(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 935 616**

(51) Int. CI.:

H04L 9/00 (2012.01)
H04L 9/08 (2006.01)
H04W 12/00 (2011.01)
H04W 12/04 (2011.01)
H04W 12/041 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2016 PCT/US2016/052682**

(87) Fecha y número de publicación internacional: **29.03.2018 WO18056957**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2016 E 16916929 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2022 EP 3516819**

(54) Título: **Identificador del conjunto de claves de próxima generación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2023

(73) Titular/es:

NOKIA SOLUTIONS AND NETWORKS OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

JERICHOW, ANJA y
NAIR, SURESH

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Identificador del conjunto de claves de próxima generación

Antecedentes:

Campo:

Las realizaciones de la invención se refieren en general a redes de comunicaciones inalámbricas o móviles, tales como, pero sin limitarse a, la Universal Mobile Telecommunications System (red de acceso de radio terrestre - UTRAN) del Terrestrial Radio Access Network (sistema universal de telecomunicaciones móviles - UMTS), Long Term Evolution (evolución a largo plazo - LTE), Evolved UTRAN (UTRAN evolucionada - E-UTRAN), LTE-Advanced (LTE avanzada - LTE-A), LTE-A Pro y/o tecnología de acceso de radio 5G. Algunas realizaciones pueden referirse en general a la seguridad de 5G que incluye, por ejemplo, gestionar y acceder al contexto de seguridad y la jerarquía de claves en 5G, e identificar el contexto de seguridad de 5G y el punto de inicio de la derivación de claves.

Descripción de la técnica relacionada:

La Terrestrial Radio Access Network (red de acceso de radio terrestre - UTRAN) del Universal Mobile Telecommunications System (sistema universal de telecomunicaciones móviles - UMTS) se refiere a una red de comunicaciones que incluye estaciones base, o nodos B, y por ejemplo radio network controllers (controladores de red de radio - RNC). UTRAN permite la conectividad entre el user equipment (equipo de usuario - UE) y la red principal. El RNC proporciona funcionalidades de control para uno o más nodos B. El RNC y sus correspondientes nodos B se denominan Radio Network Subsystem (subsistema de red de radio - RNS). En el caso de E-UTRAN (UTRAN mejorada), no existe ningún RNC y se proporciona una funcionalidad de acceso de radio por un Nodo B evolucionado (eNodoB o eNB) o muchos eNB. Múltiples eNB están implicados para una sola conexión de UE, por ejemplo, en el caso de Coordinated Multipoint Transmission (transmisión multipunto coordinada - CoMP) y en la conectividad dual.

Long Term Evolution (Evolución a largo plazo - LTE) o E-UTRAN se refiere a las mejoras del UMTS a través de una eficiencia y unos servicios mejorados, costes más bajos y uso de nuevas oportunidades de espectro. En particular, LTE es un estándar 3GPP que proporciona tasas pico de enlace ascendente de al menos, por ejemplo, 75 megabits por segundo (Mbps) por portadora y tasas pico de enlace descendente de al menos, por ejemplo, 300 Mbps por portadora. LTE soporta anchos de banda de portadora ajustables a escala desde 20 MHz hasta 1,4 MHz y soporta tanto Frequency Division Duplexing (duplexación por división de frecuencia - FDD) como Time Division Duplexing (duplexación por división de tiempo - TDD).

Como se mencionó anteriormente, LTE también puede mejorar la eficiencia espectral en las redes, permitiendo que las portadoras proporcionen más servicios de datos y voz a través de un ancho de banda dado. Por lo tanto, LTE está diseñada para satisfacer las necesidades de transporte de datos y medios a alta velocidad además del soporte de voz de alta capacidad. Las ventajas de LTE incluyen, por ejemplo, alto rendimiento, baja latencia, soporte de FDD y TDD en la misma plataforma, una experiencia de usuario final mejorada y una arquitectura sencilla que da como resultado costes operativos bajos.

Ciertas versiones de LTE de 3GPP (por ejemplo, LTE Ver-10, LTE Ver-11, LTE Ver-12, LTE Ver-13) se refieren a sistemas international mobile telecommunications advanced (avanzados de telecomunicaciones móviles internacionales - IMT-A), denominados en el presente documento por conveniencia simplemente LTE avanzada (LTE-A).

LTE-A se refiere a extender y optimizar las tecnologías de acceso de radio de LTE de 3GPP. Un objetivo de LTE-A es proporcionar servicios significativamente mejorados por medio de mayores tasas de transmisión datos y menor latencia con coste reducido. LTE-A es un sistema de radio más optimizado que cumple los requisitos de la international telecommunication union-radio (unión de internacional telecomunicaciones, sector de radiocomunicaciones - ITU-R) para IMT-avanzado mientras se mantiene la retrocompatibilidad. Una de las características clave de LTE-A, introducida en LTE Ver-10, es la agregación de portadoras, lo que permite aumentar las tasas de transmisión de datos a través de la agregación de dos o más portadoras de LTE.

Los sistemas inalámbricos de 5ª generación (5G) se refieren a la próxima generación de sistemas de radio y a la arquitectura de red. Se espera que 5G proporcione tasas de bits y cobertura más altas que los sistemas de LTE actuales. Algunos estiman que 5G proporcionará tasas de bits cien veces más altas que las ofertas de LTE. También se espera que 5G aumente la capacidad de expansión de la red hasta cientos de miles de conexiones. Se prevé que la tecnología de señal de 5G se mejorará para mayor cobertura, así como para una mayor eficiencia espectral y de señalización. La publicación de 3GPP de Technical Specification Group Services and System Aspects con el título "Study on the security aspects of the next generation system (versión 14)", TR 33.899, V0.4.0 es una técnica anterior adicional.

Sumario:

La invención se define por las reivindicaciones anexas. Una realización se refiere a un método, que puede incluir pedir, por un nodo de red, la autenticación de un equipo de usuario con un servidor de autenticación, recibir una clave maestra y parámetros de autenticación desde el servidor de autenticación cuando la autorización es satisfactoria y verificar la validez de la petición de autenticación. El método también puede incluir, cuando la verificación es satisfactoria, instanciar un contexto de seguridad para el equipo de usuario y asignar un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario, y enviar un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie un contexto de seguridad usando el identificador de contexto de seguridad.

Según una realización, el nodo de red puede comprender una función de red de control común o función de anclaje de seguridad de un sistema de comunicación de next generation (próxima generación - NG).

En una realización, el identificador de contexto de seguridad puede comprender un next generation key set identifier (identificador de conjunto de claves de próxima generación - NG-KSI). De acuerdo con ciertas realizaciones, el identificador de conjunto de claves de próxima generación (NG-KSI) puede comprender un parámetro que está asociado con la clave maestra derivada durante el protocolo de acuerdo de autenticación y clave y un contexto de seguridad establecido basándose a la clave maestra.

En algunas realizaciones, el mensaje de comando de modo de seguridad adaptado para 5G comprende parámetros adicionales para asegurar la comunicación de non-access stratum (estrato de no acceso - NAS) (de próxima generación) entre el equipo de usuario y el nodo de red. De acuerdo con una realización, el método puede incluir además recibir un mensaje de aceptación desde el equipo de usuario que indica que el equipo de usuario ha instanciado un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de conjunto de claves de próxima generación (NG-KSI).

Otra realización se refiere a un aparato que incluye medios de petición para pedir la autenticación de un equipo de usuario con un servidor de autenticación, medios de recepción para recibir una clave maestra y parámetros/vectores de autenticación desde el servidor de autenticación cuando la autorización es satisfactoria, medios de verificación para verificar la validez de la petición de autenticación, cuando la verificación es satisfactoria, medios de instanciación para instanciar un contexto de seguridad para el equipo de usuario y asignar un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario, y medios de transmisión para enviar un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie un contexto de seguridad usando el identificador de contexto de seguridad.

De acuerdo con una realización, el aparato puede comprender una función de red de control común o función de anclaje de seguridad de un sistema de comunicación de próxima generación (NG).

En una realización, el identificador de contexto de seguridad puede comprender un identificador de conjunto de claves de próxima generación (NG-KSI). De acuerdo con ciertas realizaciones, el identificador de conjunto de claves de próxima generación (NG-KSI) puede comprender un parámetro que está asociado con la clave maestra derivada durante el protocolo de acuerdo de autenticación y clave y un contexto de seguridad establecido basándose a la clave maestra.

En algunas realizaciones, el mensaje de comando de modo de seguridad adaptado para 5G comprende parámetros adicionales para asegurar la comunicación de estrato de no acceso (NAS) (de próxima generación) entre el equipo de usuario y el nodo de red. De acuerdo con una realización, el aparato puede incluir además medios de recepción para recibir un mensaje de aceptación desde el equipo de usuario que indica que el equipo de usuario ha instanciado un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de conjunto de claves de próxima generación (NG-KSI).

Otra realización se refiere a un aparato que puede incluir al menos un procesador y al menos una memoria que comprende código de programa informático. La al menos una memoria y el código de programa informático están configurados, con el al menos un procesador, para hacer que el aparato al menos solicite la autenticación de un equipo de usuario con un servidor de autenticación, reciba una clave maestra y parámetros o vectores de autenticación del servidor de autenticación cuando la autorización es satisfactoria, verifique la validez de la petición de autenticación, cuando la verificación es satisfactoria, instancie un contexto de seguridad para el equipo de usuario y asigne un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario, y envíe un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie el contexto de seguridad usando el identificador de contexto de seguridad.

Otra realización se refiere a un método, que puede incluir después de la verificación de autenticación de un equipo de usuario, recibir un mensaje de comando de modo de seguridad desde un nodo de red. El mensaje de comando de modo de seguridad comprende instrucciones para instanciar un contexto de seguridad de estrato de no acceso (NAS) y comprende un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación. El método también puede incluir instanciar un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de contexto de seguridad como índice de seguridad.

De acuerdo con una realización, el nodo de red puede comprender una función de red de control común o función de anclaje de seguridad de un sistema de comunicación de próxima generación.

En una realización, el identificador de contexto de seguridad puede comprender un identificador de conjunto de claves de próxima generación (NG-KSI). De acuerdo con ciertas realizaciones, el identificador de conjunto de claves de próxima generación (NG-KSI) puede comprender un valor de índice asignado y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de próxima generación es un contexto de seguridad de próxima generación nativo derivado de la autenticación de próxima generación del equipo de usuario o un contexto de seguridad de próxima generación mapeado derivado de una autenticación que no es de próxima generación del equipo de usuario.

De acuerdo con una realización, el mensaje de comando de modo de seguridad comprende parámetros adicionales para asegurar la comunicación de estrato de no acceso (NAS) (de próxima generación) entre el equipo de usuario y el nodo de red. En una realización, el método puede incluir además enviar un mensaje de aceptación al nodo de red que indica que el equipo de usuario ha instanciado un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de conjunto de claves de próxima generación (NG-KSI).

Otra realización se refiere a un aparato que incluye, después de la verificación de autenticación del aparato, medios de recepción para recibir un mensaje de comando de modo de seguridad desde un nodo de red. El mensaje de comando de modo de seguridad comprende instrucciones para instanciar un contexto de seguridad de estrato de no acceso (NAS) y comprende un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación. El aparato también puede incluir medios de instanciación para instanciar un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de contexto de seguridad como índice de seguridad.

En ciertas realizaciones, el aparato puede ser un equipo de usuario. Según una realización, el nodo de red puede comprender una función de red de control común o función de anclaje de seguridad de un sistema de comunicación de próxima generación.

En una realización, el identificador de contexto de seguridad puede comprender un identificador de conjunto de claves de próxima generación (NG-KSI). De acuerdo con una realización, el identificador de conjunto de claves de próxima generación (NG-KSI) puede comprender un valor de índice asignado y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de próxima generación es un contexto de seguridad de próxima generación nativo derivado de la autenticación de próxima generación del aparato o un contexto de seguridad de próxima generación mapeado derivado de una autenticación que no es de próxima generación del aparato.

De acuerdo con ciertas realizaciones, el mensaje de comando de modo de seguridad puede comprender parámetros adicionales para asegurar la comunicación de estrato de no acceso (NAS) entre el aparato y el nodo de red. En una realización, el aparato puede incluir además medios de transmisión para enviar un mensaje de aceptación al nodo de red que indica que el aparato ha instanciado un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de conjunto de claves de próxima generación (NG-KSI).

Otra realización se refiere a un aparato que comprende al menos un procesador y al menos una memoria que incluye código de programa informático. La al menos una memoria y el código de programa informático están configurados, con el al menos un procesador, para hacer que el aparato al menos reciba, después de la verificación de autenticación del aparato, un mensaje de comando de modo de seguridad desde un nodo de red. El mensaje de comando de modo de seguridad comprende instrucciones para instanciar un contexto de seguridad de estrato de no acceso (NAS) y comprende un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación. La al menos una memoria y el código de programa informático están configurados además, con el al menos un procesador, para hacer que el aparato al menos instancie un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de contexto de seguridad como índice de seguridad.

Breve descripción de los dibujos:

Para un entendimiento apropiado de la invención, debería hacerse referencia a los dibujos adjuntos, en donde:

la Fig. 1 ilustra un diagrama de bloques de un sistema, según una realización;

la Fig. 2 ilustra un diagrama de flujo de señalización, según una realización;

la Fig. 3 ilustra un ejemplo de una estructura de un identificador de contexto de seguridad, según una realización;

la Fig. 4a ilustra un diagrama de bloques de un aparato, según una realización;

la Fig. 4b ilustra un diagrama de bloques de un aparato, según otra realización;

la Fig. 5a ilustra un diagrama de flujo de un método, según una realización; y

la Fig. 5b ilustra un diagrama de flujo de un método, según otra realización.

Descripción detallada:

Se entenderá fácilmente que los componentes de la invención, como se describe e ilustra de manera general en las figuras en el presente documento, pueden disponerse y diseñarse en una amplia variedad de configuraciones diferentes. Por lo tanto, no se pretende que la siguiente descripción detallada de realizaciones de sistemas, métodos, aparatos y productos de programa informático dirigidos a identificador(es) de conjuntos de claves de próxima generación (por ejemplo, 5G), tal como se representa en las figuras adjuntas, limite el alcance de la invención, sino que es meramente representativa de algunas realizaciones seleccionadas de la invención.

Los rasgos distintivos, las estructuras o las características de la invención descrita a lo largo de esta memoria descriptiva pueden combinarse de cualquier manera adecuada en una o más realizaciones. Por ejemplo, el uso de las expresiones "ciertas realizaciones", "algunas realizaciones" u otro lenguaje similar, a lo largo de esta memoria descriptiva se refiere al hecho de que un rasgo distintivo, una estructura o una característica particular descrita en relación con la realización puede incluirse en al menos una realización de la presente invención. Por lo tanto, las apariciones de las expresiones "en ciertas realizaciones", "en algunas realizaciones", "en otras realizaciones" u otras expresiones similares, a lo largo de esta memoria descriptiva no se refieren necesariamente todas ellas al mismo grupo de realizaciones, y los rasgos, estructuras o características descritos pueden combinarse de cualquier manera adecuada en una o más realizaciones.

Adicionalmente, si se desea, las distintas funciones comentadas a continuación pueden llevarse a cabo en un orden distinto y/o de manera simultánea entre sí. Además, si se desea, una o más de las funciones descritas pueden ser opcionales o pueden combinarse. Como tal, debe considerarse que la siguiente descripción es meramente ilustrativa de los principios, enseñanzas y realizaciones de esta invención, y no supone ninguna limitación de la misma.

El sistema de 5G de próxima generación está diseñado y requerirá retrocompatibilidad con LTE y otros sistemas. Para este propósito, se necesita una identificación clara de los conjuntos de claves utilizados. Para gestionar y acceder al contexto de seguridad y a la jerarquía de claves en 5G y para identificar el contexto de seguridad de 5G y el punto de inicio de la derivación de claves, se necesitará un nuevo parámetro que esté asociado con una clave maestra derivada durante el protocolo de acuerdo de autenticación y clave 5G y el contexto de seguridad establecido basándose en esta clave en el sistema de 5G. Debe observarse que, como se describe en el presente documento, un sistema de próxima generación (NG) puede referirse a un sistema de 5G u otro sistema de comunicaciones de próxima generación (es decir, posterior a LTE).

El identificador de clave de evolved packet core (núcleo de paquete evolucionado - EPC) para K_{ASME} se denomina identificador de conjunto de claves eKSI que puede ser de tipo KSI_{ASME} o de tipo KSI_{SGSN}. El eKSI se almacena en el UE y la mobility management entity (entidad de gestión de movilidad - MME) junto con K_{ASME} y el unique temporary identifier (identificador temporal único global - GUTI), si está disponible.

Como se detalla adicionalmente en la technical specification (especificación técnica -TS) del 3GPP 33.401: "El identificador de conjunto de claves KSI_{ASME} es un parámetro asociado con la K_{ASME} derivada durante la autenticación EPS AKA. El identificador de conjunto de claves KSI_{ASME} se asigna por la MME y se envía con el mensaje de petición de autenticación a la estación móvil donde se almacena junto con la K_{ASME}. El propósito de KSI_{ASME} es hacer posible que el UE y la MME identifiquen una K_{ASME} nativa sin invocar el procedimiento de autenticación. Esto se usa para permitir la reutilización de la K_{ASME} durante las configuraciones de conexión posteriores. El identificador de conjunto de claves KSI_{SGSN} es un parámetro asociado con la K_{ASME} mapeada derivada de las claves de UMTS durante la movilidad inter-RAT, véanse las disposiciones 9 y 10 de la presente memoria descriptiva. El identificador de conjunto de claves KSI_{SGSN} se genera tanto en el UE como en la MME respectivamente cuando se deriva el K_{ASME} mapeada durante los procedimientos inactivos en E-UTRAN y durante el traspaso de GERAN/UTRAN a E-UTRAN. El KSI_{SGSN} se almacena junto con la K_{ASME} mapeada. El propósito del KSI_{SGSN} es hacer posible que el UE y la MME indiquen el uso de la K_{ASME} mapeada en procedimientos de movilidad inter-RAT.

Por lo tanto, como se mencionó anteriormente, para gestionar y acceder al contexto de seguridad y a la jerarquía de claves en 5G y para identificar el contexto de seguridad de 5G y el punto de inicio de la derivación de claves, se necesitará un nuevo parámetro que esté asociado con una clave maestra derivada durante el protocolo de acuerdo de autenticación y clave 5G y el contexto de seguridad establecido basándose en esta clave en el sistema de 5G.

Se espera que el sistema de 5G de próxima generación tenga un identificador de conjunto de claves para gestionar y acceder al contexto de seguridad y a la jerarquía de claves en 5G. El identificador de conjunto de claves debe estar protegido por integridad y confidencialidad mientras se transmite entre el NG-UE y el sistema de NG.

De acuerdo con una realización de la invención, se proporciona un identificador de conjunto de claves de próxima generación (NG-KSI) como un parámetro asociado con una clave maestra derivada durante un protocolo acuerdo de autenticación y clave y el contexto de seguridad establecido basándose en esta clave en el sistema de 5G. En una realización, a partir de la clave maestra, se puede derivar un conjunto de claves para asegurar la señalización del plano de control de estrato de no acceso (NAS), así como los datos del plano de usuario terminados directamente en la user plane gateway (puerta de enlace de plano de usuario - UPGW). Después de la autenticación satisfactoria del UE y la clave maestra (por ejemplo, similar a K_ASME), se pueden derivar claves para proteger el access stratum (estrato de acceso - AS). Dado que el sistema de 5G está diseñado para tener una estructura de autenticación unificada para soportar múltiples tecnologías de acceso tales como 5G (NR), LTE, acceso distinto de 3GPP fiable, acceso de 3GPP fiable, etc., las claves deben derivarse para soportar el acceso desde cualquiera de estas tecnologías de acceso.

La Fig. 1 ilustra un diagrama de bloques de un sistema de ejemplo que usa el conjunto de claves y el contexto de seguridad requerido en 5G, de acuerdo con una realización. Más específicamente, la Fig. 1 ilustra un ejemplo del contexto de seguridad de 5G en el UE 100 de próxima generación (NG-UE) y la common control network function (función 120 de red de control común - CCNF)/SCMF con el índice NG-KSI para soportar una gestión unificada del contexto de seguridad y autenticación de UE a través de múltiples tecnologías de acceso. En el ejemplo de la Fig. 1, NG-UE 100 puede ser capaz de comunicarse con uno o más de un gNB 110, un eNB 111, WLAN/ePDG 112 y/o WLAN 113. La CCNF/SCMF 120 puede estar en comunicación con o acoplada a AAA/HSS 130. La Security Context Management Function (función de gestión de contexto seguridad - SCMF) se refiere a un elemento en la red central que, tras la autenticación de UE satisfactoria, puede mantener un contexto de seguridad de autenticación a partir del cual se derivarán los contextos de seguridad para la funcionalidad específica según corresponda para la CN y la AN específica.

De acuerdo con una realización, el identificador de conjunto de claves (NG-KSI) puede almacenarse en la entidad de red dedicada iniciando la authentication and key agreement (autenticación y el acuerdo de claves - AKA) en 5G. Por ejemplo, el identificador de conjunto de claves (NG-KSI) puede almacenarse en la CCNF o en una entidad de mobility management function (función de gestión de movilidad - MMF). Al final de la autenticación y verificación satisfactorias del UE, la CCNF puede asignar y enviar el NG-KSI al UE, indicándole que comience un contexto de NAS con el índice NG-KSI.

Debe observarse que, aunque ciertas realizaciones son aplicables a sistemas de 5G, algunas realizaciones descritas en el presente documento pueden referirse a elementos y protocolos de red que usan terminología 4G/LTE. Esto se debe a que aún no se ha fijado la terminología de 5G. Por lo tanto, las realizaciones de la invención pueden ser aplicables a elementos de red o protocolos con nombres o terminología diferentes de los utilizados en el presente documento.

La Fig. 2 ilustra un ejemplo de un diagrama de flujo de señalización que representa un ejemplo de un proceso, según una realización. Más específicamente, la Fig. 2 representa un proceso de instanciación de contexto de autenticación y seguridad de UE con asignación de NG-KSI, según una realización. Como se ilustra en la Fig. 2, en la etapa 1, el UE 200 de próxima generación transmite una petición de conexión al sistema de NG, por ejemplo, a un gNB, eNB, WLAN 211. La petición de conexión puede realizarse a través de cualquiera de las tecnologías de acceso de radio soportadas en el sistema de 5G. En la etapa 2, la función 220 de red de control común (CCNF) o la Security Anchor Function (función de anclaje de seguridad - SEAF) pide la autenticación de UE con una autenticación, authorization and accounting (autorización y contabilidad - AAA) o un home subscriber server (servidor 230 de abonado local - HSS) y pide vectores de clave maestra y de autenticación. Si la autenticación es satisfactoria, entonces las claves se reciben en la CCNF/SEAF 220.

Continuando con la Fig. 2, en la etapa 3, si la verificación de autenticación ha sido satisfactoria por parte de la CCNF/SEAF 220, entonces, en la etapa 4, la CCNF/SEAF 220 instancia un contexto de seguridad para el UE 200. En una realización, la CCNF/SEAF 220 asigna un identificador de contexto de seguridad, NG-KSI, para el contexto de seguridad del sistema de NG. El NG-KSI ayuda al UE 200 y al sistema de NG (por ejemplo, los nodos 211 de red) a identificar correctamente el contexto de seguridad durante los eventos de movilidad. En la etapa 5, la CCNF/SEAF 220 envía un mensaje de comando de modo de seguridad de NAS para indicar al UE 200 (por ejemplo, un NG-UE) que instancie el contexto de seguridad de NAS (por ejemplo, un contexto de seguridad de NAS) y el NG-KSI. El mensaje de comando de modo de seguridad puede contener parámetros adicionales para asegurar la comunicación de NAS entre el UE 200 y la CCNF/SEAF 220, tales como algoritmos seleccionados, contadores de NAS, etc. En la etapa 6, cuando el UE 200 recibe el comando de modo de seguridad de NAS, el UE 200 instancia el contexto de seguridad de NAS con NG-KSI como índice. A continuación, en la etapa 7, el UE 200 envía un mensaje de aceptación de comando de modo de seguridad de NAS para transmitir a la CCNF/SEAF 220 que ha instanciado el contexto de seguridad de NAS.

De acuerdo con ciertas realizaciones, el NG-KSI permite que el UE y la CCNF/MMF identifiquen el contexto de seguridad y la clave maestra correcta. Si se usa dicho parámetro, entonces el UE y la entidad de red dedicada que almacena el NG-KSI no necesitan invocar el procedimiento de autenticación durante una configuración posterior de la conexión durante eventos de movilidad desde el sistema de LTE al de NG o cuando se cambia una conexión de una tecnología de acceso a otra dentro del sistema de 5G.

El NG-KSI puede comprender un valor y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de NG es un contexto de seguridad de NG nativa derivado de la autenticación de NG del UE o un contexto de seguridad de NG mapeado derivado de LTE (u otra tecnología de acceso de radio no de NG) del UE. La Fig. 3 ilustra una estructura de ejemplo de un NG-KSI, según una realización; Como se ilustra en la Fig. 3, un NG-KSI puede incluir al menos dos campos: un tipo como el campo de NG-KSI y un valor asignado del campo índice.

Para propósitos de interfuncionamiento, el UE y la CCNF/MMF necesitan una zona de almacenamiento para varios identificadores de conjunto de claves en sus sistemas distinguidos. De acuerdo con una realización, están vinculados a NG-KSI, por ejemplo, eKSI (4G), por UE y CCNF/MMF como se muestra en la Fig. 1 comentada anteriormente. De acuerdo con una realización, el NG-KSI es una parte de nuevos mensajes de seguridad intercambiados entre el sistema de 5G o NG y un UE de NG.

La Fig. 4a ilustra un ejemplo de un aparato 10 según una realización. En una realización, el aparato 10 puede ser un nodo, anfitrión o servidor en una red de comunicaciones o que da servicio a una red de este tipo. Por ejemplo, el aparato 10 puede ser una estación base, un nodo B evolucionado, un punto de acceso WLAN, un servidor de abono (por ejemplo, HSS), un servidor de autenticación (por ejemplo, AAA), CCNF, SCMF o SEAF asociado con una red de acceso de radio, tal como una red de LTE o tecnología de acceso de radio 5G. Debe observarse que un experto en la técnica entenderá que el aparato 10 puede incluir componentes o características no mostrados en la Fig. 4a.

Como se ilustra en la Fig. 4a, el aparato 10 puede incluir un procesador 12 para procesar información y ejecutar instrucciones u operaciones. El procesador 12 puede ser cualquier tipo de procesador de propósito general o específico. Aunque en la Fig. 4a se muestra un único procesador 12, pueden usarse múltiples procesadores según otras realizaciones. De hecho, el procesador 12 puede incluir uno o más de ordenadores de propósito general, ordenadores de propósito especial, microprocesadores, digital signal processors (procesadores de señales digitales -DSP), field programmable gate array (matrices de puertas programables en el campo - FPGA), application-specific integrated circuits (circuitos integrados de aplicación específica - ASIC) y procesadores basados en una arquitectura de procesador de múltiples núcleos, como ejemplos.

El procesador 12 puede realizar funciones asociadas con el funcionamiento del aparato 10, que pueden incluir, por ejemplo, la precodificación de parámetros de ganancia/fase de antena, codificación y decodificación de bits individuales que forman un mensaje de comunicación, formateo de información y control global del aparato 10, incluyendo procedimientos relacionados con la gestión de recursos de comunicación.

El aparato 10 puede incluir además, o estar acoplado a, una memoria 14 (interna o externa), que puede estar acoplada al procesador 12, para almacenar información e instrucciones que pueden ejecutarse por el procesador 12. La memoria 14 puede ser una o más memorias de cualquier tipo adecuado para el entorno de aplicación local y puede implementarse usando cualquier tecnología de almacenamiento de datos volátil o no volátil adecuada, tal como dispositivo de memoria basado en semiconductores, un sistema y dispositivo de memoria magnético, un sistema y dispositivo de memoria óptico, memoria fija y memoria extraíble. Por ejemplo, la memoria 14 puede comprender cualquier combinación de random access memory (memoria de acceso aleatorio - RAM), read only memory (memoria de sólo lectura - ROM), almacenamiento estático tal como un disco magnético u óptico, o cualquier otro tipo de medios legibles por ordenador o máquina no transitorios. Las instrucciones almacenadas en la memoria 14 pueden incluir instrucciones de programa o código de programa informático que, cuando se ejecutan por el procesador 12, permiten que el aparato 10 realice tareas como se describe en el presente documento.

En algunas realizaciones, el aparato 10 también puede incluir o estar acoplado a una o más antenas 15 para transmitir y recibir señales y/o datos a y desde el aparato 10. El aparato 10 puede incluir además, o estar acoplado a, un transceptor 18 configurado para transmitir y recibir información. El transceptor 18 puede incluir, por ejemplo, una pluralidad de interfaces de radio que pueden estar acopladas a la(s) antena(s) 15. Las interfaces de radio pueden corresponder a una pluralidad de tecnologías de acceso de radio que incluyen una o más de LTE, 5G, WLAN, Bluetooth, BT-LE, NFC, radio frequency identifier (identificador de radiofrecuencia - RFID), ultrawideband (banda ultraancha - UWB) y similares. La interfaz de radio puede incluir componentes, tales como filtros, convertidores (por ejemplo, convertidores de digital a analógico y similares), mapeadores, un módulo de Fast Fourier Transform (transformada rápida de Fourier - FFT) y similares, para generar símbolos para una transmisión a través de uno o más enlaces descendentes y para recibir símbolos (por ejemplo, a través de un enlace ascendente). Por ejemplo, el transceptor 18 puede estar configurado para modular información sobre una forma de onda portadora para la transmisión por la(s) antena(s) 15 y demodular información recibida a través de la(s) antena(s) 15 para su procesamiento adicional por otros elementos del aparato 10. En otras realizaciones, el transceptor 18 puede ser capaz de transmitir y recibir señales o datos directamente.

En una realización, la memoria 14 puede almacenar módulos de software que proporcionan funcionalidad cuando se ejecutan por el procesador 12. Los módulos pueden incluir, por ejemplo, un sistema operativo que proporciona funcionalidad de sistema operativo para el aparato 10. La memoria también puede almacenar uno o más módulos funcionales, tales como una aplicación o programa, para proporcionar una funcionalidad adicional para el aparato 10. Los componentes del aparato 10 pueden implementarse en hardware, o como cualquier combinación adecuada de hardware y software.

En una realización, el aparato 10 puede ser un nodo o servidor de red de próxima generación (por ejemplo, 5G), tal como una CCNF o SEAF, por ejemplo. Según una realización, el aparato 10 puede controlarse por la memoria 14 y el procesador 12 para pedir la autenticación de un equipo de usuario con un servidor de autenticación o abono (por ejemplo, AAA o HSS). En una realización, cuando la autenticación es satisfactoria, el aparato 10 puede controlarse adicionalmente por la memoria 14 y el procesador 12 para recibir una clave maestra y parámetros o vectores de autenticación desde el servidor de autenticación/abono. El aparato 10 puede controlarse entonces por la memoria 14 y el procesador 12 para verificar la validez de la petición de autenticación y/o verificar la validez de los parámetros de equipo de usuario y de autenticación. Por ejemplo, la validez de la petición de autenticación puede verificarse utilizando los parámetros de autenticación recibidos para autenticar el equipo de usuario para el servicio en un sistema de comunicaciones de próxima generación. Si la verificación es satisfactoria, el aparato 10 puede controlarse por la memoria 14 y el procesador 12 para instanciar un contexto de seguridad para el equipo de usuario y asignar un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario. En una realización, el identificador de contexto de seguridad asignado es un NG-KSI. El aparato 10 puede controlarse entonces por la memoria 14 y el procesador 12 para enviar un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie un contexto de seguridad utilizando el identificador de contexto de seguridad (por ejemplo, NG-KSI).

En una realización, el NG-KSI puede incluir un parámetro asociado con la clave maestra derivada durante el protocolo de acuerdo de autenticación y clave y un contexto de seguridad establecido basándose en la clave maestra. De acuerdo con ciertas realizaciones, el NG-KSI puede incluir un valor y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de próxima generación es un contexto de seguridad de próxima generación nativo derivado de la autenticación de próxima generación del equipo de usuario o un contexto de seguridad de próxima generación mapeado derivado de una autenticación que no es de próxima generación (por ejemplo, LTE) del equipo de usuario.

De acuerdo con algunas realizaciones, el mensaje de comando de modo de seguridad enviado al equipo de usuario puede incluir, además del NG-KSI, otros parámetros para asegurar la comunicación de NAS (por ejemplo, NG-NAS) entre el equipo de usuario y el aparato 10. En una realización, el aparato 10 puede controlarse por la memoria 14 y el procesador 12 para recibir un mensaje de aceptación desde el equipo de usuario que indica que el equipo de usuario ha instanciado un contexto de seguridad de NAS usando el NG-KSI.

La Fig. 4b ilustra un ejemplo de un aparato 20 según otra realización. En una realización, el aparato 20 puede ser un nodo o elemento en una red de comunicaciones o asociado con una red de este tipo, tal como un UE, mobile equipment (equipo móvil - ME), dispositivo móvil, dispositivo estacionario u otro dispositivo. Como se describe en el presente documento, el UE puede denominarse alternativamente, por ejemplo, estación móvil, equipo móvil, unidad móvil, dispositivo móvil, dispositivo de usuario, estación de abonado, terminal inalámbrico, ordenador de tipo tableta, teléfono inteligente o similar. El aparato 20 puede implementarse, por ejemplo, en un dispositivo portátil inalámbrico, un accesorio de complemento inalámbrico o similar.

En algunas realizaciones, el aparato 20 puede incluir uno o más procesadores, uno o más medios de almacenamiento legibles por ordenador (por ejemplo, memoria, almacenamiento y similares), uno o más componentes de acceso de radio (por ejemplo, un módem, un transceptor y similares) y/o una interfaz de usuario. En algunas realizaciones, el aparato 20 puede configurarse para funcionar usando una o más tecnologías de acceso de radio, tales como LTE, LTE-A, 5G, WLAN, WiFi, Bluetooth y cualquier otra tecnología de acceso de radio. Debe observarse que un experto en la técnica entenderá que el aparato 20 puede incluir componentes o características no mostrados en la Fig. 4b.

Como se ilustra en la Fig. 4b, el aparato 20 puede incluir, o estar acoplado a, un procesador 22 para procesar información y ejecutar instrucciones u operaciones. El procesador 22 puede ser cualquier tipo de procesador de propósito general o específico. Aunque en la Fig. 4b se muestra un único procesador 22, pueden usarse múltiples procesadores según otras realizaciones. De hecho, el procesador 22 puede incluir uno o más de ordenadores de propósito general, ordenadores de propósito especial, microprocesadores, digital signal processors (procesadores de señales digitales - DSP), field programmable gate array (matrices de puertas programables en campo - FPGA), application-specific integrated circuits (circuitos integrados de aplicación específica - ASIC) y procesadores basados en una arquitectura de procesador de múltiples núcleos, como ejemplos.

El procesador 22 puede realizar funciones asociadas con el funcionamiento del aparato 20 que incluyen, sin limitación, precodificación de parámetros de ganancia/fase de antena, codificación y decodificación de bits

individuales que forman un mensaje de comunicación, formateo de información y control global del aparato 20, incluyendo procesos relacionados con la gestión de recursos de comunicación.

El aparato 20 puede incluir además, o estar acoplado a, una memoria 24 (interna o externa), que puede estar acoplada al procesador 22, para almacenar información e instrucciones que pueden ejecutarse por el procesador 22. La memoria 24 puede ser una o más memorias de cualquier tipo adecuado para el entorno de aplicación local y puede implementarse usando cualquier tecnología de almacenamiento de datos volátil o no volátil adecuada, tal como un dispositivo de memoria basado en semiconductores, un sistema y dispositivo de memoria magnética, un sistema y dispositivo de memoria óptica, memoria fija y memoria extraíble. Por ejemplo, la memoria 24 puede comprender cualquier combinación de random access memory (memoria de acceso aleatorio - RAM), read only memory (memoria de solo lectura - ROM), almacenamiento estático tal como un disco magnético u óptico, o cualquier otro tipo de medios legibles por ordenador o máquina no transitorios. Las instrucciones almacenadas en la memoria 24 pueden incluir instrucciones de programa o código de programa informático que, cuando se ejecutan por el procesador 22, permiten que el aparato 20 realice tareas como se describe en el presente documento.

En algunas realizaciones, el aparato 20 también puede incluir o estar acoplado a una o más antenas 25 para recibir un enlace descendente o una señal y para transmitir a través de un enlace ascendente desde el aparato 20. El aparato 20 puede incluir además un transceptor 28 configurado para transmitir y recibir información. El transceptor 28 también puede incluir una interfaz de radio (por ejemplo, un módem) acoplada a la antena 25. La interfaz de radio puede corresponder a una pluralidad de tecnologías de acceso de radio que incluyen una o más de LTE, LTE-A, 5G, WLAN, Bluetooth, BT-LE, NFC, RFID, UWB y similares. La interfaz de radio puede incluir otros componentes, tales como filtros, convertidores (por ejemplo, convertidores de digital a analógico y similares), desmapadores de símbolos, componentes de conformación de señal, un módulo de Inverse Fast Fourier Transform (transformada rápida de Fourier inversa - IFFT) y similares, para procesar símbolos, tales como símbolos OFDMA, transportados por un enlace descendente o un enlace ascendente.

Por ejemplo, el transceptor 28 puede estar configurado para modular información sobre una forma de onda portadora para la transmisión por la(s) antena(s) 25 y demodular información recibida a través de la(s) antena(s) 25 para su procesamiento adicional por otros elementos del aparato 20. En otras realizaciones, el transceptor 28 puede ser capaz de transmitir y recibir señales o datos directamente. El aparato 20 puede incluir además una interfaz de usuario, tal como una interfaz gráfica de usuario o pantalla táctil.

En una realización, la memoria 24 almacena módulos de software que proporcionan funcionalidad cuando se ejecutan por el procesador 22. Los módulos pueden incluir, por ejemplo, un sistema operativo que proporciona funcionalidad de sistema operativo para el aparato 20. La memoria también puede almacenar uno o más módulos funcionales, tales como una aplicación o programa, para proporcionar una funcionalidad adicional para el aparato 20. Los componentes del aparato 20 pueden implementarse en hardware, o como cualquier combinación adecuada de hardware y software.

De acuerdo con una realización, el aparato 20 puede ser un dispositivo móvil, UE o ME, por ejemplo. En esta realización, el aparato 20 puede controlarse por la memoria 24 y el procesador 22 para realizar las funciones asociadas con las realizaciones descritas en el presente documento. En una realización, el aparato 20 puede controlarse por la memoria 24 y el procesador 22 para realizar o transmitir un mensaje de petición de conexión a un nodo de red (NG/5G). Después de la verificación de autenticación del aparato 20 por el nodo de red, el aparato 20 puede controlarse por la memoria 24 y el procesador 22 para recibir un mensaje de comando de modo de seguridad desde el nodo de red (por ejemplo, CCNF/SEAF). El mensaje de comando de modo de seguridad puede incluir instrucciones para instanciar un contexto de seguridad de NAS (por ejemplo, un contexto de seguridad de NG-NAS) y también puede incluir un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación. En una realización, el identificador de contexto de seguridad es un NG-KSI.

El aparato 20 puede controlarse entonces por la memoria 24 y el procesador 22 para instanciar el contexto de seguridad de NAS (por ejemplo, un contexto de seguridad de NG-NAS) usando el identificador de contexto de seguridad como índice de seguridad. El mensaje de comando de modo de seguridad también puede incluir parámetros adicionales para asegurar la comunicación de NAS entre el aparato 20 y el nodo de red.

De acuerdo con una realización, el NG-KSI incluye un valor y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de próxima generación es un contexto de seguridad de próxima generación nativo derivado de la autenticación de próxima generación del aparato 20 o un contexto de seguridad de próxima generación mapeado derivado de una autenticación de próxima generación (por ejemplo, LTE) del aparato 20.

En una realización, el aparato 20 puede controlarse adicionalmente por la memoria 24 y el procesador 22 para enviar un mensaje de aceptación al nodo de red que indica que el aparato 20 ha instanciado un contexto de seguridad de NAS usando el NG-KSI.

La Fig. 5a ilustra un diagrama de flujo de un método, según una realización; En ciertas realizaciones, el método de la Fig. 5a puede realizarse por un nodo de acceso o nodo de control de un sistema de comunicación de próxima

generación o 5G. Por ejemplo, en algunas realizaciones, el método de la Fig. 5a puede realizarse por una CCNF o una SEAF. Como se ilustra en la Fig. 5a, el método puede incluir, en 400, pedir la autenticación de un equipo de usuario con un servidor de autenticación o abono (por ejemplo, AAA o HSS). En una realización, cuando la autorización es satisfactoria, el método puede incluir, en 410, recibir una clave maestra y parámetros o vectores de autenticación desde el servidor de autenticación/abono.

El método de la Fig. 5a puede incluir entonces, en 420, verificar la validez de la petición de autenticación y/o verificar la validez del equipo de usuario y los parámetros de autenticación. Por ejemplo, la validez de la petición de autenticación puede verificarse utilizando los parámetros de autenticación recibidos para autenticar el equipo de usuario para el servicio en un sistema de comunicaciones de próxima generación.. Si la verificación es satisfactoria, el método puede incluir, en 430, instanciar un contexto de seguridad para el equipo de usuario y asignar un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario. En una realización, el identificador de contexto de seguridad asignado es un NG-KSI. El método puede incluir entonces, en 440, enviar un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie un contexto de seguridad utilizando el identificador de contexto de seguridad (por ejemplo, NG-KSI).

De acuerdo con algunas realizaciones, el envío del mensaje de comando de modo de seguridad al equipo de usuario puede incluir además enviar, además del NG-KSI, otros parámetros para asegurar la comunicación de NAS entre el equipo de usuario y el nodo de acceso/control del sistema de próxima generación. En una realización, el método también puede incluir recibir un mensaje de aceptación desde el equipo de usuario que indica que el equipo de usuario ha instanciado un contexto de seguridad de NAS usando el NG-KSI.

La Fig. 5b ilustra un diagrama de flujo de un método, según otra realización. En ciertas realizaciones, el método de la Fig. 5b puede realizarse por un dispositivo móvil, UE o ME, por ejemplo. Como se ilustra en la Fig. 5b, el método puede incluir, en 450, después de la verificación de autenticación del UE por la red, recibir un mensaje de comando de modo de seguridad desde un nodo de red (por ejemplo, CCNF/SEAF). El mensaje de comando de modo de seguridad puede incluir instrucciones para instanciar un contexto de seguridad de NAS y también puede incluir un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación. En una realización, el identificador de contexto de seguridad es un NG-KSI. El mensaje de comando de modo de seguridad también puede incluir parámetros adicionales para asegurar la comunicación de estrato de no acceso (NAS) entre el UE y la red.

En una realización, el método de la Fig. 5b puede incluir además, en 460, instanciar un contexto de seguridad de estrato de no acceso (NAS) usando el identificador de contexto de seguridad como índice de seguridad. De acuerdo con una realización, el método también puede incluir, en 470, enviar un mensaje de aceptación al nodo de red que indica que el UE ha instanciado un contexto de seguridad de NAS usando el NG-KSI.

Las realizaciones de la invención proporcionan varias ventajas y/o mejoras técnicas. Las realizaciones de la invención pueden mejorar el rendimiento y la seguridad de las redes de comunicaciones inalámbricas y sus nodos. Como resultado, el uso de las realizaciones de la invención da como resultado un funcionamiento mejorado de redes de comunicaciones y sus nodos.

En algunas realizaciones, la funcionalidad de cualquiera de los métodos, procedimientos, diagramas de señalización o diagramas de flujo descritos en el presente documento puede implementarse mediante software y/o código de programa informático o partes de código almacenados en la memoria u otros medios tangibles o legibles por ordenador, y ejecutarse por un procesador. En algunas realizaciones, el aparato puede incluirse en, o estar asociado con, al menos una aplicación, módulo, unidad o entidad de software configurado como operación/operaciones aritmética(s), o como un programa o partes del mismo (incluyendo una rutina de software añadida o actualizada), ejecutado por al menos un procesador de funcionamiento. Los programas, también denominados productos de programa o programas informáticos, incluyendo rutinas de software, miniaplicaciones y macros, pueden almacenarse en cualquier medio de almacenamiento de datos legible por aparatos e incluir instrucciones de programa para realizar tareas particulares. Un producto de programa informático puede comprender uno o más componentes ejecutables por ordenador que, cuando se ejecuta el programa, se configuran para llevar a cabo realizaciones. El uno o más componentes ejecutables por ordenador pueden ser al menos un código de software o porciones del mismo. Las modificaciones y configuraciones requeridas para implementar la funcionalidad de una realización pueden realizarse como rutina(s), que puede(n) implementarse como rutina(s) de software añadida(s) o actualizada(s). Se puede(n) descargar rutina(s) de software en el aparato.

Un software o un código de programa informático o partes del mismo pueden estar en forma de código fuente, en forma de código objeto o en alguna forma intermedia, y puede almacenarse en algún tipo de soporte, medio de distribución o medio legible por ordenador, que puede ser cualquier entidad o dispositivo que puede portar el programa. Tales soportes incluyen un medio de grabación, memoria informática, memoria de sólo lectura, señal de portadora fotoeléctrica y/o eléctrica, señal de telecomunicaciones y paquete de distribución de software, por ejemplo. Dependiendo de la potencia de procesamiento necesaria, el programa informático puede ejecutarse en un único ordenador digital electrónico o puede distribuirse entre varios ordenadores. El medio legible por ordenador o medio de almacenamiento legible por ordenador puede ser un medio no transitorio.

En otras realizaciones la funcionalidad puede realizarse mediante hardware, por ejemplo, mediante el uso de un application-specific integrated circuits (circuito integrado de aplicación específica - ASIC), una programmable gate array (matriz de puertas programables - PGA), una field programmable gate array (matriz de puertas programables en campo - FPGA) o cualquier otra combinación de hardware y software. En aún otra realización, la funcionalidad puede implementarse como una señal, un medio no tangible que puede ser portarse por una señal electromagnética descargada de Internet u otra red.

Según una realización, un aparato, tal como un nodo, dispositivo o componente correspondiente, puede estar configurado como un ordenador o un microprocesador, tal como un elemento informático de un solo chip, o como un conjunto de chips, que incluye al menos una memoria para proporcionar capacidad de almacenamiento usada para la operación aritmética y un procesador de funcionamiento para ejecutar la operación aritmética.

Un experto en la materia entenderá fácilmente que la invención como se ha analizado anteriormente puede ponerse en práctica con etapas en un orden diferente, y/o con elementos de hardware en configuraciones que son diferentes de las que se divulgan. Por lo tanto, aunque la invención se ha descrito basándose en estas realizaciones preferidas, a los expertos en la técnica les resultará evidente que son evidentes determinadas modificaciones, variaciones y construcciones alternativas aun permaneciendo dentro del alcance de la invención. Por lo tanto, para determinar las medidas y los límites de la invención, debe hacerse referencia a las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método, que comprende:

pedir, por un nodo de red, la autenticación de un equipo de usuario con un servidor de autenticación;
recibir una clave maestra y parámetros de autenticación desde el servidor de autenticación cuando la autenticación es satisfactoria;
verificar la validez de los parámetros de autenticación;
cuando la verificación es satisfactoria, instanciar un contexto de seguridad para el equipo de usuario y asignar un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario; y
enviar un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie un contexto de seguridad usando el identificador de contexto de seguridad.

2. El método según la reivindicación 1, en donde el mensaje de comando de modo de seguridad, preferiblemente adaptado para 5G, comprende parámetros adicionales para asegurar la comunicación de estrato de no acceso, NAS, entre el equipo de usuario y el nodo de red.

3. El método según la reivindicación 1, en donde el nodo de red comprende una función de red de control común o función de anclaje de seguridad de un sistema de comunicación de próxima generación.

4. Un aparato que comprende:

medios de petición para pedir la autenticación de un equipo de usuario con un servidor de autenticación;
medios de recepción para recibir una clave maestra y parámetros/vectores de autenticación desde el servidor de autenticación cuando la autenticación es satisfactoria;
medios de verificación para verificar la validez de los parámetros de autenticación;
cuando la verificación es satisfactoria, medios de instanciación para instanciar un contexto de seguridad para el equipo de usuario y medios de asignación para asignar un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al equipo de usuario; y
medios de transmisión para enviar un mensaje de comando de modo de seguridad para indicar al equipo de usuario que instancie un contexto de seguridad usando el identificador de contexto de seguridad.

5. El aparato según la reivindicación 4, en donde el identificador de contexto de seguridad comprende un identificador de conjunto de claves de próxima generación, NG-KSI.

6. El aparato según la reivindicación 5, en donde el identificador de conjunto de claves de próxima generación, NG-KSI, comprende un parámetro que está asociado con la clave maestra derivada durante el protocolo de acuerdo de autenticación y clave y un contexto de seguridad establecido basándose en la clave maestra.

7. El aparato según una cualquiera de las reivindicaciones 4-6, en donde el mensaje de comando de modo de seguridad comprende parámetros adicionales para asegurar la comunicación de estrato de no acceso, NAS, entre el equipo de usuario y el aparato.

8. El aparato según una cualquiera de las reivindicaciones 4-7, que comprende además medios de recepción para recibir un mensaje de aceptación desde el equipo de usuario que indica que el equipo de usuario ha instanciado un contexto de seguridad de estrato de no acceso, NAS, usando el identificador de conjunto de claves de próxima generación, NG-KSI.

9. El aparato según la reivindicación 4, en donde el aparato comprende una función de red de control común o función de anclaje de seguridad de un sistema de comunicación de próxima generación.

10. Un método, que comprende:

después de la verificación de autenticación de un equipo de usuario, recibir un mensaje de comando de modo de seguridad desde un nodo de red, en donde el mensaje de comando de modo de seguridad comprende parámetros para asegurar la comunicación de estrato de no acceso, NAS, entre el equipo de usuario y el nodo de red y comprende un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación; e
instanciar un contexto de seguridad de estrato de no acceso, NAS, usando el identificador de contexto de seguridad como un índice de seguridad, en donde el identificador de contexto de seguridad comprende un identificador de conjunto de claves de próxima generación, NG-KSI; y

en donde el identificador de conjunto de claves de próxima generación, NG-KSI comprende un valor de índice asignado y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de próxima generación es un contexto de seguridad de próxima generación nativo derivado de la autenticación de próxima generación del equipo de usuario o un contexto de seguridad de próxima generación mapeado derivado de una autenticación que no es de próxima generación del equipo de usuario.

11. El método según la reivindicación 10, que comprende además enviar un mensaje de aceptación al nodo de red que indica que el equipo de usuario ha instanciado un contexto de seguridad de estrato de no acceso, NAS, usando el identificador de conjunto de claves de próxima generación, NG-KSI.

12. Un aparato que comprende:

medios de recepción para recibir, después de la verificación de autenticación del aparato, un mensaje de comando de modo de seguridad desde un nodo de red, en donde el mensaje de comando de modo de seguridad comprende parámetros para asegurar una comunicación de estrato de no acceso, NAS, entre el aparato y el nodo de red y comprende un identificador de contexto de seguridad para el contexto de seguridad del sistema de próxima generación; y
medios de instanciación para instanciar un contexto de seguridad de estrato de no acceso, NAS. usando el identificador de contexto de seguridad como un índice de seguridad, en donde el identificador de contexto de seguridad comprende un identificador de conjunto de claves de próxima generación, NG-KSI; y
en donde el identificador de conjunto de claves de próxima generación, NG-KSI, comprende un valor de índice asignado y un tipo de parámetro de contexto de seguridad que indica si un contexto de seguridad de próxima generación es un contexto de seguridad de próxima generación nativo derivado de la autenticación de próxima generación del aparato o un contexto de seguridad de próxima generación mapeado derivado de una autenticación que no es de próxima generación del aparato.

13. El aparato según la reivindicación 12, que comprende además medios de transmisión para enviar un mensaje de aceptación al nodo de red que indica que el aparato ha instanciado un contexto de seguridad de estrato de no acceso, NAS, usando el identificador de conjunto de claves de próxima generación, NG-KSI.

14. El aparato según una cualquiera de las reivindicaciones 12-13, en donde el aparato comprende en un equipo de usuario.

15. Un programa informático, realizado en un medio legible por ordenador no transitorio, configurado el programa informático para controlar un procesador para realizar un método según una cualquiera de las reivindicaciones 1-3 o 10-11.

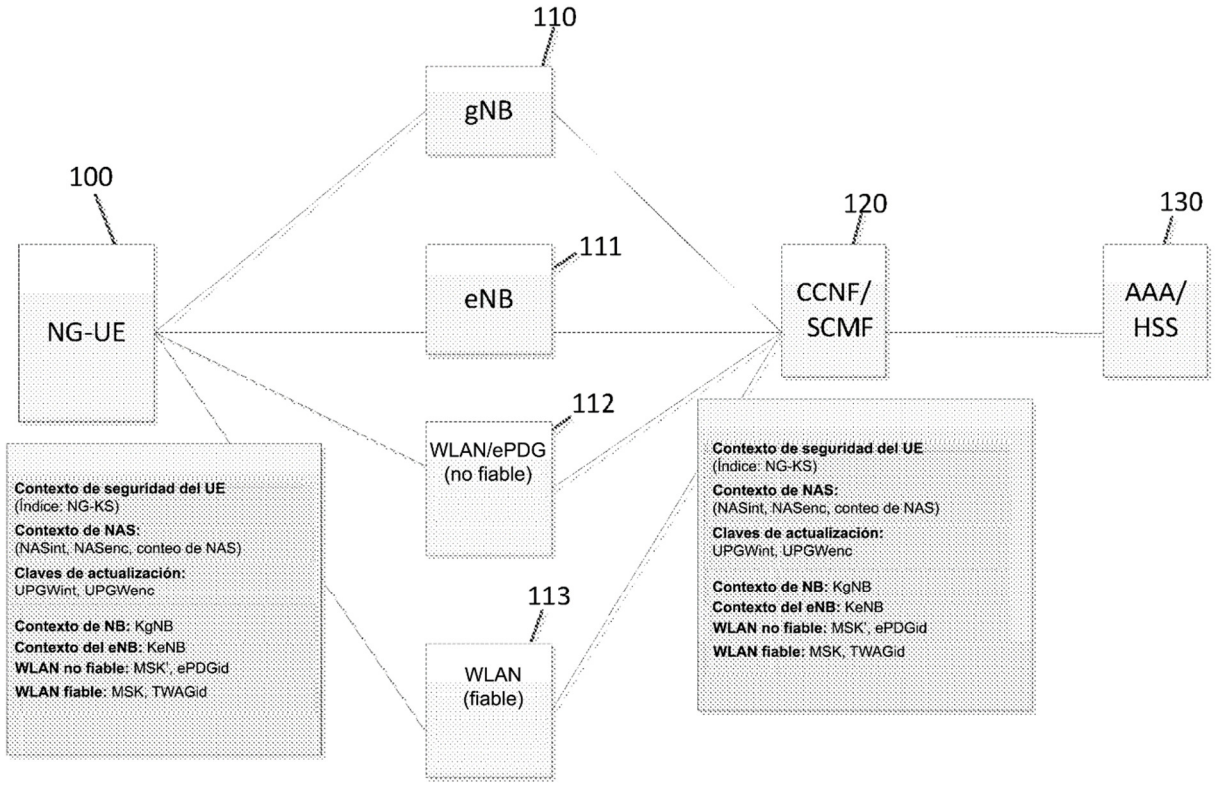

110
gNB
100
120
130
111
eNB
NG-UE
CCNF/
SCMF
AAA/
HSS
112
WLAN/ePDG
(no fiable)
Contexto de seguridad del UE
(Índice: NG-KS)
Contexto de NAS:
(NASint, NASenc, conteo de NAS)
Claves de actualización:
UPGWint, UPGWenc
Contexto de NB: KgNB
Contexto del eNB: KeNB
WLAN no fiable: MSK', ePDGid
WLAN fiable: MSK, TWAGid
113
WLAN
(fiable)
Contexto de seguridad del UE
(Índice: NG-KS)
Contexto de NAS:
(NASint, NASenc, conteo de NAS)
Claves de actualización:
UPGWint, UPGWenc
Contexto de NB: KgNB
Contexto del eNB: KeNB
WLAN no fiable: MSK', ePDGid
WLAN fiable: MSK, TWAGid

Fig. 1

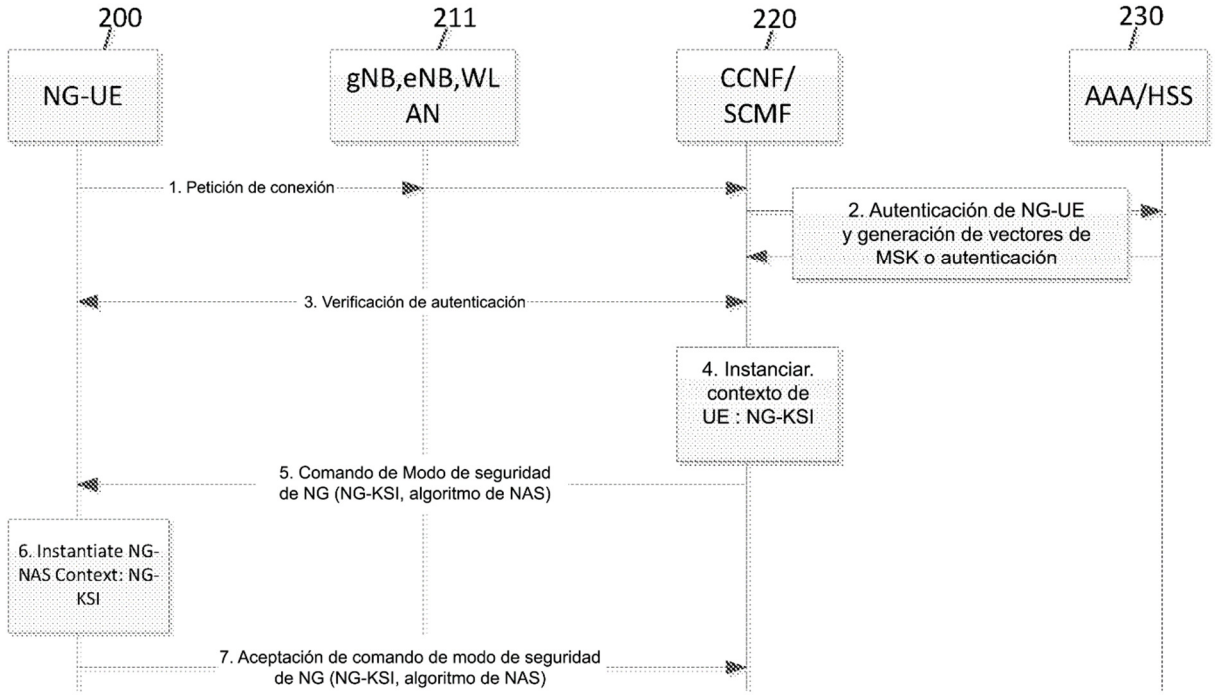

200
211
220
230
NG-UE
gNB,eNB,WLAN
CCNF/SCMF
AAA/HSS
1. Petición de conexión
2. Autenticación de NG-UE y generación de vectores de MSK o autenticación
3. Verificación de autenticación
4. Instanciar. contexto de UE : NG-KSI
5. Comando de Modo de seguridad de NG (NG-KSI, algoritmo de NAS)
6. Instantiate NG-NAS Context: NG-KSI
7. Aceptación de comando de modo de seguridad de NG (NG-KSI, algoritmo de NAS)

Fig. 2


Tipo
NG-KSI
Índice de conjunto de claves de valor asignado

Fig. 3

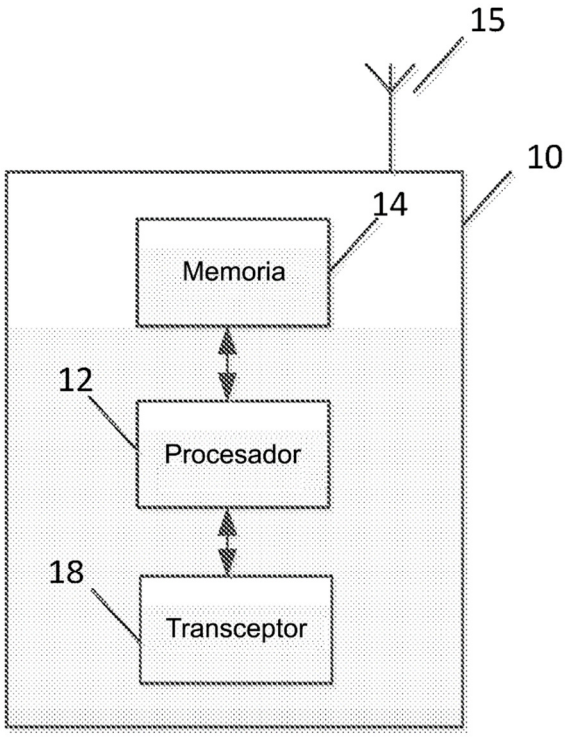

15
10
14
Memoria
12
Procesador
18
Transceptor

Fig. 4a

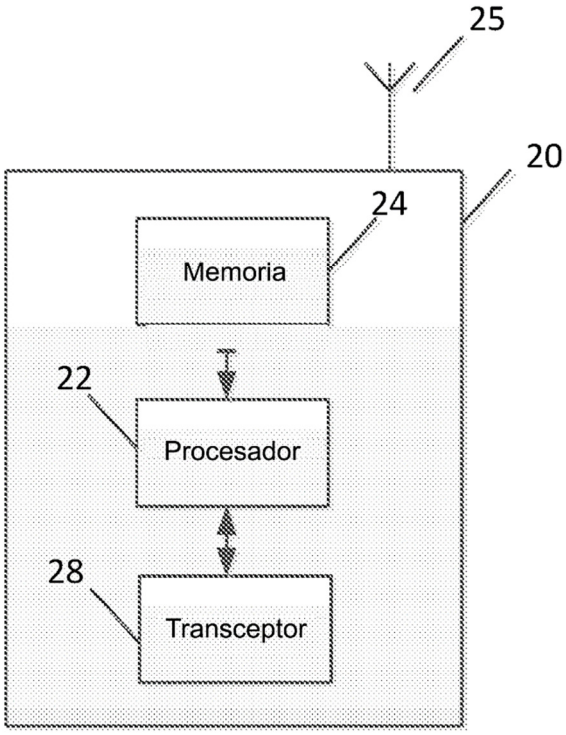

25
20
24
Memoria
22
Procesador
28
Transceptor

Fig. 4b

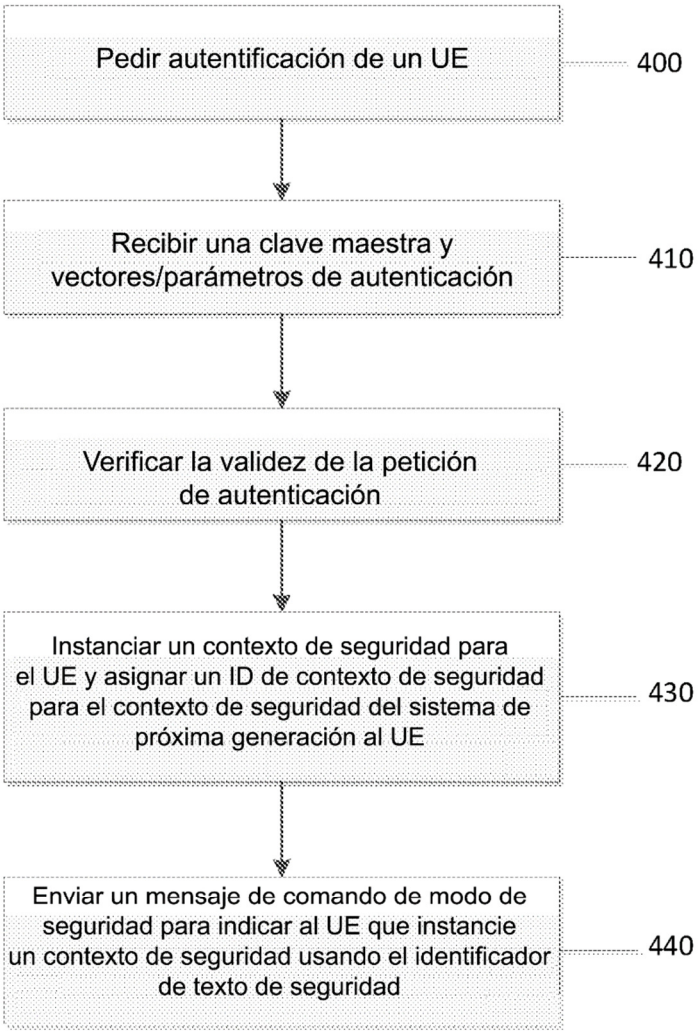

Pedir autentificación de un UE
400
Recibir una clave maestra y vectores/parámetros de autenticación
410
Verificar la validez de la petición de autenticación
420
Instanciar un contexto de seguridad para el UE y asignar un ID de contexto de seguridad para el contexto de seguridad del sistema de próxima generación al UE
430
Enviar un mensaje de comando de modo de seguridad para indicar al UE que instancie un contexto de seguridad usando el identificador de texto de seguridad
440

Fig. 5a

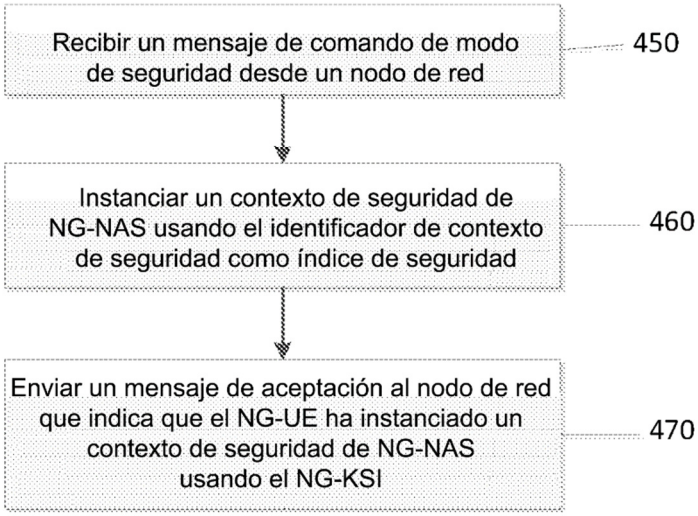

Recibir un mensaje de comando de modo de seguridad desde un nodo de red
450
Instanciar un contexto de seguridad de NG-NAS usando el identificador de contexto de seguridad como índice de seguridad
460
Enviar un mensaje de aceptación al nodo de red que indica que el NG-UE ha instanciado un contexto de seguridad de NG-NAS usando el NG-KSI
470

Fig. 5b