

SEGURIDAD EN UNA ARQUITECTURA DE TERMINACIONES DE NAS

DISTRIBUIDA

CAMPO TÉCNICO

5 Las realizaciones de la presente divulgación se refieren en general a la comunicación inalámbrica y, más particularmente, a métodos y aparatos para la seguridad en una arquitectura de terminaciones de NAS distribuida.

ANTECEDENTES

En la arquitectura de sistema de 5G, como se define en la TS 23.501 del
10 3GPP, una conexión de estrato sin acceso (NAS) para un equipo de usuario (UE) siempre se termina en la red de servicio en una única función de red (NF), por ejemplo, función de gestión de acceso y movilidad (AMF), como se muestra en la figura 1. La conexión de NAS se protege en cuanto a su integridad y confidencialidad por medio de un procedimiento de seguridad que se ejecuta
15 entre el UE y la NF que establece un contexto de seguridad de NAS que es mantenido tanto por el UE como por la NF durante la vida útil de la conexión de NAS. Este contexto de seguridad de NAS incluye, entre otros parámetros, las claves de seguridad y algoritmos usados para proteger la conexión de NAS.

En una arquitectura de terminaciones de NAS distribuida, por otro lado,
20 un UE puede tener múltiples conexiones de NAS que se terminan en la red de servicio en múltiples NF diferentes. Es decir, las conexiones de NAS se distribuyen entre diferentes NF dependiendo de los procedimientos de NAS que soportan las conexiones de NAS, como se muestra en la figura 2. Como un ejemplo, el UE puede tener dos conexiones de NAS terminadas en dos NF
25 diferentes, portando una conexión de NAS un procedimiento de gestión de

movilidad de NAS y terminándose en la NF1, y portando la otra conexión de NAS un procedimiento de gestión de sesión de NAS y terminándose en la NF2.

SUMARIO

Este sumario se proporciona para introducir conceptos simplificados de configuración de subred y procedimientos para posibilitar operaciones de subred, en particular, en identidades de subred. Este sumario no tiene por objeto identificar características clave o esenciales de la materia objeto reivindicada, ni se pretende su uso para limitar el alcance de la materia objeto reivindicada.

De acuerdo con un primer aspecto de la divulgación, se proporciona un dispositivo terminal. El dispositivo terminal comprende al menos un procesador; y al menos una memoria que almacena instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que el dispositivo terminal al menos: genere una clave de anclaje; reciba un identificador de clave de anclaje para la clave de anclaje; derive un conjunto de claves progenitoras de NAS basándose en la clave de anclaje, un identificador de abono e indicadores de NAS que indican diferentes procedimientos de NAS; y obtenga, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS.

De acuerdo con un segundo aspecto de la divulgación, se proporciona una entidad de red configurada para implementar la función de gestión de claves de seguridad (SKMF). La entidad de red comprende al menos un procesador; y al menos una memoria que almacena instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que la entidad de red al menos: genere una clave de anclaje con un dispositivo terminal; derive un identificador de clave de anclaje para la clave de anclaje, y envíe el identificador de clave de anclaje al

dispositivo terminal; derive un conjunto de claves progenitoras de NAS basándose en la clave de anclaje, un identificador de abono e indicadores de NAS que indican diferentes procedimientos de NAS; y derive, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS basándose en el indicador de NAS respectivo.

De acuerdo con un tercer aspecto de la divulgación, se proporciona una entidad de red central configurada para implementar una función de red central. La entidad de red central comprende al menos un procesador; y al menos una memoria que almacena instrucciones que, cuando son ejecutadas por el al menos un procesador, hacen que la entidad de red al menos: reciba desde un dispositivo terminal una solicitud de establecimiento de una conexión de NAS que porta un procedimiento de NAS entre el dispositivo terminal y la entidad de red central; y obtenga una clave de NAS para la conexión de NAS, en donde la clave de NAS es una clave progenitora de NAS o una clave vástago de NAS asociada con un indicador de NAS que indica el procedimiento de NAS.

De acuerdo con un cuarto aspecto de la divulgación, se proporciona un método realizado por un dispositivo terminal. El método comprende: generar una clave de anclaje; recibir un identificador de clave de anclaje para la clave de anclaje; derivar un conjunto de claves progenitoras de estrato sin acceso, NAS, basándose en la clave de anclaje, un identificador de abono e indicadores de NAS que indican diferentes procedimientos de NAS; y obtener, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS.

De acuerdo con un quinto aspecto de la presente divulgación, se proporciona un método realizado por una entidad de red configurada para

implementar la función de gestión de claves de seguridad (SKMF). El método comprende: generar una clave de anclaje con un dispositivo terminal; derivar un identificador de clave de anclaje para la clave de anclaje, y enviar el identificador de clave de anclaje al dispositivo terminal; derivar un conjunto de claves progenitoras de estrato sin acceso, NAS, basándose en la clave de anclaje, un
5 identificador de abono e indicadores de NAS que indican diferentes procedimientos de NAS; y derivar, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS basándose en el indicador de NAS respectivo.

10 De acuerdo con un sexto aspecto de la presente divulgación, se proporciona un método realizado por una entidad de red central configurada para implementar una función de red central. El método comprende: recibir desde un dispositivo terminal una solicitud de establecimiento de una conexión de NAS que porta un procedimiento de NAS entre el dispositivo terminal y la entidad de
15 red central; y obtener una clave de NAS para la conexión de NAS, en donde la clave de NAS es una clave progenitora de NAS o una clave vástago de NAS asociada con un indicador de NAS que indica el procedimiento de NAS.

De acuerdo con un séptimo aspecto de la presente divulgación, se proporciona un dispositivo terminal. El dispositivo terminal comprende medios
20 para realizar etapas de cualquier método de acuerdo con el cuarto aspecto.

De acuerdo con un octavo aspecto de la presente divulgación, se proporciona una entidad de red configurada para implementar la función de gestión de claves de seguridad (SKMF). La entidad de red comprende medios para realizar etapas de cualquier método de acuerdo con el quinto aspecto.

25 De acuerdo con un noveno aspecto de la presente divulgación, se

proporciona una entidad de red central configurada para implementar una función de red central. La entidad de red central comprende medios para realizar etapas de cualquier método de acuerdo con el sexto aspecto.

De acuerdo con un décimo aspecto de la presente divulgación, se
5 proporciona un medio de almacenamiento legible por ordenador, en el que se almacenan instrucciones, cuando son ejecutadas por al menos un procesador, las instrucciones hacen que el al menos un procesador realice cualquier método de acuerdo con el cuarto o el quinto o el sexto aspecto.

De acuerdo con un undécimo aspecto de la presente divulgación, se
10 proporciona un producto de programa informático que comprende instrucciones que, cuando son ejecutadas por al menos un procesador, hacen que el al menos un procesador realice cualquier método de acuerdo con el cuarto o el quinto o el sexto aspecto.

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

BREVE DESCRIPCIÓN DE LOS DIBUJOS

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

la figura 1 ilustra un ejemplo de una única terminación de NAS en la arquitectura de sistema de 5G;

la figura 2 ilustra un ejemplo de la arquitectura de terminaciones de NAS
25 distribuida;

la figura 3 ilustra un ejemplo de una jerarquía de claves para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

5 la figura 4 ilustra otro ejemplo de una jerarquía de claves para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

la figura 5 ilustra otro ejemplo más de una jerarquía de claves para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

10 la figura 6 ilustra aún otro ejemplo de una jerarquía de claves para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

la figura 7 es un flujo de llamada ilustrativo para asegurar múltiples conexiones de NAS de acuerdo con algunas realizaciones de la presente divulgación;

la figura 8 ilustra una arquitectura de seguridad para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

20 la figura 9 ilustra un marco de seguridad para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

la figura 10 es otro flujo de llamada ilustrativo para asegurar múltiples conexiones de NAS de acuerdo con algunas realizaciones de la presente divulgación;

25 la figura 11 es un diagrama de flujo que representa un método para la

seguridad en la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

la figura 12 es un diagrama de flujo que representa un método para la seguridad en la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación;

la figura 13 es un diagrama de flujo que representa un método para la seguridad en la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación; y

la figura 14 muestra un diagrama de bloques simplificado de un aparato de acuerdo con algunas realizaciones de la presente divulgación.

DESCRIPCIÓN DETALLADA

Algunas realizaciones de ejemplo se describirán a continuación más completamente en lo sucesivo en el presente documento con referencia a los dibujos adjuntos, en los que se muestran algunas de las realizaciones, pero no todas ellas. De hecho, las realizaciones de ejemplo pueden adoptar muchas formas diferentes y no se deberían interpretar como limitadas a las realizaciones expuestas en el presente documento; más bien, estas realizaciones se proporcionan de tal modo que esta divulgación satisfaga los requisitos legales aplicables. Números de referencia similares se refieren a elementos similares a lo largo de todo el presente documento.

En la descripción y reivindicaciones siguientes, a menos que se defina lo contrario, todos los términos técnicos y científicos usados en el presente documento tienen el mismo significado que entendería comúnmente un experto en la materia a la que pertenece esta divulgación.

Referencias en la presente divulgación a "una realización", "una

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

10 Se deberá entender que, aunque los términos "primero" y "segundo" etc., se pueden usar en el presente documento para describir diversos elementos, estos elementos no deberían estar limitados por estos términos. Estos términos se usan solo para distinguir un elemento de otro. Por ejemplo, un primer elemento se podría denominar segundo elemento y, de forma similar, un segundo
15 elemento se podría denominar primer elemento, sin apartarse del alcance de las realizaciones de ejemplo. Como se usa en el presente documento, la expresión "y/o" incluye todas y cada una de las combinaciones de uno o más de los términos enumerados.

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

cuando se usan en el presente documento, especifican la presencia de rasgos, elementos y/o componentes etc., expuestos, pero no excluyen la presencia o adición de otros uno o más rasgos, elementos o componentes diferentes, y/o combinaciones de los mismos.

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

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

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

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

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

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

25 Esta definición de "circuitería" es aplicable a todos los usos de este término en esta solicitud, incluyendo en cualquier reivindicación. Como un ejemplo adicional, como se usa en esta solicitud, el término "circuitería" también cubre una implementación de meramente un circuito de hardware o procesador

(o múltiples procesadores) o porción de un circuito de hardware o procesador y su software y/o firmware adjunto. El término "circuitería" también cubre, por ejemplo, y si es aplicable al elemento de reivindicación particular, un circuito integrado de banda base o circuito integrado de procesador para un dispositivo móvil o un circuito integrado similar en servidor, un dispositivo de red celular u otro dispositivo informático o de red.

Como se usa en el presente documento, la expresión "red de comunicación" se refiere a una red que sigue cualquier norma de comunicación adecuada, tal como evolución a largo plazo (LTE), LTE avanzada (LTE-A), acceso múltiple por división de código de banda ancha (WCDMA), acceso por paquetes de alta velocidad (HSPA), Internet de las cosas de banda estrecha (NB-IoT), nueva radio (NR) y así sucesivamente. Además, las comunicaciones entre un dispositivo terminal y un dispositivo de red en la red de comunicación se pueden realizar de acuerdo con cualquier protocolo de comunicación de generación adecuado, incluyendo, pero sin limitación, los protocolos de comunicación de la primera generación (1G), la segunda generación (2G), 2.5G, 2.75G, la tercera generación (3G), la cuarta generación (4G), 4.5G, 5G, de la sexta generación (6G) futura, y/o cualquier otro protocolo o bien conocido en la actualidad o bien que se vaya a desarrollar en el futuro. Las realizaciones de la presente divulgación se pueden aplicar en diversos sistemas de comunicación. Dado el rápido desarrollo en las comunicaciones, también existirán, por supuesto, tecnologías y sistemas de comunicación de tipo futuro con los que se pueda materializar la presente divulgación. No se debería ver como que limita el alcance de la presente divulgación a solo el sistema mencionado anteriormente.

Como se usa en el presente documento, la expresión "dispositivo terminal"

se refiere a cualquier dispositivo de extremo que pueda acceder a una red de comunicación y recibir servicios desde la misma. A modo de ejemplo y no de limitación, el dispositivo terminal se puede referir a un equipo de usuario (UE) que puede ser una combinación de una tarjeta de circuito integrado universal (UICC)/tarjeta de módulo de identidad de abonado (SIM) y un equipo móvil (ME),
5 u otros dispositivos adecuados. En la siguiente descripción, se pueden usar de forma intercambiable las expresiones "dispositivo terminal", "equipo de usuario" y "UE".

Como se usa en el presente documento, la expresión "entidad de red" se
10 refiere a cualquier entidad para soportar una función de red en una red de comunicación. La entidad de red se puede implementar en un nodo de red física o en un nodo de red virtual que realiza una función por recursos lógicos en más de un nodo de red física.

Como se ha mencionado anteriormente, la arquitectura de sistema de 5G
15 define en especificaciones de 3GPP (por ejemplo, la TS 23.501/23.502/24.501/33.501) cómo se consigue seguridad para una única conexión de NAS entre un UE y una única NF. Sin embargo, no se define ninguna solución para conseguir seguridad para múltiples conexiones de NAS de una arquitectura de terminaciones de NAS distribuida.

20 Por lo tanto, diversas realizaciones de la presente divulgación describen un marco para asegurar las conexiones de NAS de la arquitectura de terminaciones de NAS distribuida. Específicamente, el marco proporciona un mecanismo para la derivación y distribución de claves secretas compartidas e identificadores de clave asociados usados para asegurar las conexiones de NAS
25 establecidas entre el UE y las NF de terminación.

En primer lugar, se describe una jerarquía de claves para la arquitectura de terminaciones de NAS distribuida. Para ayudar en la descripción, se proporciona una analogía a un subconjunto de la jerarquía de claves de arquitectura de 5G actual en donde las expresiones "clave de anclaje" y "clave progenitora de NAS" son análogas a K_{seaf} y K_{amf} , respectivamente. Sin embargo, existen múltiples claves progenitoras de NAS en donde K_{amf} se puede considerar como una clave progenitora de NAS. Las claves progenitoras de NAS proporcionan separación de claves para conexiones de NAS que portan diferentes procedimientos de NAS tales como procedimientos de gestión de movilidad de NAS, procedimientos de gestión de sesión de NAS, procedimientos de gestión de política de UE de NAS y así sucesivamente.

La figura 3 ilustra un ejemplo de la jerarquía de claves para la arquitectura de terminaciones de NAS distribuida (la Opción 1) de acuerdo con algunas realizaciones de la presente divulgación, que incluye una clave de anclaje común y una clave progenitora de NAS común. Haciendo referencia a la figura 3, se establece una única clave de anclaje K_a por medio de un procedimiento de autenticación y acuerdo de clave (AKA), que es común a todas las conexiones de NAS. Esta clave de anclaje K_a es equivalente a la clave K_{seaf} en la jerarquía de claves de arquitectura de 5G actual. Una única clave progenitora de NAS K_p se deriva de la clave de anclaje común K_a que es común a todas las conexiones de NAS. Este enfoque requiere una única ejecución de procedimiento de AKA independientemente del número de conexiones de NAS.

La opción 1 está estrechamente alineada con la jerarquía de claves de arquitectura de 5G actual, Sin embargo, esta tiene una serie de inconvenientes cuando se aplica a la arquitectura de terminaciones de NAS distribuida: a) debido

a que la misma clave progenitora de NAS K_p se usa en diferentes conexiones de NAS, puede aumentar la superficie de ataque y debilitar la seguridad de NAS, especialmente con múltiples puntos de terminación de NAS; y b) es necesario que la misma clave progenitora de NAS K_p se distribuya a múltiples NF, lo que
5 aumenta la superficie de ataque en comparación con 5G y debilita la seguridad de NAS.

La figura 4 ilustra otro ejemplo de la jerarquía de claves para la arquitectura de terminaciones de NAS distribuida (la Opción 2) de acuerdo con algunas realizaciones de la presente divulgación, que incluye una clave de
10 anclaje común K_a y múltiples claves progenitoras de NAS, K_{p1} , K_{p2} , ... , K_{pn} . Haciendo referencia a la figura 4, se establece una clave de anclaje K_a por medio de un procedimiento de AKA, que es común a todas las conexiones de NAS. Esta clave de anclaje K_a es equivalente a la clave K_{seaf} en la jerarquía de claves de arquitectura de 5G actual. Múltiples claves progenitoras de NAS K_{p1} , K_{p2} , ... ,
15 K_{pn} se derivan de esta clave de anclaje común K_a para cada conexión de NAS. Este enfoque requiere una única ejecución de procedimiento de AKA independientemente del número de conexiones de NAS.

La figura 5 ilustra otro ejemplo más de la jerarquía de claves para la arquitectura de terminaciones de NAS distribuida (la Opción 3) de acuerdo con
20 algunas realizaciones de la presente divulgación, que incluye múltiples claves de anclaje y múltiples claves progenitoras de NAS. Haciendo referencia a la figura 5, se establecen múltiples claves de anclaje K_{a1} , K_{a2} , ... , K_{an} por medio de un procedimiento de AKA, una para cada conexión de NAS. Estas claves de anclaje K_{a1} , K_{a2} , ... , K_{an} son equivalentes a múltiples claves K_{seaf} singulares
25 derivadas de una clave K_{ausf} en la jerarquía de claves de arquitectura de 5G

actual. Una clave progenitora de NAS se deriva de cada clave de anclaje para cada conexión de NAS. Como se muestra en la figura 5, la clave progenitora de NAS Kp1 se deriva de la clave de anclaje Ka1, la clave progenitora de NAS Kp2 se deriva de la clave de anclaje Ka2, y la clave progenitora de NAS Kpn se deriva de la clave de anclaje Kan. Este enfoque requiere que se ejecute un procedimiento de AKA para cada conexión de NAS.

La opción 2 y la opción 3 proponen usar múltiples claves progenitoras de NAS que proporcionan claves de secretos compartidos singulares para cada conexión de NAS y, por lo tanto, ofrecen una mejor seguridad de NAS en comparación con la opción 1 que tiene la clave progenitora de NAS común para todas las conexiones de NAS.

Se puede considerar que la opción 3 ofrece la seguridad más robusta en el sentido de que cada conexión de NAS tiene su propia clave de anclaje y clave progenitora de NAS derivada de una ejecución de AKA. Sin embargo, la opción 3 requiere que el procedimiento de AKA se ejecute y se señalice con la red doméstica cada vez que se establece una nueva conexión de NAS, lo que puede obstaculizar la ejecución de los procedimientos de NAS. Además, también conlleva impactos para la NF de red doméstica (por ejemplo, función de autenticación (AUSF), gestión de datos unificada (UDM), repositorio de datos unificado (UDR)) así como para el UE (por ejemplo, tarjeta de circuito integrado universal (UICC), equipo móvil (ME)) para derivar, almacenar y gestionar múltiples claves de anclaje.

La opción 2 también soporta múltiples claves progenitoras de NAS, pero debido a la clave de anclaje común, requiere solo un único procedimiento de AKA para múltiples conexiones de NAS y no tiene ningún impacto sobre la NF de red

doméstica (por ejemplo, AUSF, UDM, UDR). En este sentido, la Opción 2 se considera como la jerarquía de claves más óptima para la arquitectura de terminaciones de NAS distribuida y se detallará más adelante. Además, la siguiente descripción se describirá en el contexto de la Opción 2, y también será aplicable a la Opción 3.

La figura 6 ilustra aún otro ejemplo de la jerarquía de claves para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación, en la que se propone una clave vástago de NAS además de la clave de anclaje común Ka y múltiples claves progenitoras de NAS, por ejemplo, Kp1, Kp2. Mientras que las claves progenitoras de NAS proporcionan separación de claves para conexiones de NAS que portan diferentes procedimientos de NAS, las claves vástago de NAS proporcionan separación de claves para conexiones de NAS que portan el mismo procedimiento de NAS, por ejemplo, procedimientos de gestión de sesión de NAS. Un UE puede tener dos sesiones de unidad de datos de protocolo (PDU) de NAS y, por lo tanto, tener dos conexiones de NAS que pertenecen a diferentes segmentos de red, teniendo cada segmento diferentes requisitos de seguridad. Como se muestra en la figura 6, las claves vástago de NAS Kc2-1 y Kc2-2 se derivan de la clave progenitora de NAS Kp2 para las dos conexiones de NAS. Las claves vástago de NAS proporcionan separación de claves entre estas dos conexiones de NAS. Obsérvese que la clave vástago de NAS se aplica predominantemente a procedimientos de gestión de sesión de NAS, pero su uso no se excluye para otros procedimientos de NAS.

La figura 7 es un flujo de llamada ilustrativo para asegurar múltiples conexiones de NAS de acuerdo con algunas realizaciones de la presente

divulgación, que representa un escenario en el que un UE se registra en una red y, posteriormente, establece dos conexiones de NAS diferentes, una que porta procedimientos de gestión de sesión de NAS y otra que porta procedimientos de gestión de política de UE de NAS. En este ejemplo, el flujo de llamada implica el UE, dos NF centrales, la NF1 y la NF2, y la función de gestión de claves de seguridad (SKMF) que es análoga a la función de anclaje de seguridad (SEAF) en 5G.

En la etapa 1, se ejecuta el procedimiento de AKA primario que establece, tanto en el UE como en la SKMF, una clave de anclaje y un conjunto de claves progenitoras de NAS.

En la etapa 2, el UE solicita el establecimiento de la conexión de NAS n.º 1 enviando un mensaje de solicitud de conexión de NAS n.º 1, por ejemplo, una solicitud de gestión de sesión (SM) de NAS inicial, que se encamina a la NF1. Debido a que la NF1 no tiene un contexto de seguridad válido para la conexión de NAS n.º 1, esta solicita una clave desde la SKMF, por ejemplo, enviando una solicitud de clave.

En la etapa 3, basándose en información proporcionada en la solicitud de clave desde la NF1, la SKMF puede o bien seleccionar una clave progenitora de NAS ya derivada específica de procedimientos de SM de NAS o bien, como alternativa, derivar una clave vástago de NAS a partir de la clave progenitora de NAS seleccionada, y devuelve la clave progenitora de NAS o la clave vástago de NAS a la NF1, por ejemplo, en una respuesta clave.

En la etapa 4, la NF1 usa la clave recibida para derivar adicionalmente claves de integridad y cifrado de NAS para usarse con algoritmos de integridad y cifrado de NAS seleccionados para asegurar la conexión de NAS n.º 1. La NF1

envía un mensaje de orden de modo de seguridad de NAS hacia el UE.

En la etapa 5, basándose en el mensaje de orden de modo de seguridad de NAS recibido desde la NF1, la UE puede o bien seleccionar una clave progenitora de NAS ya derivada específica de procedimientos de SM de NAS o bien, como alternativa, derivar una clave vástago de NAS a partir de la clave progenitora de NAS seleccionada, y usar la clave progenitora de NAS o la clave vástago de NAS para derivar adicionalmente claves de integridad y cifrado de NAS como se derivan en la NF1. El UE rellena el mensaje de solicitud de conexión de NAS n.º 1 completo para dar un mensaje de modo de seguridad de NAS completo, asegura el mensaje de modo de seguridad de NAS completo con las claves de integridad y cifrado de NAS y envía el mensaje de modo de seguridad de NAS completo cifrado y protegido en cuanto a su integridad a la NF1.

En la etapa 6, la NF1 usa sus claves de integridad y cifrado de NAS para realizar comprobaciones de seguridad en el mensaje de modo de seguridad de NAS completo recibido, extrae el mensaje de solicitud de conexión de NAS n.º 1 completo, lo procesa y devuelve una respuesta de conexión de NAS n.º 1 al UE. En este punto, se establece un contexto de seguridad entre el UE y la NF1 para la conexión de NAS n.º 1 usando las claves de integridad y cifrado de NAS derivadas y los algoritmos de integridad y cifrado de NAS seleccionados.

En la etapa 7, el UE solicita el establecimiento de la conexión de NAS n.º 2 enviando un mensaje de solicitud de conexión de NAS n.º 2, por ejemplo, una solicitud de política de UE de NAS inicial, que se encamina a la NF2. Debido a que la NF2 no tiene un contexto de seguridad válido para esta conexión de NAS, esta solicita una clave desde la SKMF enviando una solicitud de clave a la SKMF.

En la etapa 8, basándose en información proporcionada en la solicitud de clave desde la NF2, la SKMF puede o bien seleccionar una clave progenitora de NAS ya derivada específica de procedimientos de gestión de política de UE de NAS o bien, como alternativa, derivar una clave vástago de NAS a partir de la clave progenitora de NAS seleccionada, y devuelve la clave progenitora de NAS o la clave vástago de NAS a la NF2.

En la etapa 9, la NF2 usa la clave recibida para derivar adicionalmente claves de integridad y cifrado de NAS para usarse con algoritmos de integridad y cifrado de NAS seleccionados para asegurar la conexión de NAS n.º 2. La NF2 envía un mensaje de orden de modo de seguridad de NAS hacia el UE.

En la etapa 10, basándose en el mensaje de orden de modo de seguridad de NAS recibido desde la NF2, la UE puede o bien seleccionar una clave progenitora de NAS ya derivada específica de procedimientos de gestión de política de UE de NAS o bien, como alternativa, derivar una clave vástago de NAS a partir de la clave progenitora de NAS seleccionada, y usar la clave progenitora de NAS o la clave vástago de NAS para derivar adicionalmente claves de integridad y cifrado de NAS como se derivan en la NF2. El UE rellena el mensaje de solicitud de conexión de NAS n.º 2 completo para dar un mensaje de modo de seguridad de NAS completo, asegura el mensaje de modo de seguridad de NAS completo con las claves de integridad y cifrado de NAS y envía el mensaje de modo de seguridad de NAS completo cifrado y protegido en cuanto a su integridad a la NF2.

En la etapa 11, la NF2 usa sus claves de integridad y cifrado de NAS para realizar comprobaciones de seguridad en el mensaje de modo de seguridad de NAS completo recibido, extrae el mensaje de solicitud de conexión de NAS n.º 2

completo, lo procesa y devuelve una respuesta de conexión de NAS n.º 2 al UE. En este punto, se establece un contexto de seguridad entre el UE y la NF2 para la conexión de NAS n.º 2 usando las claves de integridad y cifrado de NAS derivadas y los algoritmos de integridad y cifrado de NAS seleccionados.

- 5 Los intercambios de mensajes de NAS posteriores en relación con la conexión de NAS n.º 1 y la conexión de NAS n.º 2 se protegen mediante sus contextos de seguridad respectivos que sobreviven a la transición de modo en reposo a conectado y, por lo tanto, evitan la necesidad de volver a ejecutar los procedimientos de orden de modo de seguridad de NAS.
- 10 Las realizaciones de la presente divulgación proporcionarán los siguientes aspectos novedosos:
- clave progenitora de NAS, identificador de clave (KI) progenitora de NAS y cómo se derivan y se usan los mismos;
 - clave vástago de NAS, identificador de clave vástago de NAS y cómo se
- 15 derivan, se distribuyen y se usan los mismos;
- concepto de TROCEO
 - potenciación del procedimiento de orden de modo de seguridad (SMC)
- de NAS para soportar nuevos parámetros
- potenciación de la funcionalidad de SEAF para soportar la derivación y
- 20 distribución de clave progenitora/vástago de NAS como una NF independiente, es decir, SKMF;
- potenciación de la funcionalidad de UE para soportar la derivación de
- clave progenitora/vástago de NAS, procedimientos de SMC de NAS potenciados que consideran un nuevo identificador temporal (por ejemplo, MM-GUTI (gestión
- 25 de movilidad - identificador temporal globalmente singular) o su versión

abreviada MM-S-TMSI (gestión de movilidad - abreviada - identidad de abonado móvil temporal), manejo de SM-GUTI (gestión de sesión - identificador temporal globalmente singular)/SM-S-TMSI, etc.) para múltiples terminaciones de NAS;

- potenciación de la jerarquía de claves en la red y el UE;
- 5 • potenciación de las NF para soportar la terminación de NAS y soportar procedimientos de SMC, establecimiento/generación de parámetros de TROCEO, procedimientos de solicitud de clave, procedimiento de solicitud de capacidades de UE potenciados;
- 10 • nuevas interfaces y procedimientos basados en servicio de gestión de claves (Solicitud/Respuesta, Abono/Notificación) para comunicaciones inter NF, por ejemplo, Comunicaciones NF-NF y NF-SKMF. Los servicios incluyen solicitudes de derivación de clave, notificaciones de derivación de nueva clave (ejecución de AKA), solicitudes de autenticación y solicitudes registradas por UE;
- 15 • potenciación del procedimiento de autenticación primario para incluir derivación de clave progenitora de NAS y, opcionalmente, derivación de identificadores de clave progenitora de NAS;
- mensajes de NAS iniciales recién definidos y Elementos de Información obligatorios mínimos.

Algunos aspectos descritos en el presente documento pueden aprovechar
20 y ampliar las siguientes funcionalidades y procedimientos en especificaciones de 3GPP tales como:

- El procedimiento de orden de modo de seguridad de NAS como se define en la TS 33.501 del 3GPP;
- La jerarquía de claves definida en la TS 33.501 del 3GPP;
- 25 • El contenedor de NAS usado en traspasos de N2 en la TS 33.501 del

3GPP.

- Procedimientos de autenticación como se definen en la TS 33.501 del 3GPP

5 También se debería hacer notar que los números de especificación para el Sistema de 6G y la seguridad no se conocen en el momento de esta publicación.

La figura 8 ilustra una arquitectura de seguridad para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación. Como se muestra en la figura 8, la arquitectura de seguridad implica el UE, múltiples NF centrales y la SKMF.

En el lado de la red, la SKMF en la red de servicio soporta la derivación y gestión de las claves e identificadores de clave (KI) de anclaje/progenitora de NAS/vástago de NAS. Se propone que la SKMF abarque y amplíe la funcionalidad de SEAF definida actualmente para soportar adicionalmente un conjunto de servicios normalizados que posibilitarían que la(s) NF central(es) obtenga(n) claves progenitoras/vástago de NAS e identificadores de clave, así como que se abone(n) a y que reciba(n) notificaciones cuando se deriven nuevas claves de seguridad, por ejemplo, nuevas claves progenitoras de anclaje/NAS derivadas como resultado de una ejecución de AKA primaria con éxito.

20 En términos de despliegues, la SKMF se puede:

Opción 1: desplegar como una SKMF autónoma en una ubicación centralizada que expone sus servicios a través de interfaces basadas en servicio (SBI) y servicios. Como un despliegue autónomo, proporciona flexibilidad en términos de ubicación de despliegue, seguridad, rendimiento y capacidad de ajuste a escala;

Opción 2: coubicar con una NF central que maneja el procedimiento de gestión de movilidad de NAS. Esta opción puede conllevar potencialmente optimizaciones en términos de carga de señalización.

Definir un conjunto de servicios de gestión de claves y exponer estos a través de SBI proporciona la mayor flexibilidad y posibilita elecciones de implementación.

En algunas realizaciones, las NF centrales pueden terminar la(s) conexión(es) de NAS y almacenar y gestionar, para cada conexión de NAS, el contexto de seguridad de NAS que incluye el identificador de clave de anclaje, el identificador de clave progenitora de NAS, la clave vástago de NAS, el identificador de clave vástago de NAS, algoritmos de NAS, claves de integridad y cifrado de NAS y recuentos de NAS. Las NF centrales también pueden soportar una función de derivación de TROCEO que es responsable de definir parámetros de entrada y la derivación de un valor de TROCEO que se proporciona al UE y a la SKMF para derivar la clave vástago de NAS. Las NF centrales también pueden soportar los procedimientos de orden de modo de seguridad de NAS y el procesamiento de contenedor de NAS (durante traspasos de N2).

Además, en algunas realizaciones, la NF central que termina los procedimientos de gestión de movilidad de NAS solo tendrá una única conexión de NAS para cada tipo de acceso en cualquier punto en el tiempo para cada UE. Estas NF centrales también son responsables de la derivación y distribución de material de gestión de claves específico del estrato de acceso (AS) como se define actualmente en la TS 33.501 del 3GPP, por ejemplo, KgNB, NCC, NH, KN3IWF.

En algunas realizaciones, el UE solo puede tener una única conexión de

NAS para procedimientos de gestión de movilidad de NAS para cada tipo de acceso en cualquier punto en el tiempo, y puede tener simultáneamente cero, una o más conexiones de NAS para procedimientos no de gestión de movilidad de NAS. En otras palabras, las conexiones de NAS para procedimientos no de gestión de movilidad de NAS solo pueden existir cuando ya hay establecida una conexión de NAS para procedimientos de gestión de movilidad de NAS.

La funcionalidad de UE se puede ampliar para soportar la derivación y gestión de clave progenitora/vástago de NAS e identificador de clave, así como ampliaciones al procedimiento de AKA y procedimientos relacionados con contenedor de SMC/NAS de NAS.

Lo siguiente explicará algunos conceptos mencionados en las realizaciones de la presente divulgación.

1. Indicador de NAS

Cuando las conexiones de NAS se terminan en diferentes tipos de NF centrales dependiendo del procedimiento de NAS que porta una conexión de NAS, se supone que el UE proporciona un indicador de NAS (con valores normalizados) para indicar el procedimiento de NAS que se porta. Por ejemplo, una conexión de NAS que porta procedimientos de gestión de movilidad de NAS se terminará en una NF central que soporta procedimientos de gestión de movilidad de NAS, una conexión de NAS que porta procedimientos de gestión de sesión de NAS se terminará en una NF central que soporta procedimientos de gestión de sesión de NAS.

En algunas realizaciones, se puede definir y normalizar el indicador de NAS, y sus valores indicarán los procedimientos de NAS soportados. Por ejemplo:

valor de indicador de NAS "MM" = procedimientos de gestión de movilidad de NAS;

valor de indicador de NAS "SM" = procedimientos de gestión de sesión de NAS;

5 valor de indicador de NAS "SMS" = procedimientos de gestión de servicio de mensajes cortos (SMS) de NAS;

valor de indicador de NAS "UEP" = procedimientos de gestión de política de UE de NAS, etc.

En algunas realizaciones, todos los valores del indicador de NAS son conocidos
10 de forma inherente por el UE y la red.

En algunas realizaciones, el indicador de NAS se puede portar en mensajes de NAS para identificar el procedimiento de NAS y se puede usar para tomar decisiones acerca de la selección de NF y las derivaciones de clave de seguridad. El indicador de NAS también se proporciona a y es visible para las
15 capas inferiores (por ejemplo, control de recursos de radio (RRC)) para posibilitar que los nodos de acceso tomen una decisión acerca del descubrimiento y selección de NF.

En algunas realizaciones, el indicador de NAS también se puede incluir en perfiles de NF para soportar posibilitar el descubrimiento y la selección de la
20 NF correcta de la función de repositorio de red (NRF), por ejemplo.

2. Jerarquía, derivación y distribución de claves de seguridad

La figura 9 ilustra un marco de seguridad para la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación. Para este marco de seguridad, la misma introduce los
25 siguientes conceptos:

- Clave de anclaje e identificador de clave de anclaje;
- Clave progenitora de NAS e identificador de clave progenitora de NAS;
- Clave vástago de NAS e identificador de clave vástago de NAS;
- Valor de TROCEO.

5 2.1 Clave de anclaje e identificador de clave de anclaje

La clave de anclaje y el identificador de clave de anclaje pueden proporcionar un anclaje con el que se construye la seguridad para la arquitectura de terminaciones de NAS distribuida. La clave de anclaje y el identificador de clave de anclaje son análogos a Kseaf y ngKSI usados respectivamente en 5G con los mismos procedimientos de AKA que tienen algunas ampliaciones/potenciaciones.

2.2 Clave progenitora de NAS e identificador de clave progenitora de NAS

Una clave progenitora de NAS puede ser derivada independientemente por el UE y la SKMF a partir de una clave de anclaje, un identificador permanente de abono (SUPI) y un indicador de NAS. Un identificador de clave progenitora de NAS está asociado con una clave progenitora de NAS y puede ser derivado independientemente por el UE y la SKMF.

El fin de la clave progenitora de NAS es proporcionar una clave secreta compartida que es singular para las conexiones de NAS que portan el mismo tipo de procedimientos de NAS. Por ejemplo, una conexión de NAS que porta procedimientos de gestión de movilidad de NAS puede tener una clave progenitora de NAS que es diferente de una conexión de NAS que está portando procedimientos de gestión de sesión de NAS y así sucesivamente.

En algunas realizaciones, una nueva clave progenitora de NAS también puede ser derivada horizontalmente por el UE y la SKMF, por ejemplo, durante

traspasos de N2, usando como entrada la clave progenitora de NAS actual y un valor de recuento de NAS. En este caso, la nueva clave progenitora de NAS se identifica por el identificador de clave progenitora de NAS existente de la clave progenitora de NAS antigua.

- 5 En algunas realizaciones, el valor de un identificador de clave progenitora de NAS puede ser el mismo que el valor de indicador de NAS usado para derivar esa clave progenitora de NAS. Debido a que todos los valores de indicador de NAS se normalizan y, por lo tanto, son conocidos tanto por el UE como por la SKMF, esto asegura que tanto el UE como la SKMF pueden derivar los mismos
- 10 identificadores de clave progenitora de NAS para las claves progenitoras de NAS que los mismos derivan, respectivamente.

Un enfoque alternativo para la generación del identificador de clave progenitora de NAS es que la SKMF puede asignar un valor singular para cada identificador de clave progenitora de NAS y proporcionar este valor y el indicador

15 de NAS asociado al UE durante el procedimiento de AKA. Este enfoque puede permitir que la red de servicio controle los valores de identificador de clave progenitora de NAS y quite el requisito de derivar los identificadores de clave progenitora de NAS a partir del UE.

2.3 Clave vástago de NAS e identificador de clave vástago de NAS

- 20 En algunas realizaciones, una clave vástago de NAS puede ser derivada independientemente por el UE y la SKMF a partir de una clave progenitora de NAS y un valor de TROCEO.

El fin de la clave vástago de NAS es proporcionar claves secretas compartidas que son singulares para conexiones de NAS que portan el mismo

25 tipo de procedimientos de NAS. Esto es necesario cuando un único tipo de

conexión de NAS se puede terminar en múltiples instancias de NF central. Por ejemplo, una conexión de NAS que porta procedimientos de gestión de sesión de NAS puede tener dos sesiones de PDU de NAS, una terminada en el SM de procesamiento de instancia de NF central del segmento 1 y la otra terminada en el SM de procesamiento de instancia de NF central al segmento 2. Se pueden derivar las claves vástago de NAS que son singulares tanto para el segmento 1 como para el segmento 2.

En algunas realizaciones, un identificador de clave vástago de NAS, que está asociado a una clave vástago de NAS específica, se puede derivar en la SKMF y se puede proporcionar posteriormente al UE durante un procedimiento de SMC de NAS o en un contenedor de NAS durante traspasos de N2.

Para que el UE derive una clave vástago de NAS, la siguiente información es proporcionada al UE por la red:

- un identificador de clave de anclaje para comprobar que esta está asociada con una ejecución de AKA actual y válida;
- un identificador de clave de anclaje y un identificador de clave progenitora de NAS para identificar la clave progenitora de NAS;
- un valor de TROCEO que se va a usar con la clave progenitora de NAS para derivar la clave vástago de NAS;
- un identificador de clave vástago de NAS que se asigna a la clave vástago de NAS derivada.

En algunas realizaciones, una nueva clave vástago de NAS también puede ser derivada horizontalmente por el UE y la SKMF, por ejemplo, durante traspasos de N2, usando como entrada la clave vástago de NAS actual y un valor de recuento de NAS. En este caso, la nueva clave vástago de NAS se puede

identificar por el identificador de clave vástago de NAS existente de la clave vástago de NAS antigua.

Para identificar una clave específica, pueden ser necesarios un único o múltiples identificadores de clave. Por ejemplo, para identificar una clave de anclaje, es necesario solo el identificador de clave de anclaje. Para identificar una clave progenitora de NAS, son necesarios el identificador de clave de anclaje y el identificador de clave progenitora de NAS. Y para identificar una clave vástago de NAS, son necesarios el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el identificador de clave vástago de NAS.

2.4 Valor de TROCEO

El fin del valor de TROCEO es proporcionar separación de las claves vástago de NAS. Un valor de TROCEO es un valor que se deriva por una NF central a partir de un conjunto específico de parámetros de entrada, y la NF central se puede configurar para seleccionar de entre los mismos y proporcionarlos al UE y la SKMF. Cada NF central puede usar los mismos o diferentes conjuntos de parámetros de entrada para derivar el valor de TROCEO. El UE y la SKMF son independientes de cómo se deriva el valor de TROCEO, lo que proporciona flexibilidad en el/los mecanismo(s) usado(s) para derivar el valor de TROCEO.

En algunas realizaciones, tales parámetros de entrada pueden ser información de asistencia de selección de segmento de red único (S-NSSAI), un ID de sesión de PDU, un ID de conjunto de NF, etc. Los parámetros usados para generar el valor de TROCEO pueden ser configurados por la red y, por lo tanto, pueden ser específicos del operador de red de servicio. El valor de TROCEO se

puede comunicar al UE como parte de un procedimiento de orden de modo de seguridad de NAS potenciado para posibilitar que el UE derive la clave vástago de NAS.

Dependiendo de cómo se deriva el valor de TROCEO, se puede usar una
5 clave vástago de NAS para asegurar una única conexión de NAS o múltiples conexiones de NAS del mismo grupo de procedimientos de NAS. Por ejemplo, si el valor de TROCEO se deriva basándose en un ID de sesión de PDU de UE, entonces la clave vástago de NAS derivada de ese valor de TROCEO solo se aplicará a una conexión de NAS que porta ese ID de sesión de PDU. Por otra
10 parte, si el valor de TROCEO se deriva basándose en una S-NSSAI, entonces la clave vástago de NAS derivada de ese valor de TROCEO será común entre las conexiones de NAS asociadas con esa S-NSSAI. En este último caso, incluso aunque la clave vástago de NAS devuelta desde la SKMF a cada NF central será la misma, los identificadores de clave vástago de NAS para las claves vástago
15 de NAS serán singulares entre diferentes NF. La razón de esto es que, aunque las claves vástago de NAS son las mismas inicialmente cuando son asignadas por la SKMF, cada NF puede ejecutar independientemente una derivación de clave horizontal de su clave vástago de NAS que dará como resultado que se deriven nuevas claves vástago de NAS y, por lo tanto, singulares entre sí, y para
20 que el UE sea capaz de distinguir estas claves vástago de NAS, es necesario que las mismas tengan un identificador de clave vástago de NAS singular.

Si un valor de TROCEO se deriva de una combinación de un ID de sesión de PDU y una S-NSSAI, entonces la clave vástago de NAS derivada de ese valor de TROCEO se dedicaría a una conexión de NAS específica asociada con esa
25 sesión de PDU dentro de esa S-NSSAI. El valor de TROCEO y los conceptos de

clave/identificador vástago de NAS proporcionan un mecanismo potente, flexible y ampliable para derivar de forma dinámica claves de seguridad basándose en requisitos de seguridad.

Para que un UE obtenga servicios a partir de una red, el UE se debe registrar en primer lugar en la red, por lo que el UE y la red se autentican entre sí, y si tiene éxito, el UE está autorizado a usar los servicios ofrecidos por la red basándose en su abono. Como parte del procedimiento de registro, el UE realiza el procedimiento de AKA que da como resultado que el UE y la red deriven la clave de anclaje. Posteriormente, las claves progenitoras de NAS también se derivan independientemente en el UE y la SKMF a partir de la clave de anclaje, SUPI y el/los indicador(es) de NAS.

El mecanismo por el que se establece un contexto de seguridad entre un UE y la red para una conexión de NAS en general sigue un procedimiento común. En primer lugar, la NF central que recibe el mensaje de NAS inicial creará un valor de TROCEO y enviará una solicitud a la SKMF para derivar una clave vástago de NAS. Si tiene éxito, la SKMF devolverá la clave vástago de NAS derivada y el identificador de clave vástago de NAS a la NF central. La NF central usará el mismo valor de TROCEO y la clave vástago de NAS recibida para generar parámetros de seguridad que se van a usar en un procedimiento de orden de modo de seguridad de NAS hacia el UE. La recepción del procedimiento de orden de modo de seguridad de NAS desencadena que el UE derive una clave vástago de NAS y que asigne el identificador vástago de NAS recibido desde la NF central a la misma. Si tiene éxito, tanto el UE como la NF central tendrán los mismos clave vástago de NAS e identificadores de clave vástago de NAS que se usan junto con algoritmos de integridad y cifrado de NAS

acordados para proteger en cuanto a su integridad y cifrar la conexión de NAS entre el UE y la NF central.

La figura 10 es otro flujo de llamada ilustrativo para asegurar múltiples conexiones de NAS de acuerdo con algunas realizaciones de la presente divulgación, que describe un escenario en el que el UE se registra con la red y establece una conexión de NAS para procedimientos de gestión de movilidad de NAS y, posteriormente, solicita otra conexión de NAS para procedimientos de gestión de sesión de NAS. Este flujo de llamada explica cómo se protegen estas conexiones de NAS.

En la etapa 1, el UE inicia una solicitud de registro con una red seleccionada y envía un mensaje de NAS inicial (por ejemplo, solicitud de registro de MM de NAS) en claro, es decir, no protegido en cuanto a su seguridad, con los elementos de información obligatorios mínimos (por ejemplo, identificador oculto de abono (SUCI)/ID temporal, capacidades de seguridad de UE, identificador de clave de anclaje, indicador de NAS) para posibilitar que la red procese la solicitud. El UE también proporciona el indicador de NAS y el identificador temporal derivado (MM-GUTI) a las capas inferiores (por ejemplo, RRC) para posibilitar que la (R)AN tome decisiones acerca del descubrimiento y selección de una NF central adecuada para este procedimiento de NAS. En este ejemplo, se selecciona la NF n.º 1. El valor del indicador de NAS indicará procedimientos de gestión de movilidad de NAS.

En la etapa 2, la NF n.º 1 determina, basándose en la solicitud de registro de NAS recibida, que se requiere autenticación de UE debido a que, por ejemplo, el identificador de clave de anclaje indica que no existe una clave de anclaje válida, o se recibe el SUCI, o el identificador temporal es no válido o no se halla.

Entonces, la NF n.º 1 envía una solicitud de autenticación a la SKMF que incluye el SUCI, el Id de red de servicio y el indicador de NAS.

En la etapa 3, la SKMF desencadena el procedimiento de AKA primario con el UE, que si tiene éxito da como resultado lo siguiente:

- 5 • El UE y la SKMF derivan y almacenan independientemente una clave de anclaje;
 - La SKMF deriva y almacena un identificador de clave de anclaje que identifica la clave de anclaje y proporciona esta al UE que almacena la misma;
 - Independientemente, cada uno del UE y la SKMF derivará claves
- 10 progenitoras de NAS usando la clave de anclaje y valores de indicador de NAS normalizados para la separación de claves, y almacenarán los mismos.
 - Independientemente, cada uno del UE y la SKMF derivará uno(s)
- 15 identificador(es) de clave progenitora de NAS usando el identificador de clave de anclaje y valores de indicador de NAS normalizados para la separación de identificadores, y almacenarán los mismos.
 - Después de que se hayan derivado y almacenado las claves progenitoras de NAS y los identificadores progenitores de NAS, la clave de anclaje se borra del UE y la SKMF, y el identificador de clave de anclaje permanece tanto en el UE como en la SKMF.
- 20 Nota: El procedimiento de AKA necesita una potenciación para dar cabida a la clave progenitora de NAS y la derivación de identificadores de clave progenitora de NAS.

En la etapa 4, la SKMF devuelve una respuesta de autenticación a la NF n.º 1 que contiene el identificador de clave de anclaje y el identificador de clave progenitora de NAS asociado con el indicador de NAS proporcionado en la

25

solicitud de autenticación.

En la etapa 5, la NF n.º 1 envía una solicitud de clave para esta conexión de NAS a la SKMF que contiene el identificador de clave de anclaje recibido, el identificador de clave progenitora de NAS y, opcionalmente, un valor de TROCEO. La NF n.º 1 puede usar información preconfigurada y la información proporcionada por el UE para determinar qué parámetros (por ejemplo, S-NSSAI-x, ID de CONJUNTO de NF, etc.) se usan como entrada para generar el valor de TROCEO.

En algunos escenarios, la clave vástago de NAS es beneficiosa para procedimientos de MM (por ejemplo, movilidad de una función de MM a otra, registro dual con funciones de MM en paralelo). Sin embargo, en otros escenarios, la clave vástago de NAS se podría considerar opcional. En este flujo de llamada, se supone la necesidad de la clave vástago de NAS para fines ilustrativos, pero no es obligatorio para procedimientos de MM con terminaciones de NAS distribuida.

En la etapa 6, la SKMF usa el identificador de clave de anclaje para comprobar que está asociado con una ejecución de AKA actual y válida, y usa el identificador de clave de anclaje y el identificador de clave progenitora de NAS para identificar la clave progenitora de NAS. Si se recibe el valor de TROCEO, la SKMF puede usar el mismo y la clave progenitora de NAS para derivar una clave vástago de NAS y un identificador de clave vástago de NAS. Entonces, la SKMF puede devolver a la NF n.º 1 la clave vástago de NAS derivada, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS, si se recibe el valor de TROCEO. Si no se recibe el valor de TROCEO, la SKMF puede devolver a la NF n.º 1 la clave progenitora de NAS identificada.

En algunas realizaciones, se puede optimizar la señalización entre la NF n.º 1 y la SKMF. En el presente caso, la NF n.º 1 se refiere a cualquier NF que maneje procedimientos de gestión de movilidad de NAS.

5 En algunas realizaciones, se pueden quitar los mensajes de solicitud y respuesta de clave entre la NF n.º 1 y la SKMF. El mensaje de solicitud de autenticación puede desencadenar implícitamente que la SKMF devuelva, en la respuesta de autenticación, ciertas claves e identificadores de clave asociados a la NF n.º 1, lo que optimizaría la carga de señalización quitando el mensaje de solicitud/respuesta de clave explícito.

10 Esto se puede lograr como sigue:

- La SKMF determina implícitamente el indicador de NAS asociado con una solicitud de autenticación debido a que este siempre está asociado con un procedimiento de gestión de movilidad de NAS que tendrá su propio valor de indicador de NAS normalizado, es decir, sin necesidad de incluir el indicador de

15 NAS en la solicitud de autenticación;

- La SKMF usa el indicador de NAS para derivar la clave progenitora de NAS a partir de la clave de anclaje y SUPI;

- La SKMF deriva el identificador de clave progenitora de NAS de la forma normal, por ejemplo, usando un valor de indicador de NAS;

20 • La SKMF devuelve la clave progenitora de NAS y el identificador de clave progenitora de NAS en la respuesta de autenticación a la NF n.º 1, si no se proporciona ningún valor de TROCEO;

- Si se requiere una clave vástago de NAS, entonces la solicitud de autenticación podría contener el valor de TROCEO, lo que permitiría que la

25 SKMF derivara y devolviera la clave vástago de NAS y el identificador de clave

vástago de NAS a la NF n.º 1.

En algunas realizaciones, se pueden coubicar la NF n.º 1 y la SKMF. La NF n.º 1 y la SKMF se pueden desplegar como coubicadas como una única NF, lo que significa que las interacciones entre las mismas son internas a la NF.

- 5 En algunas realizaciones, si la SKMF se despliega como una NF autónoma, los procedimientos de AKA que esta ejecuta hacia el UE pueden ser indirectos a través de la NF n.º 1 o directos, sorteando la NF n.º 1.

- 10 En la etapa 7, a partir de una lista configurada y priorizada de algoritmos de integridad y cifrado de NAS soportados, la NF n.º 1 selecciona los algoritmos de integridad y cifrado de NAS de la prioridad más alta soportados por el UE basándose en capacidades de seguridad de UE recibidas en la etapa 1. La NF n.º 1 usa los identificadores de algoritmos de integridad y cifrado de NAS seleccionados y la clave vástago de NAS o clave progenitora de NAS recibida desde la SKMF para derivar una clave de integridad de NAS y una clave de
15 cifrado de NAS.

- 20 La NF n.º 1 crea y envía un mensaje de orden de modo de seguridad de NAS al UE e inicia un recuento de enlace descendente (DL) de NAS para esta conexión de NAS que se inicializa a cero. El mensaje de orden de modo de seguridad de NAS puede contener el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, el valor de TROCEO, las capacidades de seguridad de UE, los algoritmos de integridad y cifrado de NAS seleccionados, una bandera que solicita que el mensaje de NAS inicial completo (por ejemplo, solicitud de registro de NAS) se devuelva en el mensaje de modo de seguridad de NAS completo. El mensaje de
25 orden de modo de seguridad de NAS se protege en cuanto a su integridad por la

clave de integridad de NAS.

Además, la NF n.º 1 puede almacenar en su contexto de seguridad de NAS para esta conexión de NAS la siguiente información: el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago de NAS, el valor de TROCEO, las capacidades de seguridad de UE, los algoritmos de integridad y cifrado de NAS seleccionados, las claves de integridad y cifrado de NAS y los recuentos de UL/DL de NAS.

En la etapa 8, a partir del mensaje de orden de modo de seguridad de NAS recibido, el UE puede usar el identificador de clave de anclaje para comprobar que está asociado con una ejecución de AKA actual y válida, y usar el identificador de clave de anclaje y el identificador de clave progenitora de NAS para identificar la clave progenitora de NAS. Si se reciben el valor de TROCEO y el identificador de clave vástago de NAS, el UE puede usar el valor de TROCEO y la clave progenitora de NAS para derivar una clave vástago de NAS, y asignar el identificador de clave vástago de NAS recibido a la clave vástago de NAS derivada. Entonces, el UE puede usar o bien la clave progenitora de NAS o bien la clave vástago de NAS e identificadores de algoritmos de integridad y cifrado de NAS seleccionados para derivar las claves de integridad y cifrado de NAS. Además, el UE puede usar la clave de integridad de NAS y el algoritmo de integridad de NAS para comprobar la integridad del mensaje de orden de modo de seguridad de NAS recibido. Asimismo, el UE puede comprobar las capacidades de seguridad de UE para asegurar que no ha tenido lugar un ataque de oferta a la baja.

Si se superan todas las comprobaciones, el UE puede generar un mensaje

de modo de seguridad de NAS completo que incluye la solicitud de registro completo (lo que es desencadenado por la bandera recibida en el mensaje de orden de modo de seguridad de NAS). Entonces, el UE puede cifrar y proteger en cuanto a su integridad el mensaje de modo de seguridad de NAS completo con los algoritmos de integridad y cifrado de NAS seleccionados y las claves de integridad y cifrado de NAS. El UE también puede preparar un contador de enlace ascendente (UL) de NAS inicializado a cero para esta conexión de NAS. Entonces, el UE envía el mensaje de modo de seguridad de NAS completo a la NF n.º 1.

Además, el UE puede almacenar en su contexto de seguridad de NAS para esta conexión de NAS la siguiente información: el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago de NAS, el valor de TROCEO, las capacidades de seguridad de UE, los algoritmos de integridad y cifrado de NAS seleccionados, las claves de integridad y cifrado de NAS y los recuentos de UL/DL de NAS.

En la etapa 9, la integridad de la NF n.º 1 comprueba y descifra el mensaje de modo de seguridad de NAS completo recibido usando los algoritmos de integridad y cifrado de NAS seleccionados y las claves de integridad y cifrado de NAS. Si tiene éxito, se procesa el mensaje de NAS inicial completo recién recibido (por ejemplo, solicitud de registro de NAS) y se devuelve una respuesta de registro de NAS al UE que contiene un identificador de contexto temporal de UE (MM-GUTI) para esta conexión de NAS.

El identificador de MM-GUTI (o su versión abreviada MM-S-TMSI) identifica de forma singular el contexto de MM de un UE dentro de una NF y la

propia NF. Un contexto de MM de UE contiene, entre otra información, el contexto de seguridad de NAS para las conexiones de NAS de MM de un UE. Obsérvese que la parte de MM de MM-GUTI/MM-S-TMSI indica que el contexto está relacionado con un procedimiento de gestión de movilidad (del cual el registro es una parte). Un contexto de UE para un procedimiento de gestión de sesión (SM) de NAS se puede identificar mediante SM-GUTI/SM-S-TMSI.

Para procedimientos de gestión de movilidad de NAS posteriores en relación con esta conexión de NAS, los mensajes de NAS contendrán el identificador temporal de MM-GUTI/MM-S-TMSI para habilitar la identificación de la NF de servicio y el contexto de UE almacenado dentro de esa NF.

Todos los mensajes de NAS posteriores para esta conexión de NAS entre el UE y la NF n.º 1 se protegen en cuanto a su integridad y se cifran usando los parámetros/claves de seguridad comunes almacenados en los contextos de seguridad de NAS almacenados tanto en el UE como en la NF n.º 1.

En la etapa 10, posteriormente a un registro de red con éxito, el UE puede iniciar una nueva conexión de NAS, por ejemplo, para iniciar el establecimiento de una sesión de PDU usando procedimientos de gestión de sesión de NAS. De forma similar a la etapa 1, el mensaje de NAS inicial se envía en claro con los Elementos de Información obligatorios mínimos para posibilitar que la red procese la solicitud, y la (R)AN usará los parámetros de indicador de NAS, MM-GUTI/MM-S-TMSI, S-NSSAI-y proporcionados por el UE a las capas inferiores para asistir en la selección de una NF central adecuada para procesar procedimientos de gestión de sesión de NAS. En este caso, el indicador de NAS mostrará que la solicitud es para procedimientos de gestión de sesión de NAS y la (R)AN seleccionará una NF central que soporta esos procedimientos. En este

ejemplo, la NF central es la NF n.º n. El mecanismo por el que la (R)AN puede seleccionar una NF central adecuada puede incluir usar el indicador de NAS como una clave de consulta en una tabla configurada localmente de NF o consultar una función de repositorio de red (NRF).

5 En una realización, el mensaje de NAS inicial para procedimientos de gestión de sesión de NAS puede incluir: el MM-GUTI, el identificador de clave de anclaje, el identificador de clave progenitora de NAS asociado con el indicador de NAS para procedimientos de gestión de sesión de NAS, y el indicador de NAS.

10 En la etapa 11, la NF n.º n puede usar el MM-GUTI/MM-S-TMSI recibido para confirmar que el UE se ha registrado con éxito con la red enviando una solicitud a la NF n.º 1 que se identifica a partir del parámetro de MM-GUTI/MM-S-TMSI. El MM-GUTI/MM-S-TMSI se puede proporcionar a la NF n.º 1 para identificar el contexto de UE que la NF n.º 1 ha almacenado para el UE.

15 En la etapa 12, si el UE se confirma como registrado con éxito, la NF n.º 1 puede devolver una respuesta de éxito que también incluye las capacidades de seguridad de UE a la NF n.º n.

 En la etapa 13, la NF n.º n envía una solicitud de clave para esta conexión de NAS a la SKMF que contiene el identificador de clave de anclaje recibido, el
20 identificador de clave progenitora de NAS y, opcionalmente, un valor de TROCEO. En una realización, la NF n.º n puede usar información preconfigurada y la información proporcionada por el UE para determinar qué parámetros (por ejemplo, S-NSSAI-y, ID de CONJUNTO de NF, etc.) se usan como entrada para generar el valor de TROCEO.

25 En la etapa 14, la SKMF usa el identificador de clave de anclaje para

comprobar que está asociado con una ejecución de AKA actual y válida, y usa el identificador de clave de anclaje y el identificador de clave progenitora de NAS para identificar la clave progenitora de NAS. Si se recibe el valor de TROCEO, la SKMF puede usar el mismo y la clave progenitora de NAS para derivar una clave vástago de NAS y un identificador de clave vástago de NAS. Entonces, la SKMF puede devolver a la NF n.º n la clave vástago de NAS derivada, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS, si se recibe el valor de TROCEO. Si no se recibe el valor de TROCEO, la SKMF puede devolver a la NF n.º n la clave progenitora de NAS identificada.

En la etapa 15, a partir de una lista configurada y priorizada de algoritmos de integridad y cifrado de NAS soportados, la NF n.º n puede seleccionar los algoritmos de integridad y cifrado de NAS de la prioridad más alta soportados por el UE basándose en las capacidades de seguridad de UE recibidas. La NF n.º n usa los identificadores de algoritmos de integridad y cifrado de NAS seleccionados y la clave vástago de NAS o clave progenitora de NAS recibida desde la SKMF para derivar una clave de integridad de NAS y una clave de cifrado de NAS.

Entonces, la NF n.º n puede crear y enviar un mensaje de orden de modo de seguridad de NAS al UE e inicia un recuento de DL de NAS para esta conexión de NAS que se inicializa a cero. El mensaje de orden de modo de seguridad de NAS puede contener el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, el valor de TROCEO, las capacidades de seguridad de UE, los algoritmos de integridad y cifrado de NAS seleccionados, una bandera que solicita que el mensaje de NAS inicial completo (por ejemplo, solicitud de sesión de PDU de NAS) se envíe en el

mensaje de modo de seguridad de NAS completo. El mensaje de orden de modo de seguridad de NAS se protege en cuanto a su integridad por la clave de integridad de NAS.

Además, la NF n.^o n puede almacenar en su contexto de seguridad de NAS para esta conexión de NAS la siguiente información: el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago de NAS, el valor de TROCEO, las capacidades de seguridad de UE, los algoritmos de integridad y cifrado de NAS seleccionados, las claves de integridad y cifrado de NAS y los recuentos de UL/DL de NAS.

En la etapa 16, a partir del mensaje de orden de modo de seguridad de NAS recibido, el UE puede usar el identificador de clave de anclaje para comprobar que está asociado con una ejecución de AKA actual y válida, y usar el identificador de clave de anclaje y el identificador de clave progenitora de NAS para identificar la clave progenitora de NAS. Si se reciben el valor de TROCEO y el identificador de clave vástago de NAS, el UE puede usar el valor de TROCEO y la clave progenitora de NAS para derivar una clave vástago de NAS, y asignar el identificador de clave vástago de NAS recibido a la clave vástago de NAS derivada. Entonces, el UE puede usar o bien la clave progenitora de NAS o bien la clave vástago de NAS e identificadores de algoritmos de integridad y cifrado de NAS seleccionados para derivar las claves de integridad y cifrado de NAS. Además, el UE puede usar la clave de integridad de NAS y el algoritmo de integridad de NAS para comprobar la integridad del mensaje de orden de modo de seguridad de NAS recibido. Asimismo, el UE puede comprobar las capacidades de seguridad de UE para asegurar que no ha tenido lugar un ataque

de oferta a la baja.

Si se superan todas las comprobaciones, el UE puede generar un mensaje de modo de seguridad de NAS completo que incluye el mensaje de NAS inicial completo (por ejemplo, solicitud de sesión de PDU de NAS), lo que es desencadenado por la bandera recibida en el mensaje de orden de modo de seguridad de NAS. Entonces, el UE puede cifrar y proteger en cuanto a su integridad el mensaje de modo de seguridad de NAS completo con los algoritmos de integridad y cifrado de NAS seleccionados y las claves de integridad y cifrado de NAS. El UE también puede preparar un contador de enlace ascendente (UL) de NAS inicializado a cero para esta conexión de NAS. Entonces, el UE envía el mensaje de modo de seguridad de NAS completo a la NF n.º n.

Además, el UE puede almacenar en su contexto de seguridad de NAS para esta conexión de NAS la siguiente información: el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago de NAS, el valor de TROCEO, las capacidades de seguridad de UE, los algoritmos de integridad y cifrado de NAS seleccionados, las claves de integridad y cifrado de NAS y los recuentos de UL/DL de NAS.

En la etapa 17, la integridad de la NF n.º n comprueba y descifra el mensaje de modo de seguridad de NAS completo recibido usando los algoritmos de integridad y cifrado de NAS seleccionados y las claves de integridad y cifrado de NAS. Si tiene éxito, se procesa el mensaje de NAS inicial completo recién recibido (por ejemplo, solicitud de sesión de PDU de NAS) y se devuelve una respuesta de sesión de PDU de NAS al UE que contiene un identificador de contexto temporal de UE (SM-GUTI) para esta conexión de NAS.

El identificador de SM-GUTI (o su versión abreviada SM-S-TMSI) identifica de forma singular el contexto de SM de un UE en términos de la NF en la que está ubicado el mismo y el contexto de SM de UE dentro de esa NF. Un contexto de SM de UE contiene, entre otra información, el contexto de seguridad de NAS para las conexiones de NAS de SM de un UE. Obsérvese que la parte
5 de SM de SM-GUTI/SM-S-TMSI indica que el contexto está relacionado con un procedimiento de gestión de sesión de NAS.

Para procedimientos de gestión de sesión de PDU de NAS posteriores en esta conexión de NAS, los mensajes de NAS contendrán el identificador temporal
10 de SM-GUTI/SM-S-TMSI para habilitar la identificación de la NF de servicio y el contexto de UE almacenado dentro de esa NF.

Todos los mensajes de NAS posteriores para esta conexión de NAS entre el UE y la NF n.^o n se protegen en cuanto a su integridad y se cifran usando los parámetros/claves de seguridad comunes almacenados en los contextos de
15 seguridad de NAS almacenados tanto en el UE como en la NF n.^o n.

Obsérvese que la clave vástago de NAS y el identificador de clave vástago de NAS y el valor de TROCEO se requieren primariamente en donde existe una necesidad de separación de clave entre conexiones de NAS que están manejando los mismos procedimientos de NAS, por ejemplo, dos o más
20 conexiones de NAS que manejan procedimientos de SM de NAS. En donde no se requiere tal separación de clave, por ejemplo, una única conexión de NAS para procedimientos de MM de NAS, se pueden usar la clave progenitora de NAS y el identificador de clave progenitora de NAS. Si hay dos conexiones de NAS que manejan los mismos procedimientos de NAS, entonces no se pueden
25 usar la clave progenitora de NAS y el identificador de clave progenitora de NAS

y se deben usar la clave vástago de NAS y el identificador de clave vástago de NAS.

Cuando no se usan una clave vástago de NAS y un identificador de clave vástago de NAS, es decir, la clave progenitora de NAS y el identificador de clave progenitora de NAS se usan para asegurar una conexión de NAS, el valor de TROCEO, la clave vástago de NAS y los identificadores de clave vástago de NAS no se derivan/distribuyen en el UE y la red. La decisión de si se derivan, o no, una clave vástago de NAS y un identificador de clave vástago de NAS depende de la configuración de la NF central que termina la conexión de NAS.

Si la NF central está configurada para proporcionar un valor de TROCEO al SKMF/UE para la derivación de clave, se derivan y se usan una clave vástago de NAS y un identificador de clave vástago de NAS, de lo contrario no se deriva ninguna clave vástago de NAS ni ningún identificador de clave vástago de NAS y, en su lugar, se usan la clave progenitora de NAS y el identificador de clave progenitora de NAS.

Se describirán más detalles de las realizaciones de ejemplo de acuerdo con la presente divulgación con referencia a las figuras 11 a 13.

La figura 11 es un diagrama de flujo que representa un método 1100 para la seguridad en la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación. El método 1100 puede ser realizado por un dispositivo terminal tal como un UE para manejar la seguridad de múltiples conexiones de NAS en la arquitectura de terminaciones de NAS distribuida.

Como se muestra en la figura 11, el dispositivo terminal genera una clave de anclaje, por ejemplo, con una entidad de red configurada para implementar la

función de gestión de claves de seguridad (SKMF) (denominada, en lo sucesivo en el presente documento, entidad de SKMF, que se puede usar de forma intercambiable con SKMF en el presente documento), en el bloque 1110. En algunas realizaciones, el dispositivo terminal y la entidad de SKMF pueden
5 realizar un procedimiento de AKA primario para generar la clave de anclaje.

En el bloque 1120, el dispositivo terminal recibe un identificador de clave de anclaje para la clave de anclaje desde la entidad de SKMF. Como se ha mencionado anteriormente, el identificador de clave de anclaje se puede usar para identificar la clave de anclaje.

10 En el bloque 1130, el dispositivo terminal deriva un conjunto de claves progenitoras de NAS basándose en la clave de anclaje, un identificador de abono e indicadores de NAS que indican diferentes procedimientos de NAS. En algunas realizaciones, el identificador de abono puede ser un SUPI. Como se ha mencionado anteriormente, el indicador de NAS puede tener diferentes valores
15 para indicar diferentes procedimientos de NAS. Por lo tanto, el dispositivo terminal puede obtener múltiples claves progenitoras de NAS basándose en la clave de anclaje, el identificador de abono (por ejemplo, SUPI) y diferentes valores del indicador de NAS.

Entonces, en el bloque 1140, el dispositivo terminal obtiene un
20 identificador de clave progenitora de NAS para cada una del conjunto de claves progenitoras de NAS. En algunas realizaciones, el dispositivo terminal puede derivar el identificador de clave progenitora de NAS para la clave progenitora de NAS basándose en el indicador de NAS sobre el cual se deriva la clave progenitora de NAS. En algunas realizaciones, los identificadores de clave
25 progenitora de NAS asociados con las claves progenitoras de NAS se pueden

recibir desde la entidad de SKMF y, por lo tanto, no es necesario que el dispositivo terminal derive los identificadores de clave progenitora de NAS.

En algunas realizaciones, el identificador de clave progenitora de NAS asociado con una clave progenitora de NAS puede tener el mismo valor que el
5 indicador de NAS basándose en el cual se deriva la clave progenitora de NAS. En algunas realizaciones, al identificador de clave progenitora de NAS le puede ser asignado un valor singular por la entidad de SKMF.

Por lo tanto, una clave progenitora de NAS se puede identificar mediante una combinación del identificador de clave de anclaje y el identificador de clave
10 progenitora de NAS.

Adicionalmente, en algunas realizaciones, el dispositivo terminal puede almacenar el identificador de clave de anclaje, las claves progenitoras de NAS y los identificadores de clave progenitora de NAS asociados. Además, la clave de anclaje se puede quitar del dispositivo terminal.

Adicionalmente, en algunas realizaciones, el dispositivo terminal puede solicitar el establecimiento de una primera conexión de NAS que porta un primer procedimiento de NAS entre el dispositivo terminal y una primera entidad de red central que está configurada para implementar una función de red central. Como se usan en el presente documento, las expresiones "entidad de red central" y
15 "función de red central" se pueden usar de forma intercambiable. En algunas realizaciones, el dispositivo terminal puede enviar una primera solicitud de conexión de NAS a la primera entidad de red central que implementa una función de red central. En algunas realizaciones, la primera solicitud de conexión de NAS puede comprender el identificador de clave de anclaje y el indicador de NAS que
20 indica el primer procedimiento de NAS, entre otra información. En una
25

realización, la primera solicitud de conexión de NAS puede ser un mensaje de NAS inicial, por ejemplo, solicitud de registro de gestión de movilidad de NAS, y el primer procedimiento de NAS pueden ser procedimientos de gestión de movilidad de NAS y, por lo tanto, la primera entidad de red central puede ser una

5 NF que soporta procedimientos de gestión de movilidad.

Entonces, el dispositivo terminal puede determinar una clave de NAS para la primera conexión de NAS basándose en información relacionada con seguridad asociada con el primer procedimiento de NAS desde la primera entidad de red central. En alguna realización, la información relacionada con

10 seguridad se puede recibir en un mensaje de orden de modo de seguridad de NAS. En algunas realizaciones, la información relacionada con seguridad puede incluir el identificador de clave de anclaje, el identificador de clave progenitora de NAS, capacidades de seguridad de UE, algoritmos de integridad y cifrado de NAS seleccionados, y una bandera que solicita que se envíe un mensaje de NAS

15 inicial completo. En este caso, el dispositivo terminal puede identificar la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS, y determinar que la clave de NAS es la clave progenitora de NAS identificada debido a que no se proporciona ningún valor de TROCEO. En algunas realizaciones, la información relacionada con

20 seguridad puede incluir además el valor de TROCEO y el identificador de clave vástago de NAS. En este caso, después de identificar la clave progenitora de NAS, el dispositivo terminal puede derivar una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO, y asignar el identificador de clave vástago de NAS recibido a la clave vástago de NAS.

25 Entonces, la clave vástago de NAS se determina como la clave de NAS para la

primera conexión de NAS. La clave vástago de NAS se puede identificar mediante una combinación del identificador de clave de anclaje, el identificador de clave progenitora de NAS y el identificador de clave vástago de NAS.

Además, en algunas realizaciones, el dispositivo terminal puede derivar
5 claves de integridad y cifrado de NAS basándose en la clave de NAS y los algoritmos de integridad y cifrado de NAS seleccionados, y generar un mensaje de modo de seguridad de NAS completo que incluye el mensaje de NAS inicial completo. Entonces, el dispositivo terminal puede cifrar y proteger en cuanto a
10 su integridad el mensaje de modo de seguridad de NAS completo y enviar el mismo a la primera entidad de red central. Además, en algunas realizaciones, el dispositivo terminal puede almacenar un contexto de seguridad de NAS para la primera conexión de NAS. El contexto de seguridad de NAS puede incluir el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago de NAS, el valor de
15 TROCEO, las capacidades de seguridad del dispositivo terminal, los algoritmos de integridad y cifrado de NAS seleccionados, las claves de integridad y cifrado de NAS y los recuentos de NAS. Además, el dispositivo terminal puede recibir un identificador de contexto temporal para la primera conexión de NAS desde la primera entidad de red central. El identificador de contexto temporal se puede
20 usar para identificar el contexto de seguridad de NAS del dispositivo terminal dentro de la primera entidad de red central y la propia primera entidad de red central.

Como alternativa, en algunas realizaciones, el dispositivo terminal puede (re)generar la clave de anclaje después de la solicitud de establecimiento de la
25 primera conexión de NAS desde la primera entidad de red central.

Adicionalmente, en algunas realizaciones, el dispositivo terminal puede solicitar el establecimiento de una segunda conexión de NAS que porta un segundo procedimiento de NAS entre el dispositivo terminal y una segunda entidad de red central. En algunas realizaciones, el dispositivo terminal puede enviar una segunda solicitud de conexión de NAS a la segunda entidad de red central. En algunas realizaciones, la segunda solicitud de conexión de NAS puede comprender el identificador de clave de anclaje y el indicador de NAS que indica el segundo procedimiento de NAS, entre otra información. En una realización, la segunda solicitud de conexión de NAS también puede ser un mensaje de NAS inicial, por ejemplo, una solicitud de sesión de PDU de NAS, y el segundo procedimiento de NAS pueden ser procedimientos de gestión de sesión de NAS, y la segunda entidad de red central puede ser una NF que soporta procedimientos de gestión de sesión.

Entonces, el dispositivo terminal puede determinar una clave de NAS para la segunda conexión de NAS basándose en información relacionada con seguridad asociada con el segundo procedimiento de NAS recibida desde la segunda entidad de red central. En algunas realizaciones, la información relacionada con seguridad se puede incluir en un mensaje de orden de modo de seguridad de NAS. En algunas realizaciones, la información relacionada con seguridad asociada con el segundo mensaje de procedimiento de NAS relacionada con seguridad puede incluir el identificador de clave de anclaje, el identificador de clave progenitora de NAS, capacidades de seguridad de UE, algoritmos de integridad y cifrado de NAS seleccionados, y una bandera que solicita que se envíe un mensaje de NAS inicial completo. En este caso, el dispositivo terminal puede identificar la clave progenitora de NAS basándose en

el identificador de clave de anclaje y el identificador de clave progenitora de NAS, y determinar que la clave de NAS es la clave progenitora de NAS identificada debido a que no se proporciona ningún valor de TROCEO. En algunas realizaciones, la información relacionada con seguridad asociada con el segundo
5 procedimiento de NAS puede incluir además el valor de TROCEO y el identificador de clave vástago de NAS. En este caso, después de identificar la clave progenitora de NAS, el dispositivo terminal puede derivar una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO, y asignar el identificador de clave vástago de NAS recibido a la
10 clave vástago de NAS. Entonces, la clave vástago de NAS se determina como la clave de NAS para la segunda conexión de NAS.

Además, en algunas realizaciones, el dispositivo terminal puede derivar claves de integridad y cifrado de NAS basándose en la clave de NAS y los algoritmos de integridad y cifrado de NAS seleccionados, y generar un mensaje
15 de modo de seguridad de NAS completo que incluye el mensaje de NAS inicial completo. Entonces, el dispositivo terminal puede cifrar y proteger en cuanto a su integridad el mensaje de modo de seguridad de NAS completo y enviar el mismo a la segunda entidad de red central. Además, en algunas realizaciones, el dispositivo terminal puede almacenar un contexto de seguridad de NAS para
20 la segunda conexión de NAS. Además, el dispositivo terminal puede recibir el identificador de contexto temporal para la segunda conexión de NAS desde la primera entidad de red central.

Aunque se proporcionan solo dos conexiones de NAS que portan diferentes procedimientos de NAS como un ejemplo para explicar el método
25 1100, los expertos en la materia apreciarán que el método 1100 puede ser

aplicable a más de dos conexiones de NAS.

Adicionalmente, en algunas realizaciones, el primer procedimiento de NAS y el segundo procedimiento de NAS son el mismo procedimiento de NAS o diferentes procedimientos de NAS, y la primera función de red central es diferente de la segunda función de red central. Obsérvese que, si el primer procedimiento de NAS son procedimientos de gestión de movilidad de NAS, el segundo procedimiento de NAS solo pueden ser procedimientos no de gestión de movilidad de NAS. El primer procedimiento de NAS y el segundo procedimiento de NAS pueden ser los mismos procedimientos no de gestión de movilidad de NAS.

La figura 12 es un diagrama de flujo que representa un método 1200 para la seguridad en la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación. El método 1200 puede ser realizado por la entidad de SKMF.

Como se muestra en la figura 12, la entidad de SKMF puede generar una clave de anclaje con un dispositivo terminal, por ejemplo, el UE en la arquitectura de terminaciones de NAS distribuida, en el bloque 1210. En algunas realizaciones, la entidad de SKMF y el dispositivo terminal pueden realizar un procedimiento de AKA primario para generar la clave de anclaje.

En el bloque 1220, la entidad de SKMF puede derivar un identificador de clave de anclaje para la clave de anclaje, y enviar el identificador de clave de anclaje al dispositivo terminal. Entonces, en el bloque 1230, la entidad de SKMF puede derivar un conjunto de claves progenitoras de NAS basándose en la clave de anclaje, un identificador de abono e indicadores de NAS que indican un procedimiento de NAS diferente. En algunas realizaciones, el identificador de

abono puede ser un SUPI. Como se ha mencionado anteriormente, el indicador de NAS puede tener diferentes valores para indicar diferentes procedimientos de NAS. Por lo tanto, la entidad de SKMF puede obtener múltiples claves progenitoras de NAS basándose en la clave de anclaje, el identificador de abono
5 (por ejemplo, SUPI) y diferentes valores del indicador de NAS.

En el bloque 1240, la entidad de SKMF puede derivar, para cada una del conjunto de claves progenitoras de NAS, un identificador de clave progenitora de NAS basándose en el indicador de NAS respectivo. Por lo tanto, la clave progenitora de NAS se puede identificar mediante una combinación del
10 identificador de clave de anclaje y el identificador de clave progenitora de NAS. En algunas realizaciones, el identificador de clave progenitora de NAS asociado con una clave progenitora de NAS puede tener el mismo valor que el indicador de NAS basándose en el cual se deriva la clave progenitora de NAS.

Como alternativa o adicionalmente, en algunas realizaciones, la entidad
15 de SKMF puede enviar los identificadores de clave progenitora de NAS al dispositivo terminal, de tal modo que el dispositivo terminal puede no derivar él mismo los identificadores de clave progenitora de NAS. Como alternativa, en algunas realizaciones, la entidad de SKMF puede asignar el identificador de clave progenitora de NAS con un valor singular, y enviar el identificador de clave
20 progenitora de NAS con el valor y el indicador de NAS asociado al dispositivo terminal.

Adicionalmente, en algunas realizaciones, la entidad de SKMF puede almacenar el identificador de clave de anclaje, las claves progenitoras de NAS y los identificadores de clave progenitora de NAS asociados. Además, la clave de
25 anclaje se puede quitar de la entidad de SKMF.

Adicionalmente, en algunas realizaciones, la entidad de SKMF puede recibir, desde una primera entidad de red central, una primera solicitud de una clave de NAS para una primera conexión de NAS que porta un primer procedimiento de NAS. Entonces, la entidad de SKMF puede determinar la clave de NAS para la primera conexión de NAS basándose en la primera solicitud, y enviar la clave de NAS para la primera conexión de NAS a la primera entidad de red central.

En algunas realizaciones, la primera solicitud puede comprender el identificador de clave de anclaje y el identificador de clave progenitora de NAS. En este caso, la entidad de SKMF puede determinar la clave de NAS al identificar la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS recibidos en la primera solicitud, y determinar que la clave de NAS es la clave progenitora de NAS identificada debido a que no se proporciona ningún valor de TROCEO. Entonces, la entidad de SKMF puede enviar la clave progenitora de NAS identificada a la primera entidad de red central.

Como alternativa, en algunas realizaciones, la primera solicitud puede comprender el valor de TROCEO además del identificador de clave de anclaje y el identificador de clave progenitora de NAS. En este caso, la entidad de SKMF puede determinar la clave de NAS al: identificar la clave progenitora de NAS basándose en el identificador de clave de anclaje y el identificador de clave progenitora de NAS, derivar una clave vástago de NAS basándose en la clave progenitora de NAS identificada y el valor de TROCEO, derivar un identificador de clave vástago de NAS para la clave vástago de NAS, y determinar que la clave de NAS es la clave vástago de NAS derivada. Entonces, la entidad de

SKMF puede enviar la clave vástago de NAS, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central.

5 En alguna realización, la primera solicitud puede ser una solicitud de clave, y la clave de NAS e información relacionada (de haber alguna) se pueden incluir en una respuesta de clave para enviarse a la primera entidad de red central.

10 Como alternativa, en algunas realizaciones, la generación de la clave de anclaje por la entidad de SKMF se puede desencadenar tras la recepción de una solicitud de autenticación desde la primera entidad de red central. La solicitud de autenticación se puede basar en una solicitud desde el dispositivo terminal para el establecimiento de una primera conexión de NAS que porta un primer procedimiento de NAS entre el dispositivo terminal y la primera entidad de red central, y puede comprender el indicador de NAS que indica el primer
15 procedimiento de NAS, entre otra información. En este caso, la entidad de SKMF puede derivar la clave progenitora de NAS asociada con el primer procedimiento de NAS basándose en la clave de anclaje, el identificador de abono (por ejemplo, SUPI) y el indicador de NAS incluido en la solicitud de autenticación, y derivar el identificador de clave progenitora de NAS para la clave progenitora de NAS.
20 Entonces, la entidad de SKMF puede enviar el identificador de clave de anclaje y el identificador de clave progenitora de NAS en una respuesta de autenticación a la primera entidad de red central.

25 Como alternativa o adicionalmente, en algunas realizaciones, la entidad de SKMF puede determinar la clave de NAS para la primera conexión de NAS basándose en la solicitud de autenticación. En algunas realizaciones, la solicitud

de autenticación puede comprender además el valor de TROCEO. En este caso, la entidad de SKMF puede derivar adicionalmente una clave vástago de NAS basándose en la clave progenitora de NAS derivada y el valor de TROCEO, derivar un identificador de clave vástago de NAS para la clave vástago de NAS, y determinar que la clave de NAS para la primera conexión de NAS es la clave vástago de NAS. Entonces, la entidad de SKMF puede enviar la clave vástago de NAS derivada, el identificador de clave vástago de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central. En algunas realizaciones, la solicitud de autenticación no incluye el valor de TROCEO. En este caso, la entidad de SKMF puede determinar la clave de NAS como la clave progenitora de NAS derivada asociada con el primer procedimiento de NAS, y enviar la clave progenitora de NAS y el identificador de clave progenitora de NAS a la primera entidad de red central.

Adicionalmente, en algunas realizaciones, la primera entidad de red central puede configurarse para manejar procedimientos de gestión de movilidad de NAS, y la entidad de red y la primera entidad de red central se pueden coubicar.

Adicionalmente, en algunas realizaciones, la entidad de SKMF puede recibir, desde una segunda entidad de red central, una segunda solicitud de una clave de NAS para una segunda conexión de NAS que porta un segundo procedimiento de NAS. Entonces, la entidad de SKMF puede determinar la clave de NAS para la segunda conexión de NAS basándose en la segunda solicitud, y enviar la clave de NAS para la segunda conexión de NAS a la segunda entidad de red central. La entidad de SKMF puede procesar la segunda solicitud de la misma forma que la primera solicitud y, por lo tanto, en el presente caso se omite

la descripción acerca del procesamiento de la segunda solicitud.

Aunque se proporcionan solo dos conexiones de NAS que portan diferentes procedimientos de NAS como un ejemplo para explicar el método 1200, los expertos en la materia apreciarán que el método 1200 puede ser aplicable a más de dos conexiones de NAS.

La figura 13 es un diagrama de flujo que representa un método 1300 para la seguridad en la arquitectura de terminaciones de NAS distribuida de acuerdo con algunas realizaciones de la presente divulgación. El método 1300 puede ser realizado por una entidad de red central configurada para implementar una función de red central, por ejemplo, una NF que soporta procedimientos de gestión de movilidad, o procedimientos de gestión de sesión, o procedimientos de gestión de política, etc.

Como se muestra en la figura 13, la entidad de red central puede recibir desde un dispositivo terminal una solicitud de establecimiento de una conexión de NAS que porta un procedimiento de NAS entre el dispositivo terminal y la entidad de red central, en el bloque 1310. El dispositivo terminal puede ser el UE en la arquitectura de terminaciones de NAS distribuida. En algunas realizaciones, la solicitud puede ser un mensaje de NAS inicial, por ejemplo, solicitud de registro de MM de NAS, o solicitud de sesión de PDU de NAS y, en consecuencia, el procedimiento de NAS puede ser procedimientos de gestión de movilidad de NAS o procedimientos de gestión de sesión de NAS.

En el bloque 1320, la entidad de red central puede obtener una clave de NAS para la conexión de NAS, por ejemplo, desde una entidad de red configurada para implementar SKMF, por ejemplo, la entidad de SKMF como se ha descrito anteriormente. La clave de NAS puede ser una clave progenitora de

NAS o una clave vástago de NAS asociada con un indicador de NAS que indica el procedimiento de NAS.

En algunas realizaciones, la entidad de red central puede determinar si se requiere una autenticación para el dispositivo terminal basándose en la solicitud de establecimiento de la conexión de NAS. En algunas realizaciones, la solicitud puede comprender SUCI o el ID de contexto temporal (por ejemplo, MM-GUTI/MM-S-TMSI), capacidades de seguridad de UE, el identificador de clave de anclaje y el indicador de NAS que indica el procedimiento de NAS. Se puede determinar que se requiere la autenticación, si el identificador de clave de anclaje indica que no existe una clave de anclaje válida, o el SUCI se incluye en la solicitud, o el ID de contexto temporal es no válido o no se halla. De lo contrario, se determina que no se requiere la autenticación.

Si se determina que se requiere la autenticación, la entidad de red central puede enviar una solicitud de autenticación a la entidad de SKMF. La solicitud de autenticación puede comprender el indicador de NAS que indica el procedimiento de NAS, entre otra información. Entonces, la entidad de red central puede recibir un identificador de clave de anclaje y un identificador de clave progenitora de NAS asociado con el indicador de NAS, por ejemplo, en una respuesta de autenticación. La entidad de red central puede desencadenar el envío de una solicitud para la clave de NAS a la entidad de SKMF, en donde la solicitud comprende el identificador de clave de anclaje recibido y el identificador de clave progenitora de NAS. En algunas realizaciones, la solicitud puede ser una solicitud de clave. Cuando la solicitud no comprende el valor de TROCEO, la entidad de red central puede recibir la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS

como la clave de NAS desde la entidad de SKMF. Cuando la solicitud comprende además el valor de TROCEO, la entidad de red central puede recibir la clave vástago de NAS basándose en el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el valor de TROCEO como la clave
5 de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS.

Como alternativa, en algunas realizaciones, cuando se determina que se requiere la autenticación, la entidad de red central puede desencadenar el envío de una solicitud de autenticación a la entidad de SKMF, y la solicitud de
10 autenticación puede comprender el indicador de NAS que indica el procedimiento de NAS y, opcionalmente, el valor de TROCEO, entre otra información. En el caso de que la solicitud de autenticación no comprenda el valor de TROCEO, la entidad de red central puede recibir la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS
15 como la clave de NAS desde la entidad de SKMF. En el caso de que la solicitud de autenticación comprenda además el valor de TROCEO, la entidad de red central puede recibir la clave vástago de NAS asociada con el indicador de NAS como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS asociado con la
20 clave progenitora de NAS basándose en la cual se deriva la clave vástago de NAS.

Adicionalmente, en algunas realizaciones, si se determina que no se requiere la autenticación, la entidad de red central puede verificar si el dispositivo terminal se registra con éxito. En algunas realizaciones, la entidad de red central
25 puede enviar una solicitud a otra entidad de red central que se identifica por el

MM-GUTI/MM-S-TMSI recibido para su verificación. Si el dispositivo terminal se verifica como registrado con éxito, la entidad de red central puede recibir una respuesta de éxito desde la otra entidad de red central. Entonces, la entidad de red central puede enviar una solicitud para la clave de NAS a la entidad de SKMF, por ejemplo, una solicitud de clave. Esta solicitud puede comprender un identificador de clave de anclaje y un identificador de clave progenitora de NAS y, opcionalmente, un valor de TROCEO. En el caso de que la solicitud no comprenda el valor de TROCEO, la entidad de red central puede recibir la clave progenitora de NAS identificada por el identificador de clave de anclaje y el identificador de clave progenitora de NAS como la clave de NAS desde la entidad de SKMF. En el caso de que la solicitud comprenda además el valor de TROCEO, la entidad de red central puede recibir la clave vástago de NAS basándose en el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el valor de TROCEO como la clave de NAS, un identificador de clave vástago de NAS para la clave vástago de NAS, y el identificador de clave progenitora de NAS desde la entidad de SKMF.

Adicionalmente, en algunas realizaciones, la entidad de red central puede generar un valor de TROCEO basándose en al menos uno de los siguientes: un ID de sesión de PDU; S-NSSAI; y un identificador de conjunto de funciones de red.

Adicionalmente, la entidad de red central puede configurarse para manejar procedimientos de gestión de movilidad de NAS, y se pueden coubicar la entidad de red central y la entidad de SKMF.

Las diversas realizaciones descritas anteriormente de la presente divulgación pueden asegurar que las conexiones de NAS terminadas en

diferentes NF centrales sean seguras, resilientes y de poco riesgo debido a que se minimiza cualquier ataque potencial. Además, las soluciones de estas realizaciones son óptimas y eficientes en cuanto al rendimiento.

Lo siguiente presentará algunos aspectos/realizaciones adicionales de la presente divulgación.

1. Manejo de claves de estrato de acceso (AS).

Un UE puede tener múltiples conexiones de NAS simultáneas terminadas en la red de servicio. Cada conexión de NAS se puede asociar con un indicador de NAS, y el mismo indicador de NAS se puede usar en más de una conexión de NAS dependiendo del valor del indicador de NAS. Por ejemplo, el indicador de NAS para procedimientos de gestión de sesión de NAS se puede usar en múltiples conexiones de NAS simultáneas en el caso en el que el UE tiene múltiples sesiones de PDU de NAS en diferentes S-NSSAI, por ejemplo. Sin embargo, el indicador de NAS para procedimientos de gestión de movilidad de NAS solo se puede usar en una única conexión de NAS para cada tipo de acceso (acceso de 3GPP o acceso no de 3GPP) en cualquier momento dado para el UE. Es decir, no puede haber múltiples conexiones de NAS activas usando el indicador de NAS para procedimientos de gestión de movilidad de NAS simultáneas activamente para acceso de 3GPP, por ejemplo.

En algunas realizaciones, la clave progenitora de NAS asociada con una conexión de NAS para procedimientos de gestión de movilidad de NAS se puede usar como entrada para derivar claves de AS por el UE y la NF central. Las claves vástago de NAS que están asociadas con conexiones de NAS para procedimientos no de gestión de movilidad de NAS se pueden no usar para derivar claves de AS.

En algunas realizaciones, las NF centrales que terminan las conexiones de NAS para procedimientos de gestión de movilidad de NAS pueden usar su clave progenitora de NAS para derivar y distribuir claves de AS de la misma forma en la que la AMF usa la clave K_{AMF} y otros parámetros (por ejemplo, recuento de NAS, NCC) como entrada para derivar y distribuir claves AS (por ejemplo, K_{gNB} , NH, K_{N3IWF}) como se define en la TS 33.501. El UE puede usar su clave progenitora de NAS asociada con procedimientos de gestión de movilidad de NAS para derivar claves de AS de la misma forma que el UE usa la clave K_{AMF} y otros parámetros (por ejemplo, recuento de NAS, NCC) como entrada para derivar claves de AS (por ejemplo, K_{gNB} , NH, K_{N3IWF}) como se define en la TS 33.501.

La derivación de nueva clave vástago/progenitora de NAS asociada con procedimientos de gestión de movilidad de NAS también puede desencadenar la derivación de nuevas claves de AS.

2. Conexiones de NAS a través de acceso de 3GPP y acceso no de 3GPP

Aprovechando y construyendo sobre la Sección 6.4.2.2 de la TS 33.501, cuando un UE tiene dos conexiones de NAS que soportan los mismos procedimientos de NAS, una a través de acceso de 3GPP y la otra a través de acceso no de 3GPP, y terminando ambas en las NF centrales en la misma PLMN, entonces el UE y las NF centrales mantendrán, como parte de sus contextos de seguridad de NAS respectivos, unos recuentos de NAS y un identificador de conexión de NAS (de 3GPP/no de 3GPP) para cada conexión de NAS. Otros parámetros de contexto de seguridad de NAS se compartirán entre ambas conexiones de NAS, tales como las claves de integridad y cifrado de NAS y los algoritmos de integridad y cifrado de NAS. Cuando un UE tiene dos conexiones

de NAS que soportan los mismos procedimientos de NAS, una a través de acceso de 3GPP y la otra a través de acceso no de 3GPP, y terminando ambas en las NF centrales en diferentes PLMN, entonces el UE y las NF centrales mantendrán, como parte de sus contextos de seguridad de NAS respectivos, un conjunto completo de parámetros de seguridad para cada conexión de NAS que incluye los recuentos de NAS, el identificador de conexión de NAS (de 3GPP/no de 3GPP), las claves de integridad y cifrado de NAS y los algoritmos de integridad y cifrado de NAS.

3. Mensaje de NAS inicial y manejo de transición de modo en reposo a conectado

Se aprovecha y se amplía el manejo de mensajes de NAS iniciales de acuerdo con la sección 6.4.6 de la TS 33.501 del 3GPP y la transición de modo en reposo a conectado de acuerdo con la sección 6.8.1.2.1 de la 33.501 del 3GPP.

En el caso en el que el UE tiene un contexto de seguridad de NAS válido, el UE proporciona, en el mensaje de NAS inicial, los Elementos de Información obligatorios mínimos (por ejemplo, SUCI/ID temporal/MM-S-TMSI/SM-S-TMSI, capacidades de seguridad de UE, identificador de clave de anclaje, identificador de clave progenitora de NAS, identificador de clave vástago de NAS, indicador de NAS en claro, así como el mensaje de NAS completo cifrado y todo el mensaje de NAS inicial protegido en cuanto a su integridad usando su contexto de seguridad de NAS.

Si la NF central tiene el mismo contexto de seguridad de NAS, entonces esta comprueba la integridad del mensaje de NAS inicial y descifra el mensaje de NAS completo recibido, lo procesa y asegura la respuesta con el contexto de

seguridad de NAS. Si la NF central no tiene o no puede obtener un contexto de seguridad de NAS válido, entonces esta puede solicitar desencadenar una ejecución de procedimiento de AKA para derivar una nueva clave de anclaje, etc. Si la NF central está manejando procedimientos de gestión de movilidad de NAS, entonces envía una autenticación solicitud a la SKMF. Si la NF central está manejando procedimientos no de gestión de movilidad de NAS, entonces esta envía una solicitud a la NF que está manejando procedimientos de gestión de movilidad de NAS, lo que desencadenará, a su vez, el procedimiento de AKA hacia la SKMF.

Si la ejecución de AKA tiene éxito, la NF central que maneja los procedimientos de gestión de movilidad de NAS desencadenará una orden de modo de seguridad de NAS hacia el UE para establecer un contexto de seguridad de NAS para la conexión de NAS como se ha explicado anteriormente con referencia a la figura 7 y la figura 10.

4. Traspaso de N2

En un traspaso de N2, una NF objetivo puede seleccionar unos algoritmos de integridad y cifrado de NAS diferentes de los usados por una NF de origen, y la NF de origen puede proporcionar a la NF objetivo una nueva clave vástago o progenitora de NAS, dependiendo de cuál se use y, en este sentido, es necesario que estos cambios se reflejen en el contexto de seguridad de NAS del UE.

Durante el traspaso de N2, se pueden aprovechar y ampliar los principios definidos en la Sección 6.9.2.3.3 de la TS 33.501 del 3GPP. Desencadenado por la recepción de un mensaje de traspaso requerido, la NF de origen puede proporcionar el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, las capacidades

de seguridad de UE, el recuento de DL de NAS, la clave vástago/progenitora de NAS y una indicación de si la clave vástago/progenitora de NAS se ha derivado horizontalmente a la NF objetivo. El contexto de seguridad de NAS de una conexión de NAS asegurada usando una clave progenitora de NAS tiene la clave progenitora de NAS y el identificador de clave progenitora de NAS, pero no tiene una clave vástago de NAS ni un identificador de clave vástago de NAS. El contexto de seguridad de NAS de una conexión de NAS asegurada usando una clave vástago de NAS tiene una clave progenitora de NAS, un identificador de clave progenitora de NAS, la clave vástago de NAS y un identificador de clave vástago de NAS.

La decisión de realizar la derivación de clave horizontal de una clave progenitora de NAS o una clave vástago de NAS se puede determinar por la presencia o ausencia de un identificador de clave vástago de NAS. Si el identificador de clave vástago de NAS está presente, entonces tiene lugar la derivación de clave horizontal de la clave vástago de NAS, y si falta el identificador de clave vástago de NAS, entonces tiene lugar la derivación de clave horizontal de la clave progenitora de NAS.

De forma similar, la NF objetivo puede decidir si usar la clave progenitora de NAS o la clave vástago de NAS para derivar las claves de integridad y cifrado de NAS basándose en la presencia o ausencia de una clave vástago de NAS. Si la clave vástago de NAS está presente, entonces esta se usa para derivar las claves de integridad y cifrado de NAS, de lo contrario se usa la clave progenitora de NAS.

De acuerdo con la configuración de política local, la NF de origen puede decidir si se realiza la derivación de clave horizontal. La NF de origen puede

realizar la derivación horizontal de la clave vástago/progenitora de NAS usando la clave vástago/progenitora de NAS activa actual y el recuento de DL de NAS como entradas, para derivar una nueva clave vástago/progenitora de NAS. La NF de origen puede enviar estas entradas en una solicitud de derivación de clave horizontal a la SKMF que devuelve la nueva clave vástago/progenitora de NAS derivada horizontalmente.

Basándose en las capacidades de seguridad de UE que indican los algoritmos de integridad y cifrado de NAS soportados, la NF objetivo puede seleccionar, de entre sus algoritmos de integridad y cifrado de NAS soportados, los de la prioridad más alta y usa estos identificadores de algoritmo de integridad y cifrado de NAS como entrada, junto con la clave progenitora/vástago de NAS, para derivar claves de integridad y cifrado de NAS. La NF objetivo puede almacenar en su contexto de seguridad de NAS el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago/progenitora de NAS, las claves de integridad y cifrado de NAS, las capacidades de seguridad de UE, el recuento de DL de NAS y los algoritmos de integridad y cifrado de NAS.

La NF objetivo puede crear un contenedor de NAS con parámetros de seguridad, que se protege en cuanto a su integridad con la clave de integridad de NAS y se proporciona a través de (R)AN al UE. El fin del contenedor de NAS se puede considerar similar al de la orden de modo de seguridad de NAS. El contenedor de NAS puede contener el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, las capacidades de seguridad de UE, el recuento de DL de NAS, los algoritmos de integridad y cifrado de NAS seleccionados y una indicación de si

la clave vástago/progenitora de NAS se ha derivado horizontalmente.

A partir de su contexto de seguridad de NAS almacenado localmente, el UE puede usar el identificador de clave de anclaje para comprobar que este está asociado con una ejecución de AKA actual y válida, usar el identificador de clave de anclaje y el identificador de clave progenitora de NAS para identificar la clave progenitora de NAS, y usar el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el identificador de clave vástago de NAS para identificar la clave vástago de NAS. Si se indica la derivación de clave horizontal, el UE puede usar la clave vástago/progenitora de NAS identificada localmente y el recuento de DL de NAS recibido para derivar horizontalmente una nueva clave vástago/progenitora de NAS que está asociada con el identificador de clave vástago/progenitora de NAS existente.

Los identificadores de algoritmos de integridad y cifrado de NAS y la nueva clave vástago/progenitora de NAS se pueden usar como entradas para derivar las claves de integridad y cifrado de NAS. La clave de integridad de NAS se puede usar para comprobar la integridad del contenedor de NAS recibido, y las capacidades de seguridad de UE recibidas se pueden comprobar para asegurar que no ha tenido lugar un ataque de oferta a la baja.

Si se supera la comprobación de integridad de NAS, entonces el contexto de seguridad de NAS del UE se puede actualizar con las nuevas claves progenitoras/vástago/de NAS, las nuevas claves de integridad y cifrado de NAS y los recuentos de NAS. Obsérvese que, según la Sección 6.9.2.3.3 de la TS 33.501, si la clave vástago/progenitora de NAS se deriva horizontalmente, los recuentos de NAS se establecen a cero, de lo contrario se usa el recuento de NAS recibido.

El procedimiento anterior se refiere principalmente al escenario de reubicación de función de gestión de movilidad, pero esto se puede ampliar y se puede hacer aplicable para cualquier NF que se pudiera reubicar como parte de la movilidad de UE.

5 5. Traspaso de Xn

La NF que ancla la conexión de gestión de movilidad de NAS puede ser responsable de proporcionar a la RAN objetivo el material de gestión de claves como se define en la Sección 6.9.2.3.2 de la TS 33.501 del 3GPP, en donde el Kamf es equivalente a la clave vástago/progenitora de NAS.

10 6. Actualizaciones de registro de movilidad de modo en reposo

Cuando una NF objetivo recibe una actualización de registro de movilidad de NAS, esta puede usar el identificador temporal (por ejemplo, MM-GUTI/MM-S-TMSI) para identificar la NF de origen que almacena el contexto del UE que incluye el contexto de seguridad de NAS de UE. Si la NF de origen halla un contexto de UE válido, esta puede proporcionar a la NF objetivo el SUPI y puede proporcionar su información de contexto de seguridad de NAS almacenada.

Durante la actualización de registro de movilidad de NAS, se pueden aprovechar y ampliar los principios definidos en la Sección 6.9.3 de la TS 33.501 del 3GPP.

De acuerdo con la configuración de política local, la NF de origen puede decidir si se realiza una derivación de clave horizontal. La NF de origen puede realizar la derivación horizontal de la clave vástago/progenitora de NAS usando la clave vástago/progenitora de NAS activa actual y el recuento de UL de NAS de la solicitud de registro de NAS recibida (actualización de movilidad) como entradas para derivar una nueva clave vástago/progenitora de NAS. La NF de

origen puede enviar estas entradas en una solicitud de derivación de clave horizontal a la SKMF que devuelve la nueva clave vástago/progenitora de NAS derivada horizontalmente.

5 La NF de origen puede proporcionar la información de contexto de seguridad de NAS de UE a la NF objetivo, lo que incluye el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, las capacidades de seguridad de UE, el recuento de UL de NAS, la clave vástago/progenitora de NAS y una indicación de si la clave vástago/progenitora de NAS se ha derivado horizontalmente.

10 Basándose en las capacidades de seguridad de UE que indican los algoritmos de integridad y cifrado de NAS soportados, la NF objetivo puede seleccionar, de entre sus algoritmos de integridad y cifrado de NAS soportados, los de la prioridad más alta y usa estos identificadores de algoritmo de integridad y cifrado de NAS como entradas, junto con la clave progenitora/vástago de NAS,
15 para derivar claves de integridad y cifrado de NAS.

La NF objetivo puede almacenar en su contexto de seguridad de NAS el identificador de clave de anclaje, el identificador de clave progenitora de NAS, el identificador de clave vástago de NAS, la clave vástago/progenitora de NAS, las claves de integridad y cifrado de NAS, las capacidades de seguridad de UE, el
20 recuento de UL de NAS y los algoritmos de integridad y cifrado de NAS.

De acuerdo con la configuración de política local, la NF objetivo puede decidir si se usa, o no, una clave vástago/progenitora de NAS que incluye una derivada horizontalmente a partir de la NF de origen. Si no, la NF objetivo puede desencadenar un procedimiento de reautenticación que puede derivar una nueva
25 clave de anclaje, identificador de clave de anclaje, identificador de clave

progenitora de NAS, identificador de clave vástago de NAS, clave vástago/progenitora de NAS, y establecer un nuevo contexto de seguridad de NAS con el UE.

Si se usa la información de contexto de seguridad de NAS de la NF de
5 origen, la NF objetivo puede crear y enviar al UE un mensaje de orden de modo de seguridad de NAS que se protege en cuanto a su integridad con la clave de integridad de NAS e incluye un identificador de clave de anclaje, un identificador de clave progenitora de NAS, un identificador de clave vástago de NAS, capacidades de seguridad de UE, algoritmos de integridad y cifrado de NAS
10 seleccionados y una indicación de si la clave vástago/progenitora de NAS se ha derivado horizontalmente.

A partir de su contexto de seguridad de NAS almacenado localmente, el UE puede usar el identificador de clave de anclaje para comprobar que este está asociado con una ejecución de AKA actual y válida, usar el identificador de clave
15 de anclaje y el identificador de clave progenitora de NAS para identificar la clave progenitora de NAS, y usar el identificador de clave de anclaje, el identificador de clave progenitora de NAS y el identificador de clave vástago de NAS para identificar la clave vástago de NAS. Si se indica la derivación de clave horizontal, el UE puede usar la clave vástago/progenitora de NAS identificada localmente y
20 el recuento de UL de NAS de la solicitud de registro de NAS para derivar horizontalmente una nueva clave vástago/progenitora de NAS.

Los identificadores de algoritmos de integridad y cifrado de NAS y la nueva clave vástago/progenitora de NAS se pueden usar como entradas para derivar las claves de integridad y cifrado de NAS. La clave de integridad de NAS se
25 puede usar para comprobar la integridad de la orden de modo de seguridad de

NAS recibida, y las capacidades de seguridad de UE recibidas se pueden usar para asegurar que no ha tenido lugar un ataque de oferta a la baja.

Si se supera la comprobación de integridad de NAS, entonces el UE puede actualizar su contexto de seguridad de NAS con la nueva clave vástago/progenitora de NAS, las nuevas claves de integridad y cifrado de NAS, los algoritmos de integridad y cifrado de NAS y los recuentos de NAS, y devuelve un modo de seguridad de NAS completo a la NF objetivo.

A continuación se hace referencia a la figura 14, que ilustra un diagrama de bloques simplificado de un aparato 1400 que se puede materializar como el dispositivo terminal, o la entidad de red configurada para implementar SKMF, o la entidad de red central configurada para implementar una NF central. El aparato 1400 puede comprender al menos un procesador 1401, tal como un procesador de datos (DP) y al menos una memoria (MEM) 1402 acoplada al al menos un procesador 1401. El aparato 1400 puede comprender además una unidad de envío y una unidad de recepción 1403 acopladas a los uno o más procesadores 1401.

Los procesadores 1401 pueden ser de cualquier tipo adecuado para el entorno técnico local y pueden incluir uno o más de los siguientes: ordenadores de propósito general, ordenadores de propósito especial, microprocesadores, procesadores de señales digitales (DSP) y procesadores basándose en arquitectura de procesador de múltiples núcleos, como ejemplos no limitantes.

La(s) MEM 1402 puede(n) ser de cualquier tipo adecuado al entorno técnico local y se puede(n) implementar usando cualquier tecnología de almacenamiento de datos adecuada, tal como dispositivos de memoria basados en semiconductores, dispositivos y sistemas de memoria magnéticos,

dispositivos y sistemas de memoria ópticos, memoria fija y memoria extraíble, como ejemplos no limitantes.

La MEM 1402 almacena un programa (PROG) 1404. El PROG 1404 puede incluir instrucciones que, cuando se ejecutan en el procesador asociado
5 1401, posibilitan que el aparato 1400 opere de acuerdo con las realizaciones de la presente divulgación, por ejemplo, para realizar uno de los métodos 1100, 1200 y 1300 como se muestra en la figura 11, la figura 12 y la figura 13. Una combinación del al menos un procesador 1401 y la al menos una MEM 1402 puede formar una circuitería o medios de procesamiento 1405 adaptados para
10 implementar diversas realizaciones de la presente divulgación.

Diversas realizaciones de la presente divulgación se pueden implementar mediante un programa informático ejecutable por uno o más de los procesadores 1401, software, firmware, hardware o en una combinación de los mismos.

En general, las diversas realizaciones ilustrativas se pueden implementar
15 en hardware o circuitos de propósito especial, software, lógica o cualquier combinación de los mismos. Por ejemplo, algunos aspectos se pueden implementar en hardware, mientras que otros aspectos se pueden implementar en firmware o software que puede ser ejecutado por un controlador, un microprocesador u otro dispositivo informático, aunque la invención no se limita
20 a ello. Aunque diversos aspectos de las realizaciones ilustrativas de esta divulgación se pueden ilustrar y describir como diagramas de bloques, diagramas de flujo o usando alguna otra representación gráfica, se entiende bien que estos bloques, aparatos, sistemas, técnicas o métodos descritos en el presente documento se pueden implementar en, como ejemplos no limitantes, hardware,
25 software, firmware, circuitos o lógica de propósito especial, controlador o

hardware de propósito general u otros dispositivos informáticos, o alguna combinación de los mismos.

En este sentido, se debería apreciar que al menos algunos aspectos de las realizaciones ilustrativas de las divulgaciones se pueden poner en práctica en diversos componentes tales como módulos y chips de circuito integrado. Por lo tanto, se debería apreciar que las realizaciones ilustrativas de esta divulgación se pueden concretar en un aparato que se materializa como un circuito integrado, en donde el circuito integrado puede comprender circuitería (así como posiblemente firmware) para materializar al menos uno o más de un procesador de datos, un procesador digital de señales, circuitería de banda base y circuitería de radiofrecuencia que son configurables con el fin de operar de acuerdo con las realizaciones ilustrativas de esta divulgación.

Se debería apreciar que al menos algunos aspectos de las realizaciones ilustrativas de las divulgaciones se pueden materializar en instrucciones ejecutables por ordenador, tales como en uno o más módulos de programa, ejecutados por uno o más ordenadores u otros dispositivos. Generalmente, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares cuando son ejecutados por un procesador en un ordenador u otro dispositivo. Las instrucciones ejecutables por ordenador se pueden almacenar en un medio legible por ordenador, por ejemplo, un medio legible por ordenador no transitorio tal como un disco duro, un disco óptico, un medio de almacenamiento extraíble, una memoria de estado sólido, una RAM, etc. Como apreciará un experto en la materia, la función de los módulos de programa se puede combinar o distribuir como se desee en diversas

realizaciones. Además, la función se puede materializar, en su totalidad o en parte, en equivalentes de firmware o hardware tales como circuitos integrados, matrices de puertas programables en campo (FPGA) y similares.

Además, aunque se representan operaciones en un orden particular, esto
5 no se debería entender como que requiere que, para lograr resultados deseables, tales operaciones se hayan de realizar en el orden particular mostrado o en orden secuencial, o que se hayan de realizar todas las operaciones ilustradas. En ciertas circunstancias, la multitarea y el procesamiento paralelo pueden ser ventajosos. De forma similar, aunque varios
10 detalles de implementación específicos están contenidos en los análisis anteriores, estos no se deberían interpretar como limitaciones al alcance de la presente divulgación, sino más bien como descripciones de características que pueden ser específicas de realizaciones particulares. Ciertas características que se describen en el contexto de realizaciones separadas también se pueden
15 implementar en combinación en una única realización. A la inversa, diversas características que se describen en el contexto de una única realización también se pueden implementar en múltiples realizaciones de forma separada o en cualquier subcombinación adecuada.

La presente divulgación incluye cualquier característica o combinación de
20 características novedosa divulgada en el presente documento, o bien de forma explícita o bien cualquier generalización de la misma. Diversas modificaciones y adaptaciones a las realizaciones ilustrativas anteriores de esta divulgación se pueden hacer evidentes para los expertos en las materias pertinentes en vista de la descripción anterior, cuando se leen en conjunto con los dibujos adjuntos.
25 No obstante, todas y cada una de las modificaciones seguirán cayendo dentro

del alcance de las realizaciones no limitantes e ilustrativas de esta divulgación.