en donde el elemento de RAN (200) corresponde al elemento de RAN que implementa la primera RAT y es diferente de un elemento de RAN que implementa la segunda RAT, en donde el paso de iniciar (S304) la configuración del contexto de seguridad de AS comprende transmitir, por un elemento de red central, CN, (300) a través del elemento de RAN (200), un único mensaje de comando de modo de seguridad de estrato de no acceso, NAS, común para la primera RAT y la segunda RAT a un dispositivo de comunicación inalámbrica (100) de la red de comunicación inalámbrica.

2. El método según la reivindicación 1, comprendiendo el método recibir, por el elemento de RAN (200), un primer material de clave de RAN desde el elemento de red central, CN, (300) de la red de comunicación inalámbrica, permitiendo el primer material de clave de RAN al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la primera RAT y recibir, por el elemento de RAN, un segundo material de clave de RAN desde el elemento de CN de la red de comunicación inalámbrica, permitiendo el segundo material de clave de RAN al elemento de RAN iniciar la configuración del contexto de seguridad de AS para la segunda RAT; o comprendiendo el método recibir, por el elemento de RAN (200), un primer material de clave de RAN desde un elemento de CN de la red de comunicación inalámbrica, permitiendo el primer material de clave de RAN al elemento de RAN (200) iniciar la configuración del contexto de seguridad de AS para la primera RAT y derivar, por el elemento de RAN (200), un segundo material de clave de RAN a partir del primer material de clave de RAN recibido, permitiendo el segundo material de clave de RAN al elemento de RAN (200) iniciar la configuración del contexto de seguridad de AS para la segunda RAT.

3. El método de la reivindicación 1 ó 2, en donde sólo hay una conexión de CN de RAN por dispositivo de comunicación inalámbrica (100) para ambas RAT.

4. El método de cualquiera de las reivindicaciones 1 a 3, en donde el paso de iniciar la configuración del contexto de seguridad de AS incluye:

- utilizar directamente el primer material de clave de RAN recibido para iniciar la configuración del contexto de seguridad de AS para la primera RAT; o

- derivar el tercer material de clave de RAN a partir del primer material de clave de RAN recibido y utilizar el tercer material de clave de RAN derivado para iniciar la configuración del contexto de seguridad de AS para la primera RAT.

5. El método de cualquiera de las reivindicaciones 1 a 4, comprendiendo el método recibir, por el elemento de RAN (200), un mensaje de modo de seguridad de NAS completo que informa al elemento de RAN de la finalización de la configuración del contexto de seguridad de AS para la primera RAT y la segunda RAT.

6. Método para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica, comprendiendo el método informar, por un elemento de red central, CN, (300) de la red de comunicación inalámbrica, a un elemento de red de acceso por radio, RAN, (200) de la red de comunicación inalámbrica, que inicie la configuración del contexto de seguridad de estrato de acceso, AS, para una primera tecnología de acceso por radio, RAT, y una segunda RAT en un procedimiento de señalización común, en donde el elemento de RAN (200) corresponde al elemento de RAN que implementa la primera RAT y es diferente de un elemento de RAN que implementa la segunda RAT, en donde el inicio de la configuración del contexto de seguridad de AS comprende transmitir, por el elemento de CN (300) a través del elemento de RAN (200), un único mensaje de comando de modo de seguridad de NAS común para la primera RAT y la segunda RAT a un dispositivo de comunicación inalámbrica (100) de la red de comunicación inalámbrica.

7. El método de la reivindicación 6, comprendiendo el método recibir, por el elemento de CN (300) desde un dispositivo de comunicación inalámbrica (100), información sobre las capacidades de seguridad del dispositivo de comunicación inalámbrica con respecto a la primera RAT y la segunda RAT.

8. El método de la reivindicación 6 ó 7, comprendiendo el método iniciar, por el elemento de CN (300), la configuración del contexto de seguridad de estrato de no acceso, NAS, para la primera RAT y la segunda RAT en un procedimiento de señalización común, en donde, opcionalmente, el paso de iniciar la configuración del contexto de seguridad de NAS comprende solicitar, por el elemento de CN (300), a un dispositivo de comunicación inalámbrica (100) que realice la autenticación hacia el elemento de CN (300); y/o comprendiendo el método derivar, por el elemento de CN (300), material de clave de CN que permite a un dispositivo de comunicación inalámbrica realizar la autenticación para la primera RAT y que permite al dispositivo de comunicación inalámbrica (100) realizar la autenticación para la segunda RAT, comprendiendo el método, por ejemplo, transmitir, por el elemento de CN (300), el material de clave de CN al dispositivo de comunicación inalámbrica (100).

9. El método de la reivindicación 8, comprendiendo el método recibir, por el elemento de CN (300), un mensaje de respuesta de autenticación desde el dispositivo de comunicación inalámbrica (100).

10. El método de cualquiera de las reivindicaciones 6 a 9, comprendiendo el método derivar, por el elemento de CN (300), material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS, en donde el mensaje de comando de modo de seguridad de NAS permite al dispositivo de comunicación inalámbrica derivar el material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS, comprendiendo además el método, por ejemplo, recibir, por el elemento de CN (300), de un mensaje de modo de seguridad de NAS completo para la primera RAT y la segunda RAT desde el dispositivo de comunicación inalámbrica (100).

11. Un método para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica, comprendiendo el método:

- recibir, por un dispositivo de comunicación inalámbrica (100) de la red de comunicación inalámbrica desde un elemento de red central, CN, (300) a través de un elemento de red de acceso por radio, RAN, (200) de la red de comunicación inalámbrica en un procedimiento de señalización común, información que permite a la comunicación inalámbrica configurar un contexto de seguridad de estrato de acceso, AS, para una primera tecnología de acceso por radio, RAT, y una segunda RAT,

- y configurar, por el dispositivo de comunicación inalámbrica (100), el contexto de seguridad de AS para la primera RAT y la segunda RAT,

en donde el elemento de RAN (200) corresponde al elemento de RAN que implementa la primera RAT y es diferente de un elemento de RAN que implementa la segunda RAT, comprendiendo el método recibir, por el dispositivo de comunicación inalámbrica (100) desde el elemento de red central, CN, (300) a través del elemento de RAN (200) de la red de comunicación inalámbrica, un único mensaje de comando de modo de seguridad de estrato de no acceso, NAS, común para la primera RAT y la segunda RAT.

12. El método según la reivindicación 11, comprendiendo el método transmitir, por el dispositivo de comunicación inalámbrica (100), un mensaje de modo de seguridad de NAS completo al elemento de RAN (200), informando el mensaje de modo de seguridad de NAS completo al elemento de RAN de la finalización de la configuración del contexto de seguridad de AS para la primera RAT y la segunda RAT; y/o comprendiendo el método transmitir, por el dispositivo de comunicación inalámbrica (100) a un elemento de red central, CN, (300) de la red de comunicación inalámbrica, información sobre las capacidades de seguridad del dispositivo de comunicación inalámbrica con respecto a la primera RAT y la segunda RAT; y/o comprendiendo el método recibir, por el dispositivo de comunicación inalámbrica (100) desde un elemento de CN (300), una solicitud para realizar la autenticación hacia el elemento de CN (300), en donde el método opcionalmente comprende además transmitir, por el dispositivo de comunicación inalámbrica (100), un mensaje de respuesta de autenticación al elemento de CN (300).

13. El método según la reivindicación 11 ó 12, comprendiendo el método derivar, por el dispositivo de comunicación inalámbrica (100), material de clave de CN para la protección de la integridad y el cifrado de la comunicación de NAS para la primera RAT y la segunda RAT a partir del mensaje de comando de modo de seguridad de NAS recibido; y/o comprendiendo el método transmitir, por el dispositivo de comunicación inalámbrica (100), un mensaje de modo de seguridad de NAS completo para la primera RAT y la segunda RAT al elemento de CN (300).

14. Un elemento de red de acceso por radio, RAN, (200) para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica, estando configurado el elemento de RAN para realizar el método de cualquiera de las reivindicaciones 1 a 5.

15. Elemento de RAN (200) según la reivindicación 14, comprendiendo el elemento de RAN (200) o estando configurado como o siendo parte de una estación base de radio, un controlador de red de radio, un NodoB, un eNodoB, un controlador de unidad de radio de 5G o una estación base de 5G.

16. Un elemento de red central, CN, (300) para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica, estando configurado el elemento de CN (300) para realizar el método de cualquiera de las reivindicaciones 6 a 10.

17. Un dispositivo de comunicación inalámbrica (100) para soportar la configuración del contexto de seguridad en una red de comunicación inalámbrica, estando el dispositivo de comunicación inalámbrica (100) configurado para realizar el método de cualquiera de las reivindicaciones 11 a 13.

18. Un sistema de comunicación inalámbrica (20) que comprende el elemento de RAN (200) de la reivindicación 14 ó 15, el elemento de CN (300) de la reivindicación 16 y uno o más dispositivos de comunicación inalámbrica (100) de la reivindicación 17.

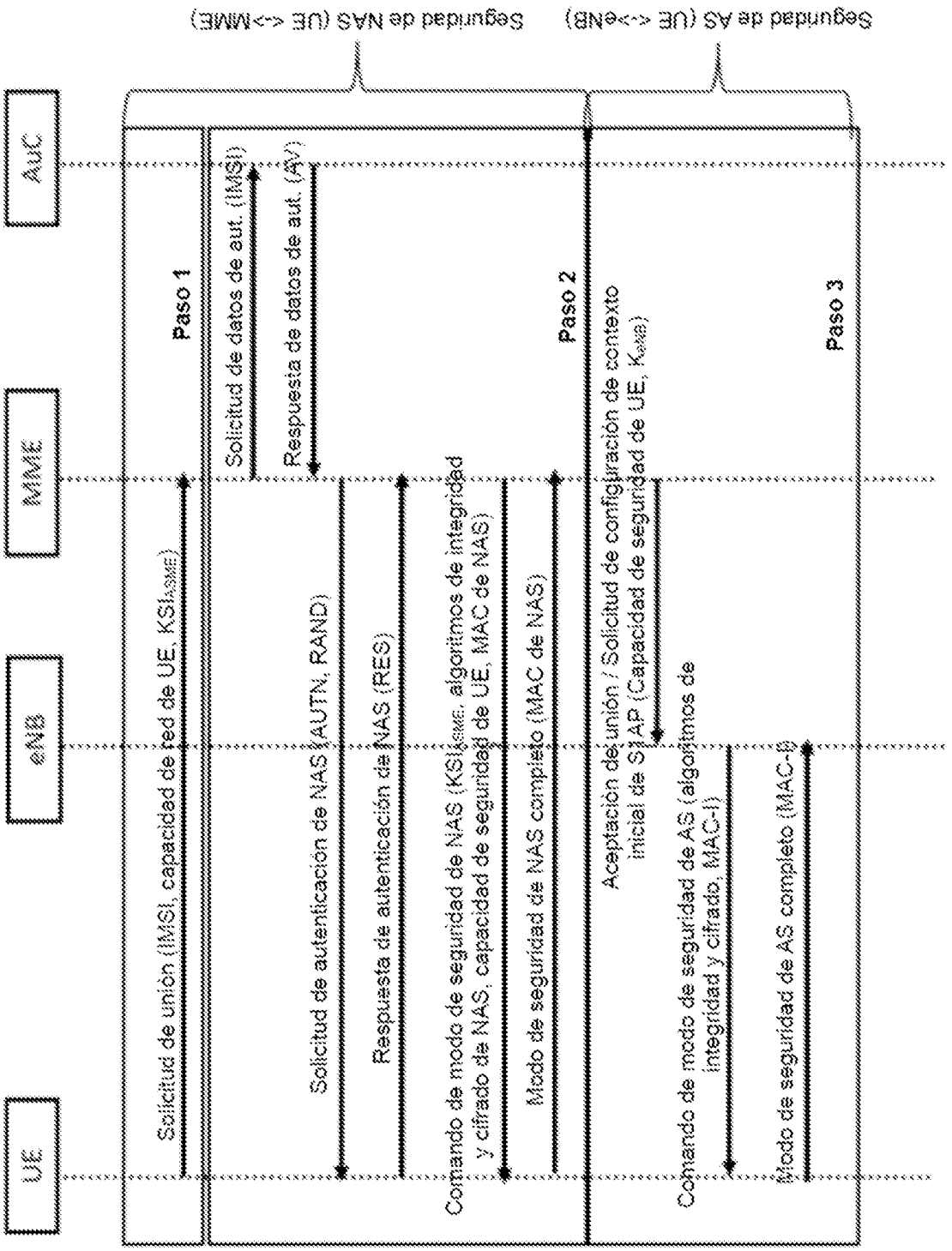
UE
eNB
MME
AuC
Seguridad de NAS (UE <->MME)
Seguridad de AS (UE <->eNB)
Paso 1
Paso 2
Paso 3
Solicitud de unión (IMSI, capacidad de red de UE, KSI)
Solicitud de datos de aut. (IMSI)
Respuesta de datos de aut. (AV)
Solicitud de autenticación de NAS (AUTN, RAND)
Respuesta de autenticación de NAS (RES)
Comando de modo de seguridad de NAS (KSI, algoritmos de integridad y cifrado de NAS, capacidad de seguridad de UE, MAC de NAS)
Modo de seguridad de NAS completo (MAC de NAS)
Aceptación de unión / Solicitud de configuración de contexto inicial de S1AP (Capacidad de seguridad de UE, K)
Comando de modo de seguridad de AS (algoritmos de integridad y cifrado, MAC-I)
Modo de seguridad de AS completo (MAC-I)

Fig. 1

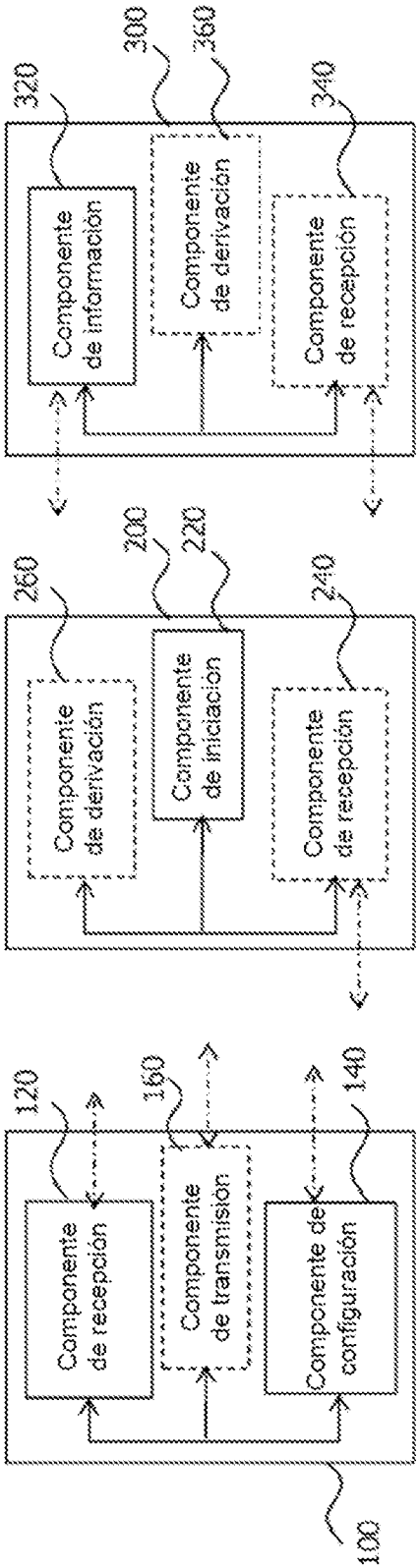
320
300
360
340
Componente de información
Componente de derivación
Componente de recepción
260
200
220
240
Componente de derivación
Componente de iniciación
Componente de recepción
120
160
140
Componente de recepción
Componente de transmisión
Componente de configuración
100
20

Fig. 2

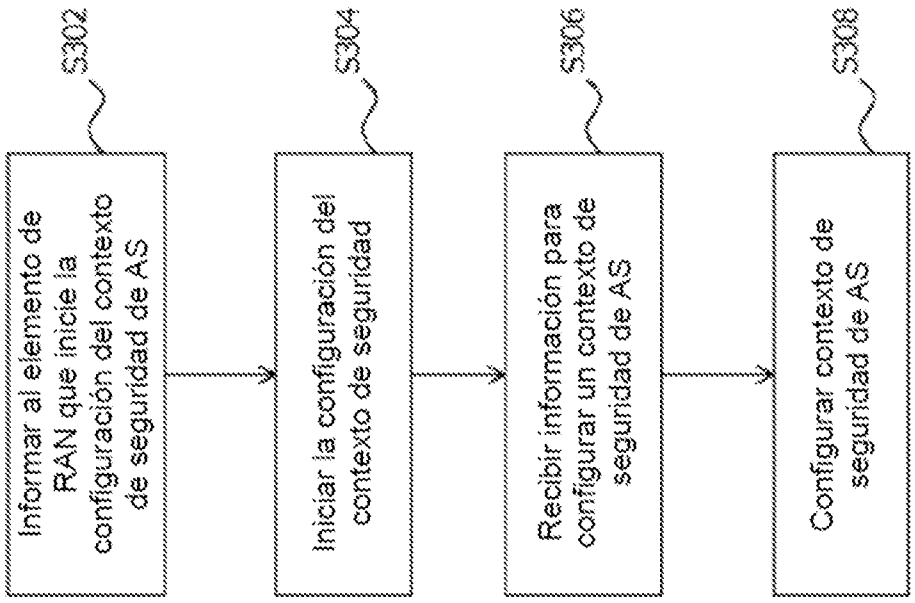
S302
Informar al elemento de RAN que inicie la configuración del contexto de seguridad de AS
S304
Iniciar la configuración del contexto de seguridad
S306
Recibir información para configurar un contexto de seguridad de AS
S308
Configurar contexto de seguridad de AS

Fig. 3

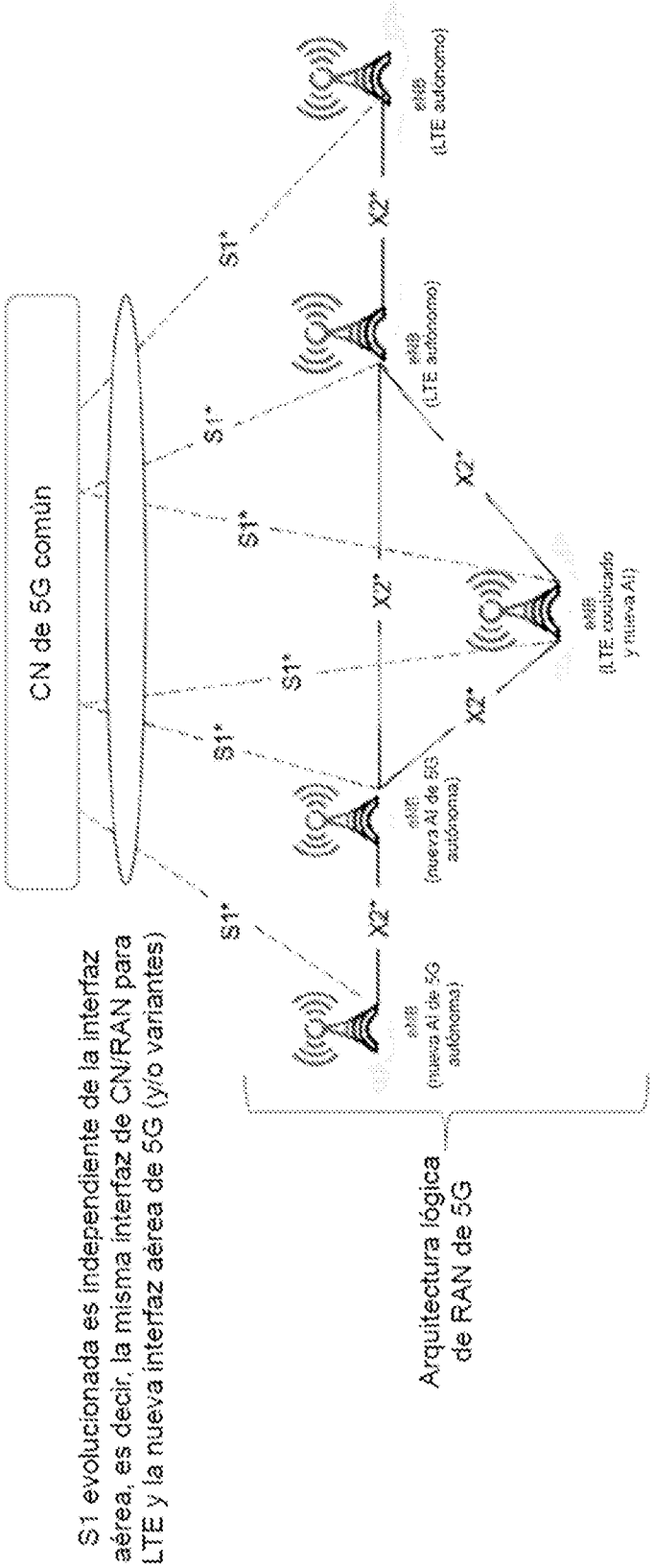
CN de 5G común
S1 evolucionada es independiente de la interfaz aérea, es decir, la misma interfaz de CN/RAN para LTE y la nueva interfaz aérea de 5G (y/o variantes)
S1*
X2*
eNB (nueva AI de 5G autónoma)
eNB (nueva AI de 5G autónoma)
eNB (LTE autónomo)
eNB (LTE autónomo)
eNB (LTE combinado y nueva AI)
Arquitectura lógica de RAN de 5G

Fig. 4

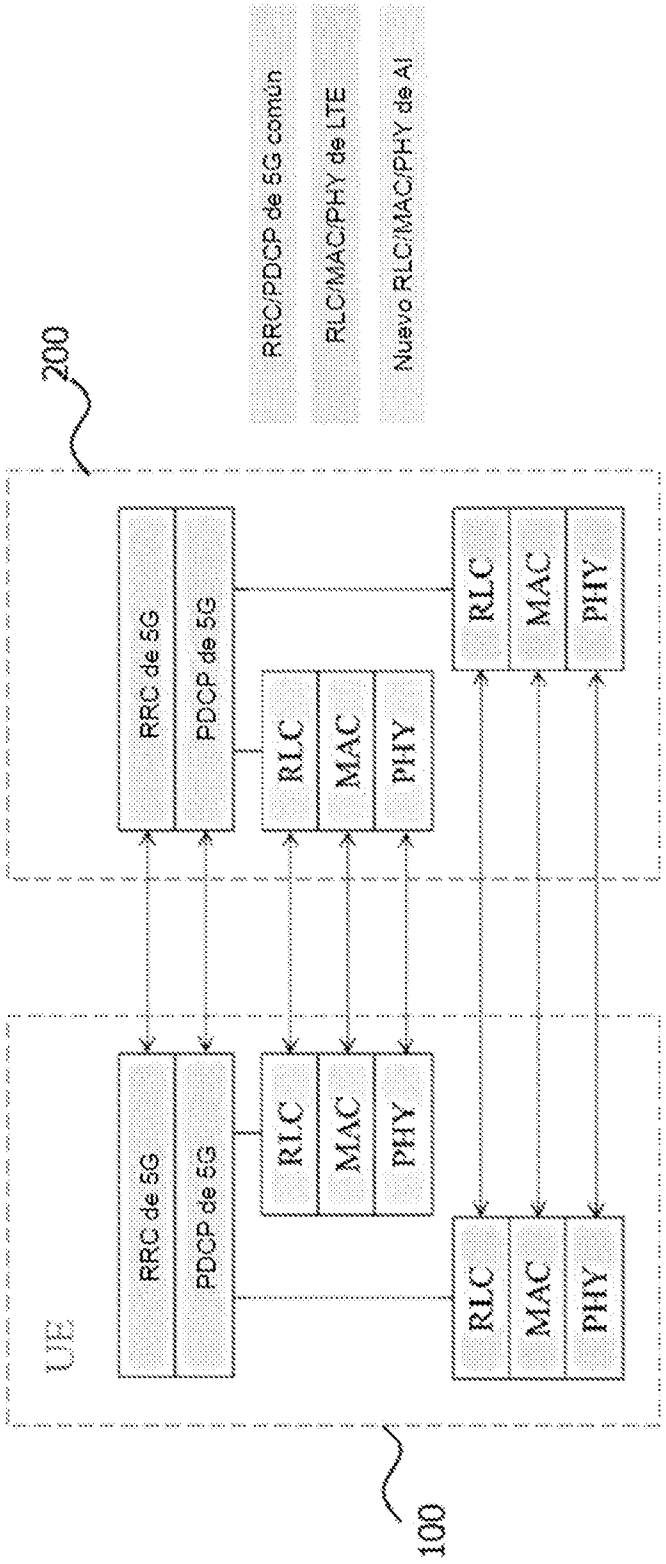
RRC/PDCP de 5G común
RLC/MAC/PHY de LTE
Nuevo RLC/MAC/PHY de AI
200
RRC de 5G
PDCP de 5G
RLC
MAC
PHY
RLC
MAC
PHY
UE
RRC de 5G
PDCP de 5G
RLC
MAC
PHY
RLC
MAC
PHY
100

Fig. 5

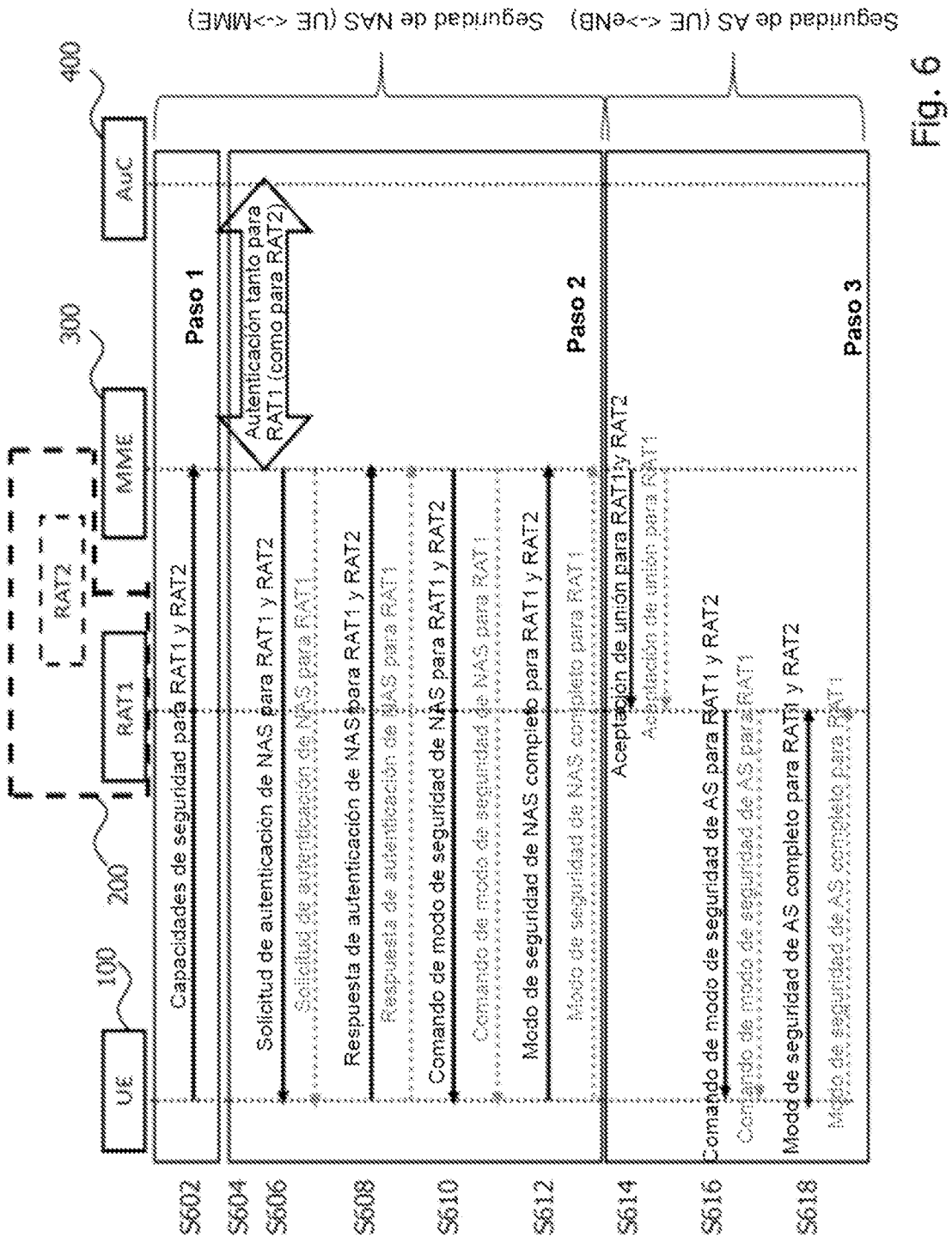
Seguridad de AS (UE <->eNB)
Seguridad de NAS (UE <->MME)
UE
100
RAT1
200
RAT2
MME
300
AuC
400
Paso 1
Paso 2
Paso 3
Capacidades de seguridad para RAT1 y RAT2
Solicitud de autenticación de NAS para RAT1 y RAT2
Autenticación tanto para RAT1 (como para RAT2)
Solicitud de autenticación de NAS para RAT1
Respuesta de autenticación de NAS para RAT1 y RAT2
Respuesta de autenticación de NAS para RAT1
Comando de modo de seguridad de NAS para RAT1 y RAT2
Comando de modo de seguridad de NAS para RAT1
Modo de seguridad de NAS completo para RAT1 y RAT2
Modo de seguridad de NAS completo para RAT1
Aceptación de unión para RAT1 y RAT2
Aceptación de unión para RAT1
Comando de modo de seguridad de AS para RAT1 y RAT2
Comando de modo de seguridad de AS para RAT1
Modo de seguridad de AS completo para RAT1 y RAT2
Modo de seguridad de AS completo para RAT1
S602
S604
S606
S608
S610
S612
S614
S616
S618

Fig. 6

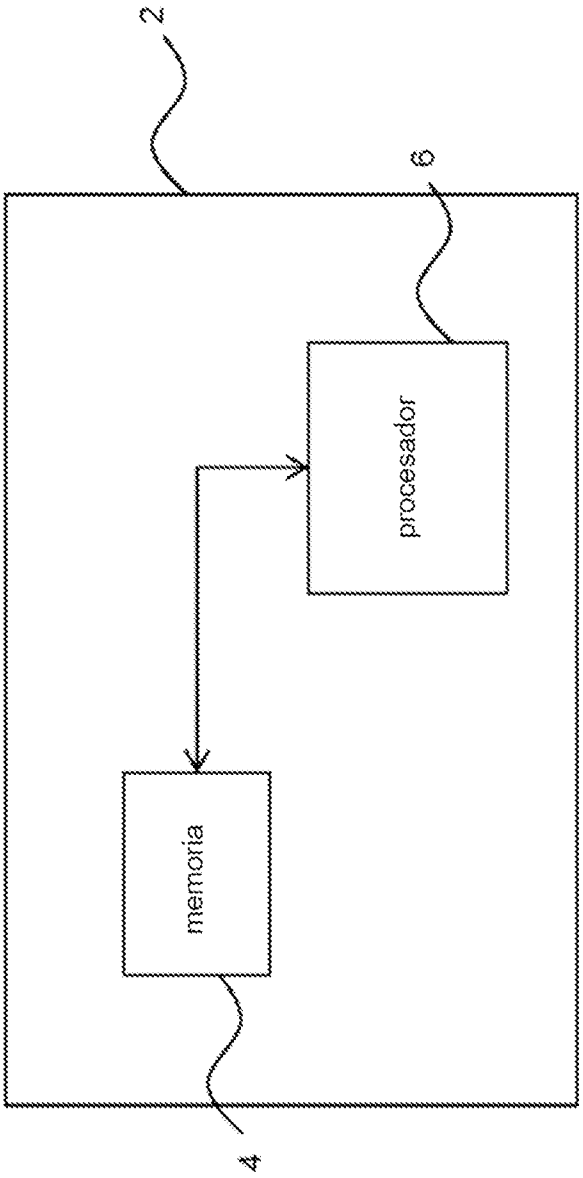

Fig. 7

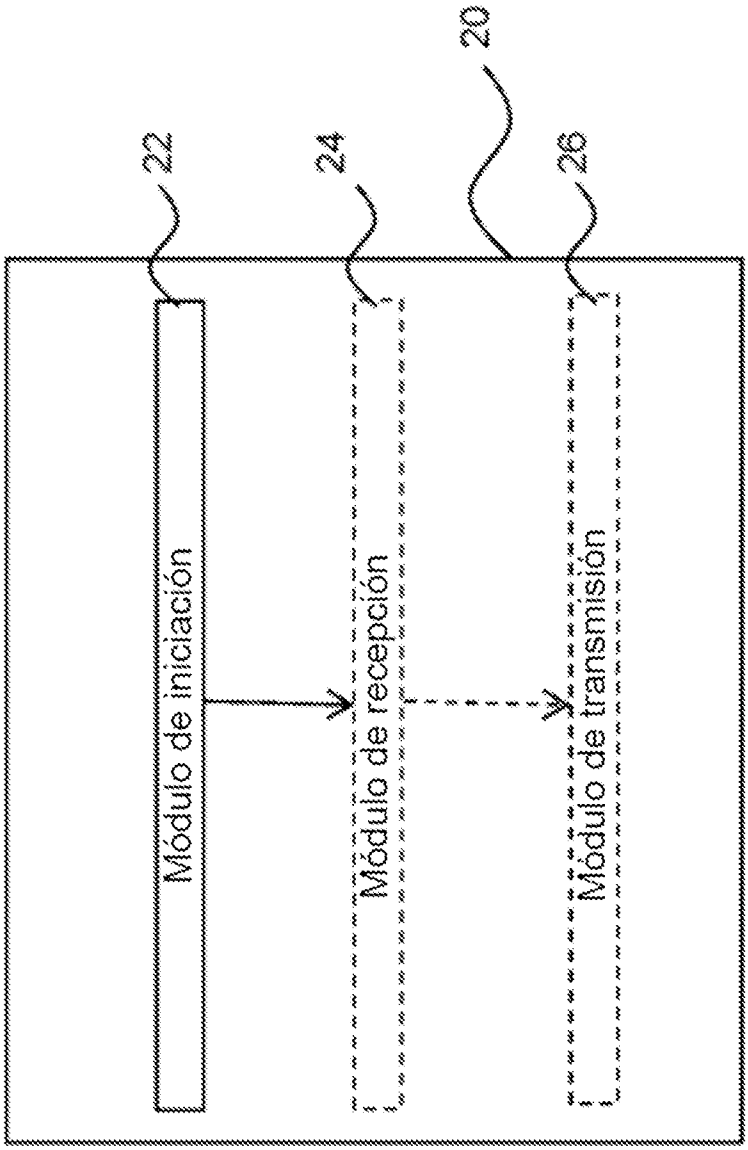
20
22
24
26
Módulo de iniciación
Módulo de recepción
Módulo de transmisión

Fig. 8

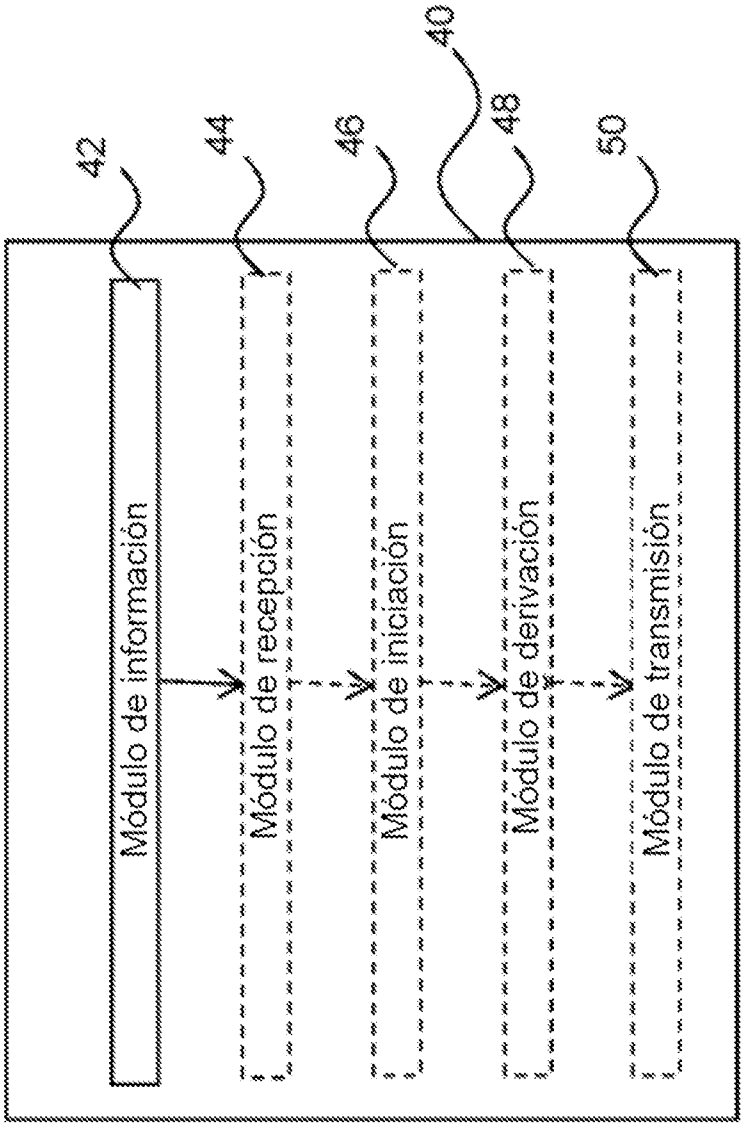
40
42
44
46
48
50
Módulo de información
Módulo de recepción
Módulo de iniciación
Módulo de derivación
Módulo de transmisión

Fig. 6

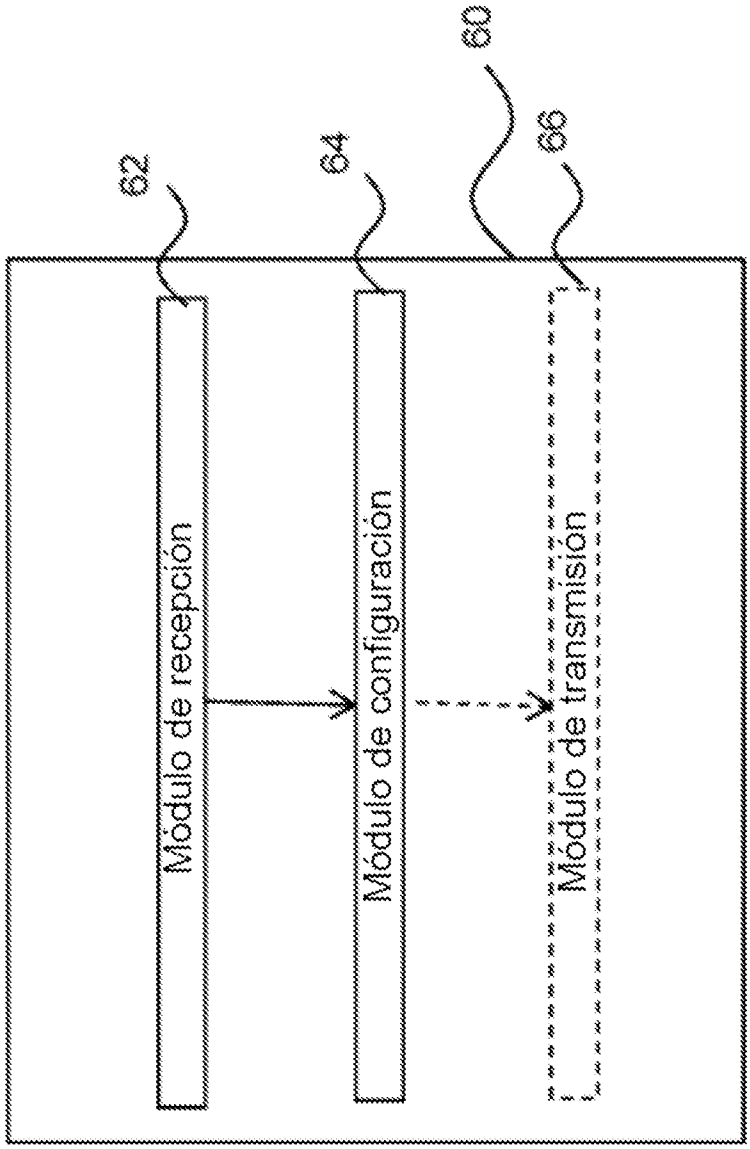
60
62
64
66
Módulo de recepción
Módulo de configuración
Módulo de transmisión

Fig. 10