(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 823 552**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 29/06 (2006.01)
H04W 12/10 (2009.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.05.2018 PCT/EP2018/061713**

(87) Fecha y número de publicación internacional: **15.11.2018 WO18206501**

(96) Fecha de presentación y número de la solicitud europea: **07.05.2018 E 18722549 (5)**

(97) Fecha y número de publicación de la concesión europea: **29.07.2020 EP 3622737**

(54) Título: **Métodos que proporcionan seguridad para conexiones múltiples de NAS usando conteos separados y nodos de red y terminales inalámbricos relacionados**

(30) Prioridad:

08.05.2017 US 201762502966 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.05.2021

(73) Titular/es:

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

(72) Inventor/es:

BEN HENDA, NOAMEN y
WIFVESSON, MONICA

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Métodos que proporcionan seguridad para conexiones múltiples de NAS usando conteos separados y nodos de red y terminales inalámbricos relacionados

Campo técnico

La presente divulgación se refiere en general al campo de las comunicaciones, y más particularmente a las comunicaciones inalámbricas y los nodos de red y terminales inalámbricos relacionados.

Antecedentes

En los sistemas 5G, un UE puede registrarse simultáneamente en la misma PLMN a través del acceso 3GPP (por ejemplo, usando un nodo de acceso LTE o 5G, también conocido como estación base, eNB, gNB, etc.) y acceso no 3GPP (por ejemplo, usando un nodo WiFi o satélite). Para este propósito, se espera que el Terminal inalámbrico UE y la AMF (función de gestión de acceso) de red mantengan una conexión para cada tipo de acceso (es decir, una conexión para el acceso 3GPP y una conexión para la conexión de NAS no 3GPP). En tales escenarios, TS 23.501 (denominado referencia [1]) describe además qué elementos del contexto de usuario en la AMF se compartirían entre las conexiones y cuáles no. Por ejemplo, puede haber varios estados de gestión de conexión (CM) y gestión de registro, uno por tipo de acceso. Por otro lado, se puede usar un identificador temporal común.

Como se describe en TS 33.401 [2], los mecanismos de seguridad en los sistemas heredados pueden proporcionar integridad, confidencialidad y protección de reproducción para los mensajes de NAS. El contexto de seguridad de NAS incluye la clave KASME, las claves de protección derivadas KNASint y KNASenc, el identificador de conjunto de claves eKSI y un par de contadores CONTEOS DE NAS, uno para cada dirección (enlace ascendente y descendente). Estos parámetros de seguridad pueden proporcionarse para una conexión de NAS y pueden actualizarse tras la creación de una nueva KASME, por ejemplo, siguiendo un procedimiento de autenticación.

Además, un mecanismo de protección de reproducción, realizado en parte por los CONTEOS DE NAS, puede basarse en suposiciones de que el protocolo es confiable y que los procedimientos NAS se ejecutan secuencialmente de modo que un nuevo procedimiento solo se inicia después de la terminación del actual. Esto puede proporcionar/garantizar la entrega en orden de los mensajes de NAS, de modo que tanto el UE como la MME solo necesitan almacenar dos valores para CONTEOS DE NAS, uno por dirección (es decir, un CONTEO DE NAS para el enlace ascendente y un CONTEO DE NAS para el enlace descendente). Estos serían los siguientes y los únicos valores esperados/aceptados.

Sin embargo, con múltiples conexiones a través de accesos 3GPP y no 3GPP, la entrega en orden de los mensajes de NAS a través de las diferentes conexiones puede no ser confiable.

El documento de patente US 2016/0286600 describe un dispositivo que inicia el transporte de un primer mensaje de NAS en una primera conexión a un primer nodo de red central (MME) y que establece un primer contexto NAS. Dicho dispositivo también puede iniciar el transporte de un segundo mensaje de NAS a través de una segunda conexión a un segundo nodo de red central (MME) y establecer un segundo contexto NAS. Además, una pluralidad de contextos puede asociarse con una pluralidad de nodos de servicio, y cada uno de los contextos puede asociarse con un conjunto separado de credenciales, en el que los datos correspondientes a un contexto pueden encriptarse basándose en las credenciales asociadas con el contexto.

Sumario

La presente invención se define en las reivindicaciones independientes. Las reivindicaciones dependientes definen las realizaciones de la presente invención.

De acuerdo con algunas realizaciones de conceptos de la invención, un método en un primer nodo de comunicación puede proporcionar comunicación de mensajes de estrato de acceso a red (NAS) con un segundo nodo de comunicación. Puede proporcionarse una primera identificación de conexión de NAS para una primera conexión de NAS entre el primer y el segundo nodo de comunicación, y puede proporcionarse una segunda identificación de conexión de NAS para una segunda conexión de NAS entre el primer y el segundo nodo de comunicación. Además, la primera y la segunda identificación de la conexión de NAS pueden ser diferentes, y la primera y la segunda conexión de NAS pueden ser diferentes. Se puede comunicar un primer mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la primera conexión de NAS, y comunicar el primer mensaje de NAS puede incluir realizar al menos uno de generar un código de autenticación de mensaje para la autenticación de integridad del primer mensaje de NAS usando la primera identificación de conexión de NAS y/o cifrar/descifrar el primer mensaje de NAS usando la primera identificación de conexión de NAS. Se puede comunicar un segundo mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la segunda conexión de NAS, y comunicar el segundo mensaje de NAS puede incluir realizar al menos uno de generar un código de autenticación de mensaje para la autenticación de integridad del segundo mensaje de NAS usando la segunda identificación de

conexión de NAS y/o cifrar/descifrar el segundo mensaje de NAS usando la segunda identificación de conexión de NAS.

De acuerdo con algunas otras realizaciones de conceptos de la invención, un método en un primer nodo de comunicación puede proporcionar la comunicación de mensajes de estrato de acceso a red (NAS) con un segundo nodo de comunicación. Puede proporcionarse una primera conexión de NAS entre el primer y el segundo nodo de comunicación, y puede proporcionarse una segunda conexión de NAS entre el primer y el segundo nodo de comunicación. Además, la primera y la segunda conexión de NAS pueden ser diferentes. Se puede asignar un dominio conteo de NAS de modo que una primera porción del dominio conteo de NAS se asigne para los mensajes de NAS comunicados a través de la primera conexión de NAS y de modo que una segunda porción del dominio conteo de NAS se asigne a los mensajes de NAS comunicados a través de la segunda conexión de NAS. Además, la primera y la segunda porción del dominio conteo de NAS pueden ser mutuamente excluyentes. Los mensajes de NAS pueden estar a través de la primera conexión de NAS usando un valor de conteo de NAS más bajo desde la primera porción del dominio conteo de NAS que no se haya usado previamente para cada mensaje de NAS comunicado a través de la primera conexión de NAS. Los mensajes de NAS se pueden comunicar a través de la segunda conexión de NAS usando un valor de conteo de NAS más bajo desde la segunda porción del dominio conteo de NAS que no se haya usado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS.

De acuerdo con algunas realizaciones de conceptos de la invención divulgados en el presente documento, se puede mejorar la gestión de conexiones de NAS paralelas.

Breve descripción de los dibujos

Los dibujos adjuntos, que se incluyen para proporcionar una comprensión adicional de la divulgación y se incorporan y constituyen una parte de esta solicitud, ilustran ciertas realizaciones no limitativas de conceptos de la invención. En los dibujos:

la figura 1 es un diagrama que ilustra un ejemplo de organización de mensajes para un mensaje de NAS protegido por seguridad;

la figura 2 es una tabla que ilustra los tipos de encabezados de seguridad del mensaje de NAS protegido por seguridad de la figura 1;

las figuras 3 A y 3B ilustran el uso de un proceso EIA de integridad de 128 bits para autenticar la integridad de los mensajes;

las figuras 4A y 4B ilustran el uso de un proceso EEA de cifrado de 128 bits para cifrar datos de mensajes;

la figura 5 es un diagrama de bloques que ilustra conexiones múltiples de NAS entre un nodo de red central y un terminal inalámbrico de acuerdo con algunas realizaciones de conceptos de la invención;

la figura 6 es un diagrama de bloques que ilustra elementos de un Terminal inalámbrico UE de acuerdo con algunas realizaciones de conceptos de la invención;

la figura 7 es un diagrama de bloques que ilustra elementos de un nodo de red de acuerdo con algunas realizaciones de conceptos de la invención;

las figuras 8 y 9 son diagramas de bloques que ilustran las funciones de seguridad de NAS en el nodo de red de las figuras 5 y 7 y en el terminal inalámbrico de las figuras 5 y 6, respectivamente, de acuerdo con algunas realizaciones de conceptos de la invención;

las figuras 10A, 10B, 12A y 12B ilustran el uso de un proceso de integridad para autenticar la integridad de los mensajes de NAS de acuerdo con algunas realizaciones de conceptos de la invención;

las figuras 11A, 11B, 13A y 13B ilustran el uso de un proceso de cifrado/descifrado para cifrar/descifrar datos de mensajes de NAS de acuerdo con algunas realizaciones de conceptos de la invención;

la figura 14 ilustra diferenciadores de tipo de proceso que pueden usarse de acuerdo con algunas realizaciones de conceptos de la invención;

las figuras 15 y 16 ilustran derivaciones clave que pueden usarse de acuerdo con algunas realizaciones de conceptos de la invención;

las figuras 17A y 18A son diagramas de flujo que ilustran operaciones de comunicación de mensajes de NAS a través de conexiones múltiples de NAS de acuerdo con algunas realizaciones de conceptos de la invención; y

las figuras 17B y 18B son diagramas de bloques que ilustran módulos de memoria correspondientes a las operaciones de las figuras 17A y 18A respectivamente, de acuerdo con algunas realizaciones de conceptos de la invención.

Descripción detallada

Los conceptos de la invención se describirán ahora más completamente a continuación con referencia a los dibujos adjuntos, en los que se muestran ejemplos de realizaciones de conceptos de la invención. Sin embargo, los conceptos de la invención pueden realizarse de muchas formas diferentes y no deben interpretarse como limitados a las realizaciones expuestas en el presente documento. Más bien, estas realizaciones se proporcionan para que esta divulgación sea minuciosa y completa, y transmita completamente el alcance de los presentes conceptos de la invención a los expertos en la técnica. También debe tenerse en cuenta que estas realizaciones no se excluyen mutuamente. Se puede suponer tácitamente que los componentes de una realización están presentes/se usan en otra realización.

La siguiente descripción presenta varias realizaciones de la materia divulgada. Estas realizaciones se presentan como ejemplos de enseñanza y no deben interpretarse como limitativas del alcance de la materia divulgada. Por ejemplo, ciertos detalles de las realizaciones descritas pueden modificarse, omitirse o ampliarse sin apartarse del alcance de la materia divulgada.

La figura 5 es un diagrama de bloques que ilustra conexiones múltiples de NAS entre el nodo 501 de red central (que proporciona gestión de acceso) y un terminal inalámbrico UE 505 de acuerdo con algunas realizaciones de conceptos de la invención. Como se muestra, se puede proporcionar una primera conexión de NAS a través de un nodo de acceso 3GPP (por ejemplo, una estación base, eNB, eNodoB, gNB, gNodoB), se puede proporcionar una segunda conexión de NAS a través de un primer nodo de acceso no 3GPP (por ejemplo, un nodo de acceso WiFi) y se puede proporcionar una tercera conexión de NAS a través de un segundo nodo de acceso no 3GPP (por ejemplo, un nodo satélite). Con diferentes conexiones de NAS proporcionadas a través de diferentes nodos de acceso de diferentes tecnologías, la probabilidad de que el nodo de recepción (el terminal inalámbrico 505 en el enlace descendente o el nodo 501 de red central en el enlace ascendente) reciba todos los mensajes de NAS en orden puede reducirse.

La figura 6 es un diagrama de bloques que ilustra los elementos de un terminal inalámbrico UE 505 (también denominado dispositivo inalámbrico, dispositivo de comunicación inalámbrica, terminal de comunicación inalámbrica, equipo de usuario, nodo/terminal/dispositivo de equipo de usuario, etc.) configurado para proporcionar comunicación inalámbrica de acuerdo con realizaciones de conceptos de la invención. Como se muestra, el Terminal inalámbrico UE puede incluir un circuito 601 de transceptor (también denominado transceptor) que incluye un transmisor y un receptor configurado para proporcionar comunicaciones de radio de enlace ascendente y de enlace descendente con una estación o estaciones base de una red de acceso por radio. El Terminal inalámbrico UE también puede incluir un circuito 603 de procesador (también denominado procesador) acoplado al circuito de transceptor, y un circuito 605 de memoria (también denominado memoria) acoplado al circuito de procesador. El circuito 605 de memoria puede incluir un código de programa legible por computadora que, cuando es ejecutado por el circuito 603 de procesador, hace que el circuito de procesador realice operaciones de acuerdo con las realizaciones divulgadas en el presente documento. De acuerdo con otras realizaciones, el circuito 603 de procesador puede definirse para incluir memoria de modo que no se requiera un circuito de memoria separado. El Terminal inalámbrico UE también puede incluir una interfaz 607 (tal como una interfaz de usuario) acoplada con el procesador 603, y/o el Terminal inalámbrico UE puede incorporarse en un vehículo. La interfaz 607 de usuario puede incluir, por ejemplo, una pantalla (por ejemplo, una pantalla táctil) que proporciona salida visual, un altavoz que proporciona salida de audio y/o un dispositivo de entrada de usuario (por ejemplo, una pantalla táctil, teclado, botón o botones, etc.) que acepta la entrada del usuario.

Como se explica en el presente documento, las operaciones del terminal inalámbrico UE 505 pueden realizarse mediante el procesador 603 y/o el transceptor 601. Por ejemplo, el procesador 603 puede controlar el transceptor 601 para transmitir comunicaciones a través del transceptor 601 a través de una interfaz de radio a un nodo de acceso y/o para recibir comunicaciones a través del transceptor 601 desde un nodo de acceso a través de una interfaz de radio. Además, los módulos pueden almacenarse en la memoria 605, y estos módulos pueden proporcionar instrucciones de modo que cuando el procesador 603 ejecute las instrucciones de un módulo, el procesador 603 realice las operaciones respectivas (por ejemplo, las operaciones que se explican a continuación con respecto a las realizaciones de ejemplo).

La figura 7 es un diagrama de bloques que ilustra los elementos de un nodo de red (también denominado nodo de red central, estación base, eNB, eNodoB, gNB, gNodoB, etc.) de una red de acceso por radio (RAN) configurada para soportar comunicaciones inalámbricas de acuerdo con las realizaciones de conceptos de la invención. Como se muestra, el nodo de red puede incluir un circuito 501 de interfaz de red (también conocido como interfaz de red) que incluye un transmisor y un receptor configurado para proporcionar comunicaciones de radio de enlace ascendente y de enlace descendente con terminales inalámbricos, por ejemplo, a través de nodos de acceso como se muestra en

la figura. 5. El nodo de red también puede incluir un circuito 703 de procesador (también denominado procesador) acoplado al circuito de interfaz de red, y un circuito 705 de memoria (también denominado memoria) acoplado al circuito de procesador. El circuito 705 de memoria puede incluir un código de programa legible por computadora que cuando es ejecutado por el circuito 703 de procesador hace que el circuito de procesador realice operaciones de acuerdo con las realizaciones divulgadas en el presente documento. De acuerdo con otras realizaciones, el circuito 703 de procesador puede definirse para incluir memoria de modo que no se requiera un circuito de memoria separado.

Como se explica en el presente documento, las operaciones del nodo 501 de red pueden realizarse mediante el procesador 703 y/o la interfaz 701 de red. Por ejemplo, el procesador 703 puede controlar la interfaz 701 de red para transmitir comunicaciones a través de la interfaz 701 de red a uno o más nodos de acceso y/o para recibir comunicaciones a través de la interfaz de red desde uno o más nodos de acceso como se muestra en la figura 5. Además, los módulos pueden almacenarse en la memoria 705, y estos módulos pueden proporcionar instrucciones de modo que cuando el procesador 703 ejecute las instrucciones de un módulo, el procesador 703 realice las operaciones respectivas (por ejemplo, las operaciones que se explican a continuación con respecto a las realizaciones de ejemplo). Aunque no se muestra en las figuras 5 y 7, las operaciones del nodo 503-1 de acceso 3GPP y el nodo 501 de red pueden combinarse proporcionando un transceptor en el nodo 501 de red. En tales realizaciones, el transceptor del nodo 501 de red puede proporcionar la conexión de NAS 3GPP a través de una interfaz 3GPP directa con el terminal inalámbrico 505. De acuerdo con tales realizaciones, el procesador 703 puede controlar el transceptor para transmitir comunicación a través del transceptor por una interfaz de radio al terminal inalámbrico 505 y/o para recibir comunicaciones a través del transceptor desde el terminal inalámbrico 505.

Ahora se explicará un formato de mensaje general y la codificación de elementos de información para los mensajes de NAS en EPC.

Para los sistemas EPC/LTE heredados, TS 24.301 (también denominado referencia [3]) describe un formato de mensaje general y codificación de elementos de información para mensajes de NAS. Si el mensaje de NAS es un mensaje de NAS protegido por seguridad, el mensaje incluye las siguientes partes:

a) discriminador de protocolo;

b) tipo de encabezado de seguridad;

c) código de autenticación de mensaje (MAC);

d) número de secuencia; y

e) mensaje de NAS simple.

La organización de un mensaje de NAS protegido por seguridad se ilustra en el ejemplo que se muestra en la figura 1, que ilustra una organización de mensajes para un mensaje de NAS protegido por seguridad.

Los bits 5 a 8 del primer octeto de cada mensaje de gestión de movilidad de EPS (EMM) contienen el IE de tipo de encabezado de seguridad. Este IE incluye información de control relacionada con la protección de seguridad de un mensaje de NAS. El tamaño total del IE de tipo de encabezado de seguridad es de 4 bits. El IE de tipo de encabezado de seguridad puede tomar los valores que se muestran en la tabla de la figura 2, que ilustra los tipos de encabezado de seguridad del mensaje de NAS protegido por seguridad de la figura 1.

El elemento de información del código de autenticación de mensaje (MAC) de la figura 1 incluye/contiene la información de protección de integridad para el mensaje. El IE de MAC se incluye en el mensaje de NAS protegido por seguridad si existe un contexto de seguridad EPS válido y se inician las funciones de seguridad.

El IE de número de secuencia en la figura 1 incluye el número de secuencia (SN) del mensaje de NAS que consta de los ocho bits menos significativos del CONTEO DE NAS para un mensaje de NAS protegido por seguridad.

Cuando se va a enviar un mensaje de NAS cifrado y protegido por integridad, primero se cifra el mensaje de NAS y luego el mensaje de NAS cifrado y el número de secuencia de NAS (CONTEO DE NAS) se protegen por integridad calculando el MAC.

Cuando un mensaje de NAS debe enviarse solo con protección por integridad y sin cifrar, el mensaje de NAS no cifrado y el número de secuencia de NAS se protegen en integridad calculando el MAC.

TS 33.401 (también denominado referencia [2]) y TS 24.301 (también denominado referencia [3]) describen que cada KASME por separado tiene un par distinto de CONTEOS DE NAS, un CONTEO DE NAS para el enlace ascendente y un CONTEO DE NAS para el enlace descendente, asociados a ello.

Los CONTEOS DE NAS para una KASME en particular no se restablecen a los valores iniciales (es decir, los CONTEOS DE NAS solo tienen su valor inicial cuando se crea una nueva KASME). Esta reduce/previene un problema de seguridad de usar los mismos CONTEOS DE NAS con las mismas claves NAS, por ejemplo reutilización del flujo de claves.

TS 24.301 (también denominado referencia [3]) describe que el emisor usa su CONTEO DE NAS almacenado localmente como entrada al proceso de protección/verificación de integridad (también denominado n algoritmo de verificación/protección de integridad) que se usa para proporcionar integridad y verificación. El receptor usa el número de secuencia de NAS incluido en el mensaje recibido (o estimado a partir de los 5 bits del número de secuencia de NAS recibido en el mensaje) y una estimación del contador de desbordamiento de NAS para formar la entrada CONTEO DE NAS al proceso de verificación de integridad.

La protección de integridad incluye los octetos 6 a n del mensaje de NAS protegido por seguridad, es decir, el IE de número de secuencia y el IE de mensaje de NAS. Después de la validación exitosa de la protección de integridad, el receptor actualiza su CONTEO DE NAS almacenado localmente correspondiente con el valor del CONTEO DE NAS estimado para este mensaje de NAS.

La protección de reproducción debería/debe garantizar que el receptor no acepte dos veces el mismo mensaje de NAS. Específicamente, para un contexto de seguridad EPS dado, un valor CONTEO DE NAS dado se aceptará como máximo una vez y solo si la integridad del mensaje se verifica correctamente.

Se puede usar un proceso de integridad de 128 bits en EPC/LTE. De acuerdo con TS 33.401 (también denominado referencia [2]), los parámetros de entrada para el proceso de integridad de 128 bits son una clave de integridad de 128 bits llamada CLAVE, un CONTEO de 32 bits (es decir, CONTEO DE NAS), una identidad de portador de 5 bits denominada PORTADOR, la dirección de transmisión de 1 bit (es decir, DIRECCIÓN) y el mensaje en sí (es decir, MENSAJE). El bit DIRECCIÓN puede ser 0 para enlace ascendente y 1 para enlace descendente. La longitud de bits del MENSAJE es LONGITUD. Las figuras 3A y 3B ilustran el uso del proceso de integridad de 128 bits EIA para autenticar la integridad de los mensajes. Como se muestra en la figura 3A, el emisor puede derivar MAC-I/NAS-MAC, y como se muestra en la figura 3B, el receptor puede derivar XMAC-I/XNAS-MAC.

Basándose en estos parámetros de entrada, el emisor calcula un código de autenticación de mensaje de 32 bits (MAC-I/NAS-MAC) usando el proceso de integridad EIA (también denominado algoritmo de integridad EIA) de la figura 3A. El código de autenticación del mensaje (MAC) se adjunta al mensaje cuando se envía como se muestra en la figura 1. El receptor calcula el código de autenticación de mensaje esperado (XMAC-I/XNAS-MAC) en el mensaje recibido (usando el proceso de integridad EIA de la figura 3B, también conocido como algoritmo de integridad) de la misma manera que el emisor calculó su código de autenticación de mensaje en el mensaje enviado y verifica la integridad de los datos del mensaje comparando el MAC calculado con el código de autenticación del mensaje recibido, es decir, MAC-I/NAS-MAC.

TS 24.301 (también denominado referencia [3]) describe que el emisor usa su CONTEO DE NAS almacenado localmente como entrada para el algoritmo de cifrado. El receptor usa el número de secuencia de NAS incluido en el mensaje recibido (o estimado a partir de los 5 bits del número de secuencia de NAS recibido en el mensaje) y una estimación para el contador de desbordamiento de NAS para formar la entrada CONTEO DE NAS al algoritmo de descifrado.

Se puede usar un algoritmo de cifrado de 128 bits. De acuerdo con TS 33.401 (también denominado referencia [2]), los parámetros de entrada para el proceso de cifrado (también denominado algoritmo de cifrado) son una clave de cifrado de 128 bits llamada CLAVE, un CONTEO de 32 bits (es decir, CONTEO DE NAS), una identidad de portador de 5 bits PORTADOR, la dirección de la transmisión de 1 bit (es decir, DIRECCIÓN) y la longitud del flujo de claves requerido (es decir, LONGITUD). El bit DIRECCIÓN será 0 para enlace ascendente y 1 para enlace descendente.

Las figuras 4A y 4B ilustran el cifrado de datos. Basándose en los parámetros de entrada, el proceso EEA genera el bloque de flujo de claves de salida FLUJO DE CLAVES que se usa para encriptar el bloque de texto plano de entrada TEXTO PLANO para producir el bloque de texto cifrado de salida TEXTO CIFRADO.

El soporte de conexiones múltiples de NAS terminadas en la misma AMF puede dar lugar a nuevos problemas que incluyen pruebas futuras, concurrencia, agnosticismo y/o flexibilidad.

En cuanto a las pruebas futuras, la categorización de tipos de accesos en 3GPP y no 3GPP es de hecho a prueba de futuro y se puede aplicar a cualquier nueva tecnología de acceso futura. Aunque parece que no es necesario soportar más de dos conexiones de NAS, no se puede descartar con certeza que no habrá funciones o mejoras futuras que requieran el soporte de más de dos conexiones de NAS simultáneas, una a través de accesos 3GPP y dos a través de accesos no 3GPP (por ejemplo, Wifi y satélite). Por esta razón, puede ser mejor que el nuevo mecanismo de seguridad no se limite a dos conexiones y que soporte de manera eficiente un número arbitrario (hasta un límite) de conexiones simultáneas.

En cuanto a la concurrencia, la introducción de conexiones múltiples de NAS puede causar problemas de concurrencia, ya que ahora es posible que el sistema se ejecute en paralelo con múltiples procedimientos NAS en los diferentes tramos del NAS. Es concebible ordenar que la AMF ejecute los procedimientos NAS de uno en uno, independientemente de la conexión de NAS, de modo que se conserven las suposiciones subyacentes del mecanismo de seguridad heredado. No es de esperar. Por ejemplo, un procedimiento NAS fallido en una conexión de NAS puede poner en espera todas las operaciones en curso en la otra conexión de NAS, por ejemplo, hasta que expire un temporizador de fallo. Esta puede ser una elección de diseño indeseable. Por lo tanto, puede ser mejor que el nuevo mecanismo de seguridad soporte la ejecución paralela de procedimientos NAS en las diferentes conexiones.

En cuanto al agnosticismo, se espera que el nuevo mecanismo de seguridad brinde los mismos servicios de seguridad independientemente del tipo de acceso. Los servicios de seguridad pueden incluir integridad, confidencialidad y protección de reproducción. Los servicios de seguridad deben proporcionarse de manera transparente para el tipo de acceso, en línea con el principio de diseño general de una arquitectura 5G agnóstica de acceso.

En cuanto a la flexibilidad, la nueva característica de conexiones múltiples de NAS puede dar lugar a nuevos escenarios que no eran posibles en los sistemas heredados. Por ejemplo, una conexión de NAS a través de un tipo de acceso podría estar constantemente activa mientras que otra a través de un tipo de acceso diferente, abusando de la terminología, parpadea. Más precisamente, el UE puede registrarse en un tramo NAS mientras oscila entre los dos estados de registro en el otro tramo. Esto sin mencionar que, mientras tanto, el UE podría realizar varios traspasos que implican cambios de AMF. Por lo tanto, el nuevo mecanismo de seguridad puede ser deseablemente lo suficientemente flexible para soportar tales escenarios de movilidad.

De acuerdo con algunas realizaciones de conceptos de la invención, se pueden proporcionar métodos para asegurar conexiones de NAS paralelas. Tales métodos pueden basarse en compartir parcialmente el contexto de seguridad de modo que la clave maestra (equivalente a KASME en 5G) se comparta para diferentes conexiones de NAS con el mismo terminal inalámbrico, mientras que para cada conexión de NAS con el mismo terminal inalámbrico hay una par de CONTEOS DE NAS basados en el uso de un parámetro NAS llamado IDENTIFICACIÓN DE CONEXIÓN DE NAS (identificación de conexión de NAS) para identificar cada conexión de NAS con el mismo terminal inalámbrico.

De acuerdo con algunas realizaciones, los métodos/dispositivos divulgados pueden abordar problemas relacionados con pruebas futuras, concurrencia, agnosticismo y flexibilidad, al tiempo que proporcionan un nivel similar o igual de servicios de seguridad y protección en relación con la conexión de NAS que en los sistemas heredados.

Con respecto a las conexiones múltiples de NAS, se pueden hacer las siguientes suposiciones.

Primero, puede haber una clave específica de AMF denotada por KAMF que es el equivalente de KASME en los sistemas 5G. Esta clave se establece mediante una autenticación exitosa y se usa para derivar las claves de protección del protocolo de NAS, es decir, KNASint y KNASenc.

En segundo lugar, el sistema puede proporcionar/garantizar la entrega en orden de los mensajes de NAS en cada tramo (conexión). Más particularmente, los supuestos de transporte NAS subyacentes de los sistemas heredados pueden seguir aplicándose pero por conexión de NAS, pero esto no excluye las ejecuciones paralelas de los procedimientos NAS en diferentes conexiones.

En tercer lugar, la elección de los procesos criptográficos (también denominados algoritmos criptográficos) puede aplicarse a todas las conexiones de NAS de forma indiscriminada. En otras palabras, se puede suponer que no existe una negociación de seguridad específica de la conexión de NAS. Se espera que la negociación tenga lugar una vez durante el establecimiento y activación de la clave AMF, por ejemplo, el procedimiento NAS SMC equivalente en 5G. El procedimiento NAS SMC (comando de modo de seguridad) se describe en detalle en TS 33.401 (también denominado referencia [2]).

También se puede suponer que la seguridad de NAS es una función adicional del NAS que proporciona servicios de seguridad a la entidad de gestión del protocolo de NAS, como se ilustra en las figuras 8 y 9. Aunque esto podría dejarse a la implementación, los modelos de referencia de las figuras 8 y 9 se proporcionan como ejemplos. Para la recepción de mensajes de NAS de enlace ascendente y la transmisión de mensajes de NAS de enlace descendente, las operaciones de la entidad de protocolo de NAS (incluyendo la función de seguridad de NAS y la función de gestión de conexión de NAS) de la figura 8 pueden ser realizadas por el procesador 703 del nodo 501 de red. Para la recepción de mensajes de NAS de enlace descendente y la transmisión de mensajes de NAS de enlace ascendente, las operaciones de la entidad de protocolo de NAS (incluida la función de seguridad de NAS y la función de gestión de conexión de NAS) de la figura 9 pueden realizarse mediante el procesador 603 del terminal inalámbrico 505 de la figura 6.

Por ejemplo, los servicios de seguridad de NAS pueden proporcionarse mediante una función de seguridad autónoma que interactúa con las otras entidades o funciones del protocolo de NAS. Por ejemplo, la función de

gestión de conexión de NAS puede reenviar mensajes protegidos recibidos en el enlace ascendente a la función de seguridad que realiza las comprobaciones y operaciones criptográficas y devuelve el resultado (por ejemplo, si la comprobación de integridad falla o pasa, y/o si el mensaje es descifrado, etc.). Cuando se va a proteger un mensaje en el enlace descendente, la función de gestión de la conexión de NAS proporciona la carga útil a la función de seguridad que realiza las operaciones necesarias y devuelve el mensaje protegido.

Las figuras 8 y 9 ilustran las funciones de seguridad de NAS en un nodo de red central y en un terminal inalámbrico, respectivamente.

Para 5G, se espera que el contexto de seguridad de NAS pueda incluir la KAMF de clave AMF, las claves de protección derivadas KNASint y KNASenc, y el identificador de conjunto de claves equivalente a eKSI en 5G. De acuerdo con algunas realizaciones de la presente divulgación, puede usarse un par separado de CONTEOS DE NAS para cada conexión de NAS con un terminal inalámbrico en este contexto de seguridad de NAS.

Como se explicó anteriormente, para cada conexión de NAS, se puede usar/mantener un par separado de CONTEOS DE NAS, uno para cada dirección. Dado que las claves de seguridad se comparten y para reducir/evitar la reutilización del flujo de claves, se pueden usar/requerir métodos para la separación criptográfica. Para este propósito, se puede introducir un parámetro específico de conexión de NAS, y este parámetro específico de conexión de NAS puede denominarse identificador de conexión de NAS e indicarse como IDENTIFICACIÓN DE CONEXIÓN DE NAS.

La IDENTIFICACIÓN DE CONEXIÓN DE NAS es un número que se incrementa cada vez que se configura una nueva conexión de NAS para un terminal inalámbrico. En el contexto de seguridad, cada par de CONTEO DE NAS está asociado con un valor de IDENTIFICACIÓN DE CONEXIÓN DE NAS única. El nuevo parámetro se usa como diferenciador al interactuar con la función de seguridad de NAS para indicar a qué conexión de NAS pertenece cada mensaje. Para realizar un seguimiento de los valores de IDENTIFICACIÓN DE CONEXIÓN DE NAS no asignados, se puede usar/necesitar un parámetro adicional. Este nuevo parámetro, denotado por SIGUIENTE IDENTIFICACIÓN DE CONEXIÓN DE NAS también puede ser parte del contexto de seguridad. El parámetro SIGUIENTE IDENTIFICACIÓN DE CONEXIÓN DE NAS se establece inicialmente en 0 y se incrementa cada vez que se configura una nueva conexión de NAS para un terminal inalámbrico. Cada vez que se crea una nueva conexión de NAS para un terminal inalámbrico, se asigna como identificador el valor actual de SIGUIENTE IDENTIFICACIÓN DE CONEXIÓN DE NAS. Más particularmente, se crea un nuevo par de CONTEO DE NAS y se asocia con una IDENTIFICACIÓN DE CONEXIÓN DE NAS cuyo valor se establece en el valor actual del SIGUIENTE IDENTIFICACIÓN DE CONEXIÓN DE NAS. A continuación, se incrementa el valor de SIGUIENTE IDENTIFICACIÓN DE CONEXIÓN DE NAS. La identificación de conexión de NAS IDENTIFICACIÓN DE CONEXIÓN DE NAS se puede usar como entrada (directa o indirectamente) para procesos de autenticación y/o cifrado/descifrado.

De acuerdo con algunas realizaciones de conceptos de la invención, cuando se crea un nuevo par de CONTEO DE NAS, los valores de los contadores se establecen en 0. La IDENTIFICACIÓN DE CONEXIÓN DE NAS puede ser un valor de 8 bits que se usa para rellenar la representación interna de CONTEO DE NAS de 24 bits al construir la entrada a los procesos de cifrado/descifrado y/o integridad de NAS. En los sistemas heredados, el relleno siempre se puede establecer en 0 como se describe en TS 24.301 (también denominado referencia [3]). Dado que cada conexión de NAS se identifica mediante una ID DE CONEXIÓN DE NAS única, el relleno proporciona/garantiza la separación criptográfica de los mensajes que viajan a través de diferentes conexiones de NAS.

Las figuras 10A y 10B ilustran el uso del proceso de integridad EIA (también denominado algoritmo de integridad EIA) para autenticar la integridad de los mensajes usando la IDENTIFICACIÓN DE CONEXIÓN DE NAS en los lados del emisor y del receptor. Al incorporar la identificación de conexión de NAS IDENTIFICACIÓN DE CONEXIÓN DE NAS en la entrada CONTEO, se puede proporcionar una separación para la autenticación de diferentes conexiones de NAS para el mismo terminal inalámbrico. La entrada CONTEO, por ejemplo, puede ser un valor de 32 bits generado como una concatenación de la IDENTIFICACIÓN DE CONEXIÓN DE NAS de 8 bits para la conexión de NAS y el CONTEO DE NAS de 24 bits para la conexión de NAS (es decir, CONTEO (32 bits) = IDENTIFICACIÓN DE CONEXIÓN DE NAS (8 bits) CONTEO DE NAS (24 bits)). La figura 10A ilustra por tanto el uso de la IDENTIFICACIÓN DE CONEXIÓN DE NAS para derivar MAC-I/NAS-MAC en el lado del transmisor, y la figura 10B ilustra el uso de la IDENTIFICACIÓN DE CONEXIÓN DE NAS para derivar XMAC-I/XNAS-MAC en el lado del receptor.

Las figuras 11A y 11B ilustran el uso del algoritmo de cifrado/descifrado EEA para cifrar/descifrar mensajes usando la IDENTIFICACIÓN DE CONEXIÓN DE NAS en los lados del emisor y del receptor. Al incorporar la identificación de conexión de NAS IDENTIFICACIÓN DE CONEXIÓN DE NAS en la entrada CONTEO, se puede proporcionar una separación para cifrar/descifrar diferentes conexiones de NAS para el mismo terminal inalámbrico. La entrada CONTEO, por ejemplo, puede ser un valor de 32 bits generado como una concatenación de la IDENTIFICACIÓN DE CONEXIÓN DE NAS de 8 bits para la conexión de NAS y el CONTEO DE NAS de 24 bits para la conexión de NAS (es decir, CONTEO (32 bits) = IDENTIFICACIÓN DE CONEXIÓN DE NAS (8 bits) || CONTEO DE NAS (24 bits)). Por tanto, la figura 11A ilustra el uso de la IDENTIFICACIÓN DE CONEXIÓN DE NAS para cifrar el texto sin formato

en el lado del transmisor, y la figura 11B ilustra el uso de la IDENTIFICACIÓN DE CONEXIÓN DE NAS para descifrar el texto cifrado en el lado del receptor.

De acuerdo con algunas otras realizaciones, la IDENTIFICACIÓN DE CONEXIÓN DE NAS puede ser un valor de 5 bits que se usa como entrada de PORTADOR para procesos de autenticación y/o cifrado/descifrado como se describe a continuación.

Las figuras 12A y 12B ilustran el uso del algoritmo de integridad EIA para autenticar la integridad de los mensajes usando la IDENTIFICACIÓN DE CONEXIÓN DE NAS en los lados del emisor y del receptor. Al usar la identificación de conexión de NAS IDENTIFICACIÓN DE CONEXIÓN DE NAS como entrada PORTADOR, se puede proporcionar una separación para la autenticación de diferentes conexiones de NAS para el mismo terminal inalámbrico. La figura 12A ilustra el uso de IDENTIFICACIÓN DE CONEXIÓN DE NAS como la entrada PORTADOR para derivar MAC-I/NAS-MAC en el lado del transmisor, y la figura 12B ilustra el uso de IDENTIFICACIÓN DE CONEXIÓN DE NAS como la entrada PORTADOR para derivar XMAC-I/XNAS- MAC en el lado del receptor.

Las figuras 13A y 13B ilustran el uso del proceso de cifrado/descifrado EEA para cifrar/descifrar mensajes usando la IDENTIFICACIÓN DE CONEXIÓN DE NAS en los lados del emisor y del receptor. Al usar la identificación de conexión de NAS IDENTIFICACIÓN DE CONEXIÓN DE NAS como entrada PORTADOR, se puede proporcionar una separación para cifrar/descifrar diferentes conexiones de NAS para el mismo terminal inalámbrico. La figura 13A ilustra el uso de IDENTIFICACIÓN DE CONEXIÓN DE NAS como la entrada PORTADOR para cifrar el texto sin formato en el lado del transmisor, y la figura 13B ilustra el uso de IDENTIFICACIÓN DE CONEXIÓN DE NAS como la entrada PORTADOR para descifrar el texto cifrado en el lado del receptor.

Las operaciones que proporcionan autenticación de integridad y/o cifrado/descifrado de las figuras 10A-B, 11A-B, 12A-B y/o 13A-B se explicarán ahora con respecto al diagrama de flujo de las figuras 17A y 17B.

Las operaciones de un nodo de comunicación se explicarán ahora con referencia al diagrama de flujo de la figura 17A y los módulos de la figura 17B. Por ejemplo, los módulos de la figura 17B pueden almacenarse en la memoria del nodo de comunicación (por ejemplo, la memoria 605 del terminal inalámbrico de la figura 6 si el nodo de comunicación es un terminal inalámbrico, o la memoria 705 del nodo de red de la figura 7 si el nodo de comunicación es un nodo de red), y estos módulos pueden proporcionar instrucciones para que cuando las instrucciones de un módulo sean ejecutadas por el procesador de nodo de comunicación (por ejemplo, el procesador 603 de terminal inalámbrico si el nodo de comunicación es un terminal inalámbrico, o el procesador 705 de nodo de red si el nodo de comunicación es un nodo de red), el procesador realiza las operaciones respectivas del diagrama de flujo de la figura 17A.

Como se explicó anteriormente con respecto a la figura 5, se pueden proporcionar la primera y la segunda conexión de NAS entre el primer y el segundo nodo de comunicación, tales como entre el terminal inalámbrico 505 y el nodo 501 de red (por ejemplo, un nodo de red central). El procesador de nodo de comunicación puede proporcionar una primera identificación de conexión de NAS para una primera conexión de NAS entre el primer y el segundo nodo de comunicación en el bloque 1711 (por ejemplo, usando el primer módulo 1751 de identificación). El procesador de nodo de comunicación también puede proporcionar una segunda identificación de conexión de NAS para una segunda conexión de NAS entre el primer y el segundo nodo de comunicación en el bloque 1713 (por ejemplo, usando el segundo módulo 1753 de identificación). Además, la primera y la segunda identificación de la conexión de NAS son diferentes, y la primera y la segunda conexión de NAS son diferentes.

Para una comunicación a través de la primera conexión de NAS en el bloque 1717, el procesador de nodo de comunicación puede comunicar un primer mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la primera conexión de NAS (por ejemplo, usando el primer módulo 1757 de comunicación). Más particularmente, comunicar el primer mensaje de NAS puede incluir al menos uno de realizar la protección de integridad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y/o realizar la protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS.

Para una comunicación a través de la segunda conexión de NAS en el bloque 1719, el procesador de nodo de comunicación puede comunicar un segundo mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la segunda conexión de NAS (por ejemplo, usando el segundo módulo 1759 de comunicación). Más particularmente, comunicar el segundo mensaje de NAS puede incluir al menos uno de realizar al menos uno de realizar la protección de integridad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y/o realizar la protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS.

La primera y la segunda conexión de NAS comparten una clave maestra de un contexto de seguridad de NAS. Además, comunicar el primer mensaje de NAS puede incluir al menos uno de realizar la protección de integridad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra y/o realizar la protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y la llave maestra. De manera similar, comunicar el segundo mensaje de NAS puede incluir al menos uno de

realizar la protección de integridad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave maestra y/o realizar la protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la llave maestra.

Las operaciones de la figura 17A pueden ser realizadas por un nodo de comunicación que está transmitiendo mensajes de NAS (por ejemplo, el terminal inalámbrico 505 en el enlace ascendente, o el nodo 501 de red en el enlace descendente). Como se explicó anteriormente, la primera y la segunda conexión de NAS pueden compartir una clave maestra de un contexto de seguridad de NAS. En el bloque 1717, la comunicación del primer mensaje de NAS puede incluir realizar la protección de integridad generando un primer código de autenticación de mensaje basándose en la primera identificación de conexión de NAS, la clave maestra y el primer mensaje de NAS, y transmitir el primer mensaje de NAS con el primer código de autenticación de mensaje a través de la primera conexión de NAS al segundo nodo de comunicación. En el bloque 1719, comunicar el segundo mensaje de NAS puede incluir realizar la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basándose en la identificación de la segunda conexión de NAS, la clave maestra y el segundo mensaje de NAS, y transmitir el segundo mensaje de NAS con el segundo código de autenticación de mensaje a través de la segunda conexión de NAS al segundo nodo de comunicación.

De acuerdo con algunas realizaciones para el nodo de transmisión, la primera identificación de conexión de NAS puede concatenarse con un primer conteo de NAS para el primer mensaje de NAS, la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS pueden proporcionarse como entrada para generar el primer código de autenticación de mensaje, la segunda identificación de conexión de NAS puede concatenarse con un segundo conteo de NAS para el segundo mensaje de NAS, y la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS pueden proporcionarse como una entrada para generar el segundo código de autenticación de mensaje. De acuerdo con algunas otras realizaciones para el nodo de transmisión, la primera identificación de conexión de NAS puede proporcionarse como entrada para generar el primer código de autenticación de mensaje, y la segunda identificación de conexión de NAS puede proporcionarse como entrada para generar el segundo código de autenticación de mensaje. De acuerdo con otras realizaciones más para el nodo de transmisión, la clave maestra y la primera identificación de conexión de NAS pueden usarse para derivar una primera clave de protección de integridad usada para generar el primer código de autenticación de mensaje, y la clave maestra y la segunda identificación de conexión de NAS pueden usarse para derivar una segunda clave de protección de integridad usada para generar el segundo código de autenticación de mensaje. Además, realizar la protección de integridad para el primer mensaje de NAS puede incluir realizar la protección de integridad para el primer mensaje de NAS usando una interfaz de protección de integridad EIA compatible con 5G, y realizar la protección de integridad para el segundo mensaje de NAS puede incluir realizar la protección de integridad para el segundo mensaje de NAS usando la interfaz de protección de integridad EIA compatible con 5G.

Las operaciones de la figura 17A pueden ser realizadas por un nodo de comunicación que está transmitiendo mensajes de NAS (por ejemplo, terminal inalámbrico 505 en el enlace ascendente, o nodo 501 de red en el enlace descendente). Como se explicó anteriormente, la primera y la segunda conexión de NAS pueden compartir una clave maestra de un contexto de seguridad de NAS. En el bloque 1717, comunicar el primer mensaje de NAS puede incluir realizar la protección de confidencialidad para el primer mensaje de NAS cifrando el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra para proporcionar un primer mensaje de NAS cifrado y transmitir el primer mensaje de NAS cifrado a través de la primera conexión de NAS al segundo nodo de comunicación. En el bloque 1719, la comunicación del segundo mensaje de NAS puede incluir realizar la protección de confidencialidad para el segundo mensaje de NAS cifrando el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave maestra para proporcionar un segundo mensaje de NAS cifrado, y transmitir el segundo mensaje de NAS cifrado a través de la segunda conexión de NAS al segundo nodo de comunicación.

De acuerdo con algunas realizaciones para el nodo de transmisión, la primera identificación de conexión de NAS puede concatenarse con un primer conteo de NAS para el primer mensaje de NAS, la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS pueden proporcionarse como entrada para generar el primer mensaje de NAS cifrado, la segunda identificación de conexión de NAS puede concatenarse con un segundo conteo de NAS para el segundo mensaje de NAS, y la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS pueden proporcionarse como entrada para generar el segundo mensaje de NAS cifrado. De acuerdo con algunas otras realizaciones del nodo de transmisión, la primera identificación de conexión de NAS puede proporcionarse como entrada para generar el primer mensaje de NAS cifrado, y la segunda identificación de conexión de NAS puede proporcionarse como entrada para generar el segundo mensaje de NAS cifrado. De acuerdo con otras realizaciones más del nodo de transmisión, la clave maestra y la primera identificación de conexión de NAS pueden usarse para derivar una primera clave de cifrado que se usa para generar el primer mensaje de NAS cifrado, y la clave maestra y la segunda identificación de conexión de NAS pueden usarse para derivar una segunda clave de cifrado que se usa para generar el segundo mensaje de NAS cifrado. El cifrado del primer mensaje de NAS puede incluir el cifrado del primer mensaje de NAS usando el cifrado EEA, y el cifrado del segundo mensaje de NAS comprende el cifrado del segundo mensaje de NAS usando el cifrado EEA. Además, la protección de confidencialidad para el primer mensaje de NAS puede incluir la protección de confidencialidad para el primer mensaje de NAS usando una interfaz de cifrado EEA compatible con 5G, y la protección de confidencialidad

para el segundo mensaje de NAS puede incluir la protección de confidencialidad para el segundo mensaje de NAS usando la interfaz de cifrado EEA compatible con 5G.

Las operaciones de la figura 17A pueden ser realizadas por un nodo de comunicación que está recibiendo mensajes de NAS (por ejemplo, un terminal inalámbrico en el enlace descendente o un nodo de red del enlace ascendente). Como se explicó anteriormente, la primera y la segunda conexión de NAS pueden compartir una clave maestra de un contexto de seguridad de NAS. En el bloque 1715, comunicar el primer mensaje de NAS puede incluir recibir el primer mensaje de NAS con un primer código de autenticación de mensaje a través de la primera conexión de NAS desde el segundo nodo de comunicación, realizar la protección de integridad del primer mensaje de NAS generando un primer código de autenticación de mensaje derivado para el primer mensaje de NAS basándose en la primera identificación de conexión de NAS, la clave maestra y el primer mensaje de NAS, y procesar el primer mensaje de NAS en respuesta al primer código de autenticación de mensaje y la primera coincidencia de código de autenticación de mensaje derivado. En el bloque 1719, comunicar el segundo mensaje de NAS puede incluir recibir el segundo mensaje de NAS con un segundo código de autenticación de mensaje a través de la segunda conexión de NAS desde el segundo nodo de comunicación, realizar la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje derivado para el segundo mensaje de NAS basándose en la segunda identificación de conexión de NAS, la clave maestra y el segundo mensaje de NAS, y procesar el segundo mensaje de NAS en respuesta al segundo código de autenticación de mensaje y la segunda coincidencia de código de autenticación de mensaje derivado.

De acuerdo con algunas realizaciones para el nodo de recepción, la primera identificación de conexión de NAS puede concatenarse con un primer conteo de NAS para el primer mensaje de NAS, la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS pueden proporcionarse como una entrada para generar el primer código de autenticación de mensaje derivado, la segunda identificación de conexión de NAS puede concatenarse con un segundo conteo de NAS para el segundo mensaje de NAS, y la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS pueden proporcionarse como entrada para generar el segundo código de autenticación del mensaje. De acuerdo con algunas otras realizaciones para el nodo de recepción, la primera identificación de conexión de NAS puede proporcionarse como entrada para generar el primer código de autenticación de mensaje derivado, y la segunda identificación de conexión de NAS puede proporcionarse como entrada para generar el segundo código de autenticación de mensaje derivado. De acuerdo con otras realizaciones más para el nodo de recepción, la clave maestra y la primera identificación de conexión de NAS pueden usarse para derivar una primera clave de protección de integridad usada para generar el primer código de autenticación de mensaje derivado, y la clave maestra y la segunda identificación de conexión de NAS pueden usarse para obtener una segunda clave de protección de integridad usada para generar el segundo código de autenticación de mensaje derivado. Además, realizar la protección de integridad para el primer mensaje de NAS puede incluir realizar la protección de integridad para el primer mensaje de NAS usando una interfaz de protección de integridad EIA compatible con 5G, y realizar la protección de integridad para el segundo mensaje de NAS puede incluir realizar la protección de integridad para el segundo mensaje de NAS usando la interfaz de protección de integridad EIA compatible con 5G.

Las operaciones de la figura 17A pueden ser realizadas por un nodo de comunicación que está recibiendo mensajes de NAS (por ejemplo, un terminal inalámbrico en el enlace descendente o un nodo de red del enlace ascendente). Como se explicó anteriormente, la primera y la segunda conexión de NAS pueden compartir una clave maestra de un contexto de seguridad de NAS. En el bloque 1717, comunicar el primer mensaje de NAS puede incluir recibir un primer mensaje de NAS cifrado a través de la primera conexión de NAS desde el segundo nodo de comunicación, realizar la protección de confidencialidad para el primer mensaje de NAS descifrando el primer mensaje de NAS cifrado usando la primera identificación de conexión de NAS y la clave maestra para proporcionar un primer mensaje de NAS descifrado y procesar el primer mensaje de NAS descifrado. En el bloque 1719, comunicar el segundo mensaje de NAS puede incluir recibir un segundo mensaje de NAS cifrado a través de la segunda conexión de NAS desde el segundo nodo de comunicación, realizar la protección de confidencialidad para el segundo mensaje de NAS descifrando el segundo mensaje de NAS cifrado usando la segunda identificación de conexión de NAS y la clave maestra para proporcionar un segundo mensaje de NAS descifrado y procesar el segundo mensaje de NAS descifrado.

De acuerdo con algunas realizaciones para el nodo de recepción, la primera identificación de conexión de NAS puede concatenarse con un primer conteo de NAS para el primer mensaje de NAS, la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS pueden proporcionarse como una entrada para generar el primer mensaje de NAS descifrado, la segunda identificación de conexión de NAS puede concatenarse con un segundo conteo de NAS para el segundo mensaje de NAS, y la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS pueden proporcionarse como entrada para generar el segundo mensaje de NAS cifrado. De acuerdo con algunas otras realizaciones para el nodo de recepción, la primera identificación de conexión de NAS puede proporcionarse como entrada para generar el primer mensaje de NAS descifrado, y la segunda identificación de conexión de NAS puede proporcionarse como entrada para generar el segundo mensaje de NAS descifrado. De acuerdo con otras realizaciones más para el nodo de recepción, la clave maestra y la primera identificación de conexión de NAS pueden usarse para derivar una primera clave de descifrado usada para generar el primer mensaje de NAS descifrado, y la clave maestra y la segunda identificación de conexión

de NAS pueden usarse para derivar una segunda clave de descifrado usada para generar el segundo mensaje de NAS descifrado. Además, realizar la protección de confidencialidad para el primer mensaje de NAS puede incluir la protección de confidencialidad para el primer mensaje de NAS usando una interfaz de descifrado EEA compatible con 5G, y realizar la protección de confidencialidad para el segundo mensaje de NAS puede incluir la protección de confidencialidad para el segundo mensaje de NAS usando la interfaz de descifrado EEA compatible con 5G.

En las realizaciones de la figura 17A, la primera conexión de NAS puede proporcionarse a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación, y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación; o la primera conexión de NAS puede proporcionarse a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación. Por ejemplo, el nodo de acceso 3GPP puede incluir una estación base de la red de acceso por radio, y el nodo de acceso no 3GPP puede incluir al menos uno de un nodo de acceso WiFi y/o un nodo de acceso de satélite.

Además, la primera y la segunda conexión de NAS de la figura 17A pueden mantenerse simultáneamente entre el primer y el segundo nodo de comunicación. Además, se puede establecer una sesión de unidad de paquete de datos (PDU) basándose en el primer y el segundo mensaje de NAS para comunicar los datos de plano de usuario entre el primer y el segundo nodo de comunicación.

Varias operaciones de la figura 17A y/o módulos de la figura 17B pueden ser opcionales con respecto a algunas realizaciones de nodos de comunicación y métodos relacionados. Con respecto a los métodos de la realización 1 de ejemplo (que se expone a continuación), por ejemplo, las operaciones del bloque 1715 de la figura 17B pueden ser opcionales.

De acuerdo con algunas otras realizaciones, el dominio CONTEO DE NAS se puede dividir dependiendo del número de conexiones de NAS en ejecución como se describe a continuación. Una diferencia relativa a las realizaciones explicadas anteriormente con respecto a las figuras 10A-B, 11A-B, 12A-B y 13A-B es que la IDENTIFICACIÓN DE CONEXIÓN DE NAS puede no aumentar constantemente y, de hecho, durante el tiempo de vida de la clave KAMF, es posible que a diferentes conexiones de NAS se les asigne el mismo valor IDENTIFICACIÓN DE CONEXIÓN DE NAS.

En tales realizaciones, se puede usar un nuevo parámetro denotado por NÚMERO DE CONEXIÓN DE NAS para realizar un seguimiento del número de conexiones de NAS en ejecución para un terminal inalámbrico. Además, se puede usar un par especial de CONTEOS DE NAS para realizar un seguimiento de los valores máximos de los CONTEOS en el enlace ascendente y descendente en todos los pares de CONTEO DE NAS disponibles. Este parámetro puede denominarse par de CONTEOS DE NAS MÁXIMOS. Inicialmente, todos los parámetros se establecen en 0. Cuando se configura una nueva conexión de NAS para un terminal inalámbrico, a la nueva conexión de NAS se le asigna el valor NÚMERO DE CONEXIÓN DE NAS actual como la IDENTIFICACIÓN DE CONEXIÓN DE NAS. Se crea un nuevo par de CONTEOS DE NAS con su valor establecido en los valores de CONTEO DE NAS MÁXIMO actuales añadidos a la conexión de IDENTIFICACIÓN DE CONEXIÓN DE NAS. Para todas las conexiones existentes, los valores de CONTEO DE NAS se ajustan a los valores actuales de CONTEO DE NAS MÁXIMOS y se agregan el valor de IDENTIFICACIÓN DE CONEXIÓN DE NAS correspondiente. Finalmente, se incrementa el NÚMERO DE CONEXIÓN DE NAS.

En caso de que se termine una conexión de NAS, entonces el NÚMERO DE CONEXIÓN DE NAS se reduce, todas las conexiones con un identificador sobre el de la conexión eliminada se reducen y todos los CONTEOS DE NAS se ajustan como en el caso de adición de conexión. Siempre que un mensaje de NAS se procesa correctamente (para su transmisión o recepción), para esa conexión de NAS, el valor CONTEO DE NAS es incrementado por el NÚMERO DE CONTEO DE NAS. Intuitivamente, el NÚMERO DE CONEXIÓN DE NAS se usa como incremento para todos los CONTEOS DE NAS. Sin embargo, para reducir/evitar la superposición, cada vez que se establece o cancela una conexión, los CONTEOS DE NAS se reajustan basándose en los valores de CONTEO DE NAS MÁXIMO actuales y los correspondientes (posiblemente reajustados) IDENTIFICACIONES DE CONEXIÓN DE NAS.

Esta realización puede no proporcionar/garantizar un uso eficiente/bueno del dominio CONTEO DE NAS. En caso de que una conexión de NAS sea más activa que las otras (impulsando los valores de CONTEO DE NAS MÁXIMO), la terminación de la conexión de NAS más activa puede provocar un salto adelante en los valores CONTEO DE NAS de las conexiones restantes y, por lo tanto, un desperdicio de los valores CONTEO DE NAS.

Las operaciones de un nodo de comunicación se explicarán ahora con referencia al diagrama de flujo de la figura del diagrama de flujo de la figura 18A y los módulos de la figura 18B. Por ejemplo, los módulos de la figura 18 pueden almacenarse en la memoria del nodo de comunicación (por ejemplo, la memoria 605 de terminal inalámbrico de la figura 6 si el nodo de comunicación es un terminal inalámbrico, o la memoria 705 de nodo de comunicación de la figura 7 si el nodo de comunicación es un nodo de red), y estos módulos pueden proporcionar instrucciones de modo que cuando las instrucciones de un módulo son ejecutadas por el procesador de nodo de comunicación (por ejemplo, el procesador 603 de terminal inalámbrico si el nodo de comunicación es un terminal inalámbrico, o el

procesador 705 de nodo de red si el nodo de comunicación es un nodo de red), el procesador realiza las respectivas operaciones del diagrama de flujo de la figura 18A.

El procesador de nodo de comunicación puede proporcionar una primera conexión de NAS entre el primer y el segundo nodo de comunicación en el bloque 1801 (por ejemplo, usando el primer módulo 1851 de conexión de NAS), y el procesador de nodo de comunicación puede proporcionar una segunda conexión de NAS entre el primer y el segundo nodo de comunicación en el bloque 1803 (por ejemplo, usando el segundo módulo 1853 de conexión de NAS). Además, la primera y la segunda conexión de NAS pueden ser diferentes.

El procesador de nodo de comunicación puede asignar un dominio conteo de NAS en el bloque 1805 (por ejemplo, usando el módulo 1855 de asignación) de modo que una primera porción del dominio conteo de NAS se asigne para mensajes de NAS comunicados a través de la primera conexión de NAS y de modo que una segunda porción del dominio conteo de NAS se asigna a los mensajes de NAS comunicados a través de la segunda conexión de NAS. Además, la primera y la segunda porción del dominio conteo de NAS pueden ser mutuamente excluyentes.

Para una comunicación NAS en el bloque 1807, el procesador de nodo de comunicación puede determinar qué conexión se usa en el bloque 1809. El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la primera conexión de NAS en el bloque 1811 usando un valor de conteo de NAS más bajo de la primera porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la primera conexión de NAS (por ejemplo, usando el primer módulo 1851 de comunicación NAS). El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la segunda conexión de NAS en el bloque 1813 usando un valor de conteo de NAS más bajo de la segunda porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS (por ejemplo, usando un segundo módulo 1853 de comunicación NAS).

Los valores de conteo de NAS de la primera y la segunda porción del dominio conteo de NAS pueden estar intercalados. Con dos conexiones de NAS, la primera porción del dominio conteo de NAS puede incluir valores de conteo de NAS pares, y la segunda porción del dominio conteo de NAS puede incluir valores de conteo de NAS impares. Con tal partición del dominio conteo de NAS, a los mensajes de NAS comunicados a través de la primera conexión de NAS se les pueden asignar números de secuencia 0, 2, 4, 6, 8, etc. de la primera porción del dominio conteo de NAS, y a los mensajes de NAS comunicados a través de segunda conexión de NAS se les pueden asignar los números de secuencia 1, 3, 5, 7, etc. de la segunda porción del dominio conteo de NAS. Además, si una de las conexiones de NAS está más activa, se pueden asignar más números de secuencia de una porción del dominio conteo de NAS que de la otra porción del dominio conteo de NAS. A modo de ejemplo, si se transmiten 8 mensajes de NAS a través de la primera conexión de NAS y se transmiten 3 mensajes de NAS a través de la segunda conexión de NAS, los números de secuencia 0, 2, 4, 6, 8, 10, 12 y 14 pueden asignarse respectivamente a los mensajes de NAS transmitidos a través de la primera conexión de NAS, los números de secuencia 1, 3 y 5 pueden asignarse respectivamente a los mensajes de NAS transmitidos a través de la segunda conexión de NAS, y el valor de CONTEO DE NAS MÁXIMO será 14.

Las operaciones de los bloques 1807, 1809, 1811 y 1813 pueden repetirse en el bloque 1815 hasta que se produzca un cambio en las conexiones. En el bloque 1816, por ejemplo, el procesador de nodo de comunicación puede proporcionar una tercera conexión de NAS entre el primer y el segundo nodo de comunicación (por ejemplo, usando el tercer módulo 1856 de conexión de NAS). La primera y la tercera conexión de NAS son diferentes, y la segunda y la tercera conexión de NAS son diferentes. Además, el procesador de nodo de comunicación puede reasignar el dominio conteo de NAS en el bloque 1817 (por ejemplo, usando el módulo 1857 de reasignación). Tras la reasignación, una primera porción del dominio conteo de NAS puede asignarse para mensajes de NAS comunicados a través de la primera conexión de NAS, una segunda porción del dominio conteo de NAS puede asignarse para mensajes de NAS comunicados a través de la segunda conexión de NAS, y una tercera porción del dominio conteo de NAS puede asignarse para mensajes de NAS comunicados a través de la tercera conexión de NAS, con la primera, la segunda y la tercera porción del dominio conteo de NAS siendo mutuamente excluyentes.

Continuando con el ejemplo anterior, si el valor de CONTEO DE NAS MÁXIMO es 18, la reasignación puede ocurrir para los valores de conteo de NAS superiores a 14, por lo que los valores de conteo de NAS 7, 9, 11 y 13 no se usan. De acuerdo con tal ejemplo, después de la reasignación, la primera porción del dominio conteo de NAS puede incluir valores de conteo de NAS mayores que 14 que son divisibles por 3 (por ejemplo, 15, 18, 21, 24, etc.), la segunda porción del dominio conteo de NAS puede incluir valores de conteo de NAS mayores que 14 para los cuales la división por 3 proporciona un resto de 1 (por ejemplo, 16, 19, 22, 25, etc.), y la tercera porción del dominio conteo de NAS puede incluir valores de conteo de NAS mayores que 14 para lo cual la división entre 3 proporciona un resto de 2 (por ejemplo, 17, 20, 23, 26, etc.).

Para una comunicación NAS en el bloque 1819, el procesador de nodo de comunicación puede determinar qué conexión se usa en el bloque 1821. El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la primera conexión de NAS en el bloque 1831 usando un valor de conteo de NAS más bajo de la primera porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la primera conexión de NAS (por ejemplo, usando el primer módulo 1861 de comunicación NAS). El

procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la segunda conexión de NAS en el bloque 1833 usando un valor de conteo de NAS más bajo de la segunda porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS (por ejemplo, usando un segundo módulo 1863 de comunicación NAS). El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la tercera conexión de NAS en el bloque 1835 usando un valor de conteo de NAS más bajo de la tercera porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la tercera conexión de NAS (por ejemplo, usando el segundo módulo 1865 de comunicación NAS).

De acuerdo con algunas realizaciones de la figura 18A, el primer nodo de comunicación puede ser un nodo de red, el segundo nodo de comunicación puede ser un terminal inalámbrico y el dominio conteo de NAS puede ser un dominio conteo de NAS de enlace ascendente. En consecuencia, comunicar mensajes de NAS a través de la primera conexión de NAS puede incluir recibir mensajes de NAS a través de la primera conexión de NAS, y comunicar mensajes de NAS a través de la segunda conexión de NAS puede incluir recibir mensajes de NAS a través de la segunda conexión de NAS.

De acuerdo con algunas otras realizaciones de la figura 18A, el primer nodo de comunicación puede ser un nodo de red, el segundo nodo de comunicación puede ser un terminal inalámbrico, y el dominio conteo de NAS puede ser un dominio conteo de NAS de enlace descendente. En consecuencia, comunicar mensajes de NAS a través de la primera conexión de NAS puede incluir la transmisión de mensajes de NAS a través de la primera conexión de NAS, y comunicar mensajes de NAS a través de la segunda conexión de NAS puede incluir transmitir mensajes de NAS a través de la segunda conexión de NAS.

De acuerdo con otras realizaciones más de la figura 18A, el primer nodo de comunicación puede ser un terminal inalámbrico, el segundo nodo de comunicación puede ser un nodo de red y el dominio conteo de NAS es un dominio conteo de NAS de enlace ascendente. En consecuencia, comunicar mensajes de NAS a través de la primera conexión de NAS puede incluir la transmisión de mensajes de NAS a través de la primera conexión de NAS, y comunicar mensajes de NAS a través de la segunda conexión de NAS puede incluir transmitir mensajes de NAS a través de la segunda conexión de NAS.

De acuerdo con otras realizaciones más de la figura 18A, el primer nodo de comunicación puede ser un terminal inalámbrico, el segundo nodo de comunicación puede ser un nodo de red y el dominio conteo de NAS puede ser un dominio conteo de NAS de enlace descendente. En consecuencia, comunicar mensajes de NAS a través de la primera conexión de NAS puede incluir recibir mensajes de NAS a través de la primera conexión de NAS, y comunicar mensajes de NAS a través de la segunda conexión de NAS puede incluir recibir mensajes de NAS a través de la segunda conexión de NAS.

En las realizaciones de la figura 18A, la primera conexión de NAS puede proporcionarse a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación, o la primera conexión de NAS puede proporcionarse a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación.

Además, la comunicación de mensajes de NAS a través de la primera conexión de NAS puede incluir al menos uno de realizar la protección de integridad generando códigos de autenticación de mensaje usando los valores de conteo de NAS respectivos de la primera porción del dominio conteo de NAS y/o realizar la protección de confidencialidad usando los valores de conteo de NAS respectivos desde la primera porción del dominio conteo de NAS. De manera similar, la comunicación de mensajes de NAS a través de la segunda conexión de NAS puede incluir al menos uno de realizar la protección de integridad generando códigos de autenticación de mensaje usando los valores de conteo de NAS respectivos de la segunda porción del dominio conteo de NAS y/o realizar la protección de confidencialidad usando los valores de conteo de NAS respectivos de la segunda porción del dominio conteo de NAS.

Además, la primera y la segunda conexión de NAS de la figura 18A pueden mantenerse simultáneamente entre el primer y el segundo nodo de comunicación. Además, se puede establecer una sesión de unidad de paquete de datos (PDU) basándose en el primer y el segundo mensaje de NAS para comunicar los datos de plano de usuario entre el primer y el segundo nodo de comunicación.

Varias operaciones de la figura 18A y/o módulos de la figura 18B pueden ser opcionales con respecto a algunas realizaciones de nodos de comunicación y métodos relacionados. Con respecto a los métodos de la realización 1 de ejemplo (que se expone a continuación), por ejemplo, las operaciones de los bloques 1807, 1809, 18015, 1816, 1817, 1819, 1821, 1831, 1833 y 1835 de la figura 18A pueden ser opcionales, y los módulos 1856, 1857 , 1861, 1863 y 1865 pueden ser opcionales.

De acuerdo con algunas otras realizaciones de conceptos de la invención, la separación criptográfica puede proporcionarse al nivel de las claves. Las claves de protección NAS pueden derivarse en sistemas heredados como se describe en TS 33.401 (también denominado referencia [2]).

En general, todas las derivaciones de clave (incluida la codificación de parámetros de entrada) para LTE se pueden realizar usando la función de derivación de clave (KDF) especificada en TS 33.220 (también denominado referencia [4]). La KDF toma como entrada una clave y una cadena S. La clave derivada se obtiene aplicando el HMAC-SHA-256 (descrito en RFC 2104, también denominado referencia [5]) a la clave de entrada y la cadena S. La cadena S se construye concatenando un parámetro diferenciador denominado FC y un conjunto de otros parámetros y sus longitudes respectivas: S = FC || P0 || L0 P1 || L1 || P2 || L2 || P3 || L3 || ... || Pn || Ln, donde Pi (i de 0 a n) es un parámetro y Li es su longitud en octetos.

De acuerdo con la cláusula A.7 de TS 33.401 (también denominado referencia [2]), al derivar claves para los procesos de integridad de NAS y de encriptación de NAS (también denominados como algoritmos) de KASME y los tipos de proceso/algoritmo y las ID, los siguientes parámetros pueden/deberán usarse para formar la cadena S.

- FC = 0x15

- P0 = diferenciador de tipo de proceso

- L0 = longitud del diferenciador de tipo de proceso (es decir, 0x00 0x01)

- P1 = identidad de proceso

- L1 = longitud de la identidad de proceso (es decir, 0x00 0x01)

El diferenciador de tipo de proceso será NAS-enc-alg para los procesos de encriptado NAS y NAS-int-alg para los procesos de protección de integridad de NAS (véase la tabla A.7-1). La figura 14 es una tabla que ilustra los diferenciadores de tipo de proceso.

La identidad de proceso (como se especifica en la cláusula 5 de TS 33.401, también denominado referencia [2]) puede/deberá colocarse en los cuatro bits menos significativos del octeto. Los dos bits menos significativos de los cuatro bits más significativos pueden reservarse para su futuro uso, y los dos bits más significativos de los 4 bits más significativos pueden reservarse para uso privado. Los cuatro bits más significativos pueden/deberán ponerse a todos cero.

Para derivaciones de claves de proceso NAS, la clave de entrada puede/será la KASME de 256 bits. Para una clave de proceso de longitud n bits, donde n es menor o igual a 256, los n bits menos significativos de los 256 bits de la salida KDF pueden/deben usarse como clave de proceso (también denominada clave de algoritmo).

Como se explicó anteriormente con respecto a las figuras 10A-B, 11A-B, 12A-B y 13A-B, el identificador de conexión de NAS IDENTIFICACIÓN DE CONEXIÓN DE NAS puede usarse en los procesos de autenticación y/o de cifrado/descifrado para proporcionar separación para diferentes conexiones de NAS usadas por un mismo terminal inalámbrico.

De acuerdo con algunas realizaciones, la IDENTIFICACIÓN DE CONEXIÓN DE NAS se puede usar en la derivación de las claves de protección NAS KNASenc y KNASint. Por tanto, las claves de protección resultantes pueden ser específicas de la conexión de NAS para proporcionar separación para diferentes conexiones de NAS usadas por el mismo terminal inalámbrico.

Por ejemplo, se puede introducir un nuevo parámetro P2 para la construcción de la cadena S de entrada. Este parámetro P2 sería la IDENTIFICACIÓN DE CONEXIÓN DE NAS y su longitud L2 sería cualquier longitud que tenga la IDENTIFICACIÓN DE CONEXIÓN DE NAS (en octetos). Por ejemplo, si la IDENTIFICACIÓN DE CONEXIÓN DE NAS tiene una longitud de 8 bits, entonces L2 es 1 (para un octeto). Si se especifica que la IDENTIFICACIÓN DE CONEXIÓN DE NAS tenga un valor de 32 bits, entonces L2 se establecería en la constante 4 (para cuatro octetos). Todos los demás parámetros (P0, P1) pueden permanecer iguales o pueden basarse en los equivalentes de 5G.

La figura 15 ilustra la derivación de la clave basándose en la cadena S donde se usa la IDENTIFICACIÓN DE CONEXIÓN DE NAS en la derivación de la cadena S. Aquí, la KAMF de clave maestra y S se proporcionan como entradas a la función de derivación de clave KDF para generar la CLAVE K que se usa para la autenticación EIA y/o el cifrado/descifrado EEA. En la figura 15:

• KAMF es el equivalente de KASME en 5G;

• S se construye como la concatenación FC || P0 || L0 || P1 || L1 || P2 || L2 donde:

- FC es potencialmente un nuevo diferenciador para la derivación de la clave de protección NAS,

- P0, P1, L0 y L1 se basan en parámetros potencialmente nuevos y valores equivalentes a los usados en LTE. De hecho, los algoritmos en 5G podrían tener potencialmente otros nombres y otros valores de tipo diferenciador, etc.

- P2 y L2 son los nuevos parámetros basados en la IDENTIFICACIÓN DE CONEXIÓN DE NAS.

Dependiendo del valor de FC, se usa el mismo procedimiento para derivar una clave de protección de integridad de NAS o una clave de cifrado NAS. Dado que la IDENTIFICACIÓN DE CONEXIÓN DE NAS se usa en la función de derivación, esas claves serían específicas de la conexión de NAS.

De acuerdo con algunas otras realizaciones, la IDENTIFICACIÓN DE CONEXIÓN DE NAS puede usarse para derivar un KNAS de clave de nivel nuevo a partir de la clave KAMF que luego se usa para derivar las otras claves de protección de nivel inferior. Por tanto, el KNAS y las claves de protección derivadas pueden ser específicas de la conexión de NAS.

Por ejemplo, una nueva clave llamada KNAS puede derivarse de la KAMF como se muestra en la figura 16 donde S se establece en FC || P0 || L0 con FC teniendo un nuevo valor y P0, L0 correspondiente al IDENTIFICACIÓN DE CONEXIÓN DE NAS. De hecho, P0 y L0 se definen de manera similar a P2 y L2 como se explicó anteriormente con respecto a la figura 15. Debido a que la IDENTIFICACIÓN DE CONEXIÓN DE NAS se usa en la derivación de esta nueva clave intermedia, es por lo tanto específico de la conexión de NAS. Todo lo que se derive posteriormente de la clave KNAS también sería específico de la conexión de NAS. Por lo tanto, se propone derivar la clave de protección NAS KNASint y KNASenc a partir de KNAS de manera similar a como se hace en los sistemas heredados cuando se derivan de KASME.

El esquema general de derivación de claves que produce las claves de protección NAS puede, por tanto, proporcionarse como se ilustra en la figura 16. En realizaciones de proporcionar derivación de claves basándose en la IDENTIFICACIÓN DE CONEXIÓN DE NAS, se puede usar/necesitar un mayor número de parámetros específicos de conexión en comparación con realizaciones explicadas anteriormente con respecto a las figuras 10A-B, 11A-B, 12A-B y 13A-B.

Las realizaciones de ejemplo se describen a continuación.

1. Un método en un primer nodo de comunicación que proporciona comunicación de mensajes de estrato de acceso a red (NAS) con un segundo nodo de comunicación, comprendiendo el método: proporcionar (1711) una primera identificación de conexión de NAS para una primera conexión de NAS entre el primer y el segundo nodo de comunicación; proporcionar (1713) una segunda identificación de conexión de NAS para una segunda conexión de NAS entre el primer y el segundo nodo de comunicación, en el que la primera y la segunda identificación de conexión de NAS son diferentes, y en el que la primera y la segunda conexión de NAS son diferentes; comunicar (1717) un primer mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la primera conexión de NAS, en el que comunicar el primer mensaje de NAS comprende al menos uno de realizar protección de integridad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y/o realizar protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS; y comunicar (1719) un segundo mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la segunda conexión de NAS, en el que comunicar el segundo mensaje de NAS comprende al menos uno de realizar protección de integridad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y/o realizar protección de confidencialidad para el segundo mensaje de NAS para protección de confidencialidad usando la segunda identificación de conexión de NAS.

2. El método de la realización 1, en el que la primera y la segunda conexión de NAS comparten una clave maestra de un contexto de seguridad de NAS, en el que comunicar el primer mensaje de NAS comprende al menos uno de realizar la protección de integridad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra y/o realizar protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra, y en el que comunicar el segundo mensaje de NAS comprende al menos uno de realizar protección de integridad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave maestra y/o realizar la protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave maestra.

3. El método de la realización 1, en el que la primera y la segunda conexión de NAS comparten una clave maestra de un contexto de seguridad de NAS, en el que comunicar el primer mensaje de NAS comprende realizar la protección de integridad para el primer mensaje de NAS generando un primer código de autenticación de mensaje basándose en la primera identificación de conexión de NAS, la clave maestra y el primer mensaje de NAS, y transmitir el primer mensaje de NAS con el primer código de autenticación del mensaje a través de la primera conexión de NAS al segundo nodo de comunicación, y en el que comunicar el segundo mensaje de NAS comprende realizar la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basándose en la segunda identificación de conexión de NAS, la clave maestra y el segundo mensaje de

NAS, y transmitir el segundo mensaje de NAS con el segundo código de autenticación de mensaje a través de la segunda conexión de NAS al segundo nodo de comunicación.

4. El método de la realización 3, en el que la primera identificación de conexión de NAS se concatena con un primer conteo de NAS para el primer mensaje de NAS, en el que la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS se proporcionan como una entrada para generar el primer código de autenticación de mensaje, en el que la segunda identificación de conexión de NAS se concatena con un segundo conteo de NAS para el segundo mensaje de NAS, y en el que la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS se proporcionan como una entrada para generar el segundo código de autenticación de mensaje.

5. El método de la realización 3, en el que la primera identificación de conexión de NAS se proporciona como una entrada para generar el primer código de autenticación de mensaje, y en el que la segunda identificación de conexión de NAS se proporciona como una entrada para generar el segundo código de autenticación de mensaje.

6. El método de la realización 3, en el que la clave maestra y la primera identificación de conexión de NAS se usan para derivar una primera clave de protección de integridad usada para generar el primer código de autenticación de mensaje, y en el que la clave maestra y la segunda identificación de conexión de NAS se usan para derivar una segunda clave de protección de integridad usada para generar el segundo código de autenticación de mensaje.

7. El método de cualquiera de las realizaciones 3 a 6 en el que realizar la protección de integridad para el primer mensaje de NAS comprende realizar la protección de integridad para el primer mensaje de NAS usando una interfaz de protección de integridad EIA compatible con 5G, y en el que realizar la protección de integridad para el segundo mensaje de NAS comprende realizar la protección de integridad para el segundo mensaje de NAS usando la interfaz de protección de integridad EIA compatible con 5G.

8. El método de la realización 1, en el que la primera y la segunda conexión de NAS comparten una clave maestra de un contexto de seguridad de NAS, en el que comunicar el primer mensaje de NAS comprende realizar la protección de confidencialidad para el primer mensaje de NAS cifrando el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra para proporcionar un primer mensaje de NAS cifrado, y transmitir el primer mensaje de NAS cifrado a través de la primera conexión de NAS al segundo nodo de comunicación, y en el que comunicar el segundo mensaje de NAS comprende realizar la protección de confidencialidad para el segundo mensaje de NAS cifrando el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave maestra para proporcionar un segundo mensaje de NAS cifrado, y transmitir el segundo mensaje de NAS cifrado a través de la segunda conexión de NAS al segundo nodo de comunicación.

9. El método de la realización 8, en el que la primera identificación de conexión de NAS se concatena con un primer conteo de NAS para el primer mensaje de NAS, en el que la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS se proporciona como una entrada para generar el primer mensaje de NAS cifrado, en el que la segunda identificación de conexión de NAS se concatena con un segundo conteo de NAS para el segundo mensaje de NAS, y en el que la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS se proporcionan como una entrada para generar el segundo mensaje de NAS cifrado.

10. El método de la realización 8, en el que la primera identificación de conexión de NAS se proporciona como una entrada para generar el primer mensaje de NAS cifrado, en el que la segunda identificación de conexión de NAS se proporciona como una entrada para generar el segundo mensaje de NAS cifrado.

11. El método de la realización 8, en el que la clave maestra y la primera identificación de conexión de NAS se usan para derivar una primera clave de cifrado que se usa para generar el primer mensaje de NAS cifrado, y en el que la clave maestra y la segunda identificación de conexión de NAS se usan para derivar una segunda clave de cifrado que se usa para generar el segundo mensaje de NAS cifrado.

12. El método de cualquiera de las realizaciones 8 a 11, en el que realizar la protección de confidencialidad para el primer mensaje de NAS comprende realizar la protección de confidencialidad para el primer mensaje de NAS usando una interfaz de cifrado EEA compatible con 5G, y en el que realizar la protección de confidencialidad para el segundo mensaje de NAS comprende realizar la protección de confidencialidad para el segundo mensaje de NAS usando la interfaz de cifrado EEA compatible con 5G.

13. El método de la realización 1, en el que la primera y la segunda conexión de NAS comparten una clave maestra de un contexto de seguridad de NAS, en el que comunicar el primer mensaje de NAS comprende recibir el primer mensaje de NAS con un primer código de autenticación de mensaje a través de la primera conexión de NAS del segundo nodo de comunicación, realizar la protección de integridad para el primer mensaje de NAS generando un primer código de autenticación de mensaje derivado para el primer mensaje de NAS basándose en la primera identificación de conexión de NAS, la clave maestra y el primer mensaje de NAS, y procesar el primer mensaje de NAS en respuesta al primer código de autenticación de mensaje y a la coincidencia del primer código de

autenticación de mensaje derivado, y en el que comunicar el segundo mensaje de NAS comprende recibir el segundo mensaje de NAS con un segundo código de autenticación de mensaje a través de la segunda conexión de NAS desde el segundo nodo de comunicación, realizar la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje derivado para el segundo mensaje de NAS basándose en la segunda identificación de conexión de NAS, la clave maestra y el segundo mensaje de NAS, y procesar el segundo mensaje de NAS en respuesta al segundo código de autenticación de mensaje y a la coincidencia del segundo código de autenticación de mensaje derivado.

14. El método de la realización 13, en el que la primera identificación de conexión de NAS se concatena con un primer conteo de NAS para el primer mensaje de NAS, en el que la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS se proporcionan como una entrada para generar el primer código de autenticación de mensaje derivado, en el que la segunda identificación de conexión de NAS se concatena con un segundo conteo de NAS para el segundo mensaje de NAS, y en el que la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS se proporcionan como una entrada para generar el segundo código de autenticación de mensaje derivado.

15. El método de la realización 13, en el que la primera identificación de conexión de NAS se proporciona como una entrada para generar el primer código de autenticación de mensaje derivado, en el que la segunda identificación de conexión de NAS se proporciona como una entrada para generar el segundo código de autenticación de mensaje derivado.

16. El método de la realización 13, en el que la clave maestra y la primera identificación de conexión de NAS se usan para derivar una primera clave de protección de integridad usada para generar el primer código de autenticación de mensaje derivado, y en el que la clave maestra y la segunda identificación de conexión de NAS se usan para derivar una segunda clave de protección de integridad usada para generar el segundo código de autenticación de mensaje derivado.

17. El método de cualquiera de las realizaciones 13 a 16 en el que realizar la protección de integridad para el primer mensaje de NAS comprende realizar la protección de integridad para el primer mensaje de NAS usando una interfaz de protección de integridad EIA compatible con 5G, y en el que realizar la protección de integridad para el segundo mensaje de NAS comprende realizar la protección de integridad para el segundo mensaje de NAS usando la interfaz de protección de integridad EIA compatible con 5G.

18. El método de la realización 1, en el que la primera y la segunda conexión de NAS comparten una clave maestra de un contexto de seguridad de NAS, en el que comunicar el primer mensaje de NAS comprende recibir un primer mensaje de NAS cifrado a través de la primera conexión de NAS desde el segundo nodo de comunicación, realizar la protección de confidencialidad para el primer mensaje de NAS descifrando el primer mensaje de NAS cifrado usando la primera identificación de conexión de NAS y la clave maestra para proporcionar un primer mensaje de NAS descifrado, y procesar el primer mensaje de NAS descifrado, en el que comunicar el segundo mensaje de NAS comprende recibir un segundo mensaje de NAS cifrado a través de la segunda conexión de NAS desde el segundo nodo de comunicación, realizar la protección de confidencialidad para el segundo mensaje de NAS descifrando el segundo mensaje de NAS cifrado usando la segunda identificación de conexión de NAS y la clave maestra para proporcionar un segundo mensaje de NAS descifrado, y procesar el segundo mensaje de NAS descifrado.

19. El método de la realización 18, en el que la primera identificación de conexión de NAS se concatena con un primer conteo de NAS para el primer mensaje de NAS, en el que la concatenación de la primera identificación de conexión de NAS y el primer conteo de NAS se proporcionan como una entrada para generar el primer mensaje de NAS descifrado, en el que la segunda identificación de conexión de NAS se concatena con un segundo conteo de NAS para el segundo mensaje de NAS, y en el que la concatenación de la segunda identificación de conexión de NAS y el segundo conteo de NAS se proporcionan como una entrada para generar el segundo mensaje de NAS cifrado.

20. El método de la realización 18, en el que la primera identificación de conexión de NAS se proporciona como una entrada para generar el primer mensaje de NAS descifrado, en el que la segunda identificación de conexión de NAS se proporciona como una entrada para generar el segundo mensaje de NAS descifrado.

21. El método de la realización 18, en el que la clave maestra y la primera identificación de conexión de NAS se usan para derivar una primera clave de descifrado usada para generar el primer mensaje de NAS descifrado, y en el que la clave maestra y la segunda identificación de conexión de NAS se usan para derivar una segunda clave de descifrado usada para generar el segundo mensaje de NAS descifrado.

22. El método de cualquiera de las realizaciones 18 a 21, en el que realizar la protección de confidencialidad para el primer mensaje de NAS comprende realizar la protección de confidencialidad para el primer mensaje de NAS usando una interfaz de descifrado EEA compatible con 5G, y en el que realizar la protección de confidencialidad para el segundo mensaje de NAS comprende realizar la protección de confidencialidad para el segundo mensaje de NAS usando la interfaz de descifrado EEA compatible con 5G.

23. El método de cualquiera de las realizaciones 1 a 22, en el que la primera conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación, o en el que la primera conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación.

24. El método de la realización 23, en el que el nodo de acceso 3GPP comprende una estación base de la red de acceso por radio, y en el que el nodo de acceso no 3GPP comprende al menos uno de un nodo de acceso WiFi y/o un nodo de acceso de satélite.

25. El método de cualquiera de las realizaciones 1 a 24, en el que la primera y la segunda conexión de NAS se mantienen simultáneamente entre el primer y el segundo nodo de comunicación.

26. El método de cualquiera de las realizaciones 1 a 25, en el que el primer nodo de comunicación comprende un nodo de red de una red de comunicación inalámbrica y el segundo nodo de comunicación comprende un terminal inalámbrico, o en el que el primer nodo de comunicación comprende un terminal inalámbrico y el segundo nodo de comunicación comprende un nodo de red de una red de comunicación inalámbrica.

27. El método de cualquiera de las realizaciones 1 a 26, el método además comprende:

establecer una sesión de unidad de paquete de datos (PDU) basándose en el primer y el segundo mensaje de NAS para comunicar los datos de plano de usuario entre el primer y el segundo nodo de comunicación.

28. Un método en un primer nodo de comunicación que proporciona la comunicación de mensajes de estrato de acceso a red (NAS) con un segundo nodo de comunicación, comprendiendo el método: proporcionar (1801) una primera conexión de NAS entre el primer y el segundo nodo de comunicación; proporcionar (1803) una segunda conexión de NAS entre el primer y el segundo nodo de comunicación, en el que la primera y la segunda conexión de NAS son diferentes; asignar (1805) un dominio conteo de NAS de modo que una primera porción del dominio conteo de NAS se asigne a los mensajes de NAS comunicados a través de la primera conexión de NAS y de modo que una segunda porción del dominio conteo de NAS se asigne a los mensajes de NAS comunicados a través de la segunda conexión de NAS, en la que la primera y la segunda porción del dominio conteo de NAS son mutuamente excluyentes; comunicar (1811, 1831) mensajes de NAS a través de la primera conexión de NAS usando un valor de conteo de NAS más bajo de la primera porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la primera conexión de NAS; y comunicar (1813, 1833) mensajes de NAS a través de la segunda conexión de NAS usando un valor de conteo de NAS más bajo de la segunda porción del dominio conteo de NAS que no se ha usado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS.

29. El método de la realización 28, en el que los valores de conteo de NAS de la primera y la segunda porción del dominio conteo de NAS están intercalados.

30. El método de la realización 29, en el que la primera porción del dominio conteo de NAS incluye valores de conteo de NAS pares, y en el que la segunda porción del dominio conteo de NAS incluye valores de conteo de NAS impares.

31. El método de cualquiera de las realizaciones 28 a 29, comprendiendo el método además: proporcionar (1816) una tercera conexión de NAS entre el primer y el segundo nodo de comunicación, en el que la primera y la tercera conexión de NAS son diferentes y la segunda y la tercera conexión de NAS son diferentes, en el que una tercera porción del dominio conteo de NAS se asigna para mensajes de NAS comunicados a través de la tercera conexión de NAS, en el que la primera, la segunda y la tercera porción del dominio conteo de NAS son mutuamente excluyentes; y comunicar (1835) mensajes de NAS a través de la tercera conexión de NAS usando un valor de conteo de NAS más bajo de la tercera porción del dominio conteo de NAS que no se ha usado previamente para la tercera conexión de NAS.

32. El método de la realización 31, en el que la primera porción del dominio conteo de NAS incluye valores de conteo de NAS divisibles por 3, en el que la segunda porción del dominio conteo de NAS comprende valores de conteo de NAS para los que la división por 3 proporciona un resto de 1, y en el que la tercera porción del dominio conteo de NAS comprende valores de conteo de NAS para los cuales la división por 3 proporciona un resto de 2.

33. El método de cualquiera de las realizaciones 28 a 32, en el que el primer nodo de comunicación comprende un nodo de red y el segundo nodo de comunicación comprende un terminal inalámbrico, en el que el dominio conteo de NAS es un dominio conteo de NAS de enlace ascendente, en el que comunicar mensajes de NAS a través de la primera conexión de NAS comprende recibir mensajes de NAS a través de la primera conexión de NAS, y en el que

comunicar mensajes de NAS a través de la segunda conexión de NAS comprende recibir mensajes de NAS a través de la segunda conexión de NAS.

34. El método de cualquiera de las realizaciones 28 a 32, en el que el primer nodo de comunicación comprende un nodo de red y el segundo nodo de comunicación comprende un terminal inalámbrico, en el que el dominio conteo de NAS es un dominio conteo de NAS de enlace descendente, en el que comunicar mensajes de NAS a través de la primera conexión de NAS comprende transmitir mensajes de NAS a través de la primera conexión de NAS, y en el que comunicar mensajes de NAS a través de la segunda conexión de NAS comprende transmitir mensajes de NAS a través de la segunda conexión de NAS.

35. El método de cualquiera de las realizaciones 28 a 32, en el que el primer nodo de comunicación comprende un terminal inalámbrico y el segundo nodo de comunicación comprende un nodo de red, en el que el dominio conteo de NAS es un dominio conteo de NAS de enlace ascendente, en el que comunicar mensajes de NAS a través de la primera conexión de NAS comprende transmitir mensajes de NAS a través de la primera conexión de NAS, y en el que comunicar mensajes de NAS a través de la segunda conexión de NAS comprende transmitir mensajes de NAS a través de la segunda conexión de NAS.

36. El método de cualquiera de las realizaciones 28 a 32, en el que el primer nodo de comunicación comprende un terminal inalámbrico y el segundo nodo de comunicación comprende un nodo de red, en el que el dominio conteo de NAS es un dominio conteo de NAS de enlace descendente, en el que comunicar mensajes de NAS a través de la primera conexión de NAS comprende recibir mensajes de NAS a través de la primera conexión de NAS, y en el que comunicar mensajes de NAS a través de la segunda conexión de NAS comprende recibir mensajes de NAS a través de la segunda conexión de NAS.

37. El método de cualquiera de las realizaciones 28 a 36, en el que la primera conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación, o en el que la primera conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación.

38. El método de la realización 37, en el que el nodo de acceso 3GPP comprende una estación base de red de acceso por radio, y en el que el nodo de acceso no 3GPP comprende al menos uno de un nodo de acceso WiFi y/o un nodo de acceso de satélite.

39. El método de cualquiera de las realizaciones 28 a 38, en el que comunicar mensajes de NAS a través de la primera conexión de NAS comprende al menos uno de realizar la protección de integridad generando códigos de autenticación de mensaje usando los valores de conteo de NAS respectivos de la primera porción del dominio conteo de NAS y/o realizar la protección de confidencialidad usando los valores de conteo de NAS respectivos de la primera porción del dominio conteo de NAS, y en el que la comunicación de mensajes de NAS a través de la segunda conexión de NAS comprende al menos uno de realizar la protección de integridad mediante la generación de códigos de autenticación de mensaje usando los valores de conteo de NAS respectivos de la segunda porción del dominio conteo de NAS y/o realizar la protección de confidencialidad usando los valores de conteo de NAS respectivos de la segunda porción del dominio conteo de NAS.

40. Un nodo de comunicación, en el que el nodo de comunicación se adapta para realizar operaciones de acuerdo con cualquiera de las realizaciones 1 a 39.

41. Un nodo de comunicación, en el que el nodo de comunicación incluye módulos configurados para realizar operaciones de acuerdo con cualquiera de las realizaciones 1 a 39.

42. Un primer nodo de comunicación que comprende: una interfaz 601, 701 de comunicación configurada para proporcionar comunicación con un segundo nodo de comunicación; y un procesador 603,703 acoplado con la interfaz de comunicación, en el que el procesador está configurado para transmitir comunicaciones al segundo nodo de comunicación y/o recibir comunicaciones desde el segundo nodo de comunicación a través de la interfaz de comunicación, en el que el procesador está configurado para realizar operaciones de acuerdo con cualquiera de las realizaciones 1 a 39.

A continuación se explican más definiciones y realizaciones.

En la descripción anterior de varias realizaciones de los presentes conceptos de la invención, debe entenderse que la terminología usada en el presente documento tiene el propósito de describir realizaciones particulares únicamente y no pretende limitar los presentes conceptos de la invención. A menos que se defina lo contrario, todos los términos (incluidos los términos técnicos y científicos) usados en el presente documento tienen el mismo significado que el que entiende comúnmente un experto en la técnica a la que pertenecen los presentes conceptos de la invención. Se entenderá además que los términos, como los definidos en los diccionarios de uso común, deben interpretarse como

si tuvieran un significado que sea consistente con su significado en el contexto de esta especificación y la técnica relevante y no se interpretarán en un sentido idealizado o excesivamente formal a menos que se defina expresamente en el presente documento.

Cuando se hace referencia a un elemento como "conectado", "acoplado", "que responde" o variantes del mismo a otro elemento, puede conectarse, acoplarse o responder directamente al otro elemento o pueden estar presentes elementos intermedios. Por el contrario, cuando se hace referencia a un elemento como "conectado directamente", "acoplado directamente", "que responde directamente" o variantes del mismo a otro elemento, no hay elementos intermedios presentes. Los números iguales se refieren a elementos iguales en todas partes. Además, "acoplado", "conectado", "que responde" o variantes de los mismos, como se usa en el presente documento, pueden incluir acoplado, conectado o que responde de forma inalámbrica. Como se usa en el presente documento, las formas singulares "un", "una", "el" y "la" pretenden incluir las formas plurales también, a menos que el contexto indique claramente lo contrario. Es posible que las funciones o construcciones conocidas no se describan en detalle por razones de brevedad y/o claridad. El término "y/o" incluye todas y cada una de las combinaciones de uno o más de los elementos enumerados asociados.

Se entenderá que aunque los términos primero, segundo, tercero, etc. pueden usarse en el presente documento para describir varios elementos/operaciones, estos elementos/operaciones no deben estar limitados por estos términos. Estos términos solo se usan para distinguir un elemento/operación de otro elemento/operación. Por tanto, un primer elemento/operación en algunas realizaciones podría denominarse un segundo elemento/operación en otras realizaciones sin apartarse de las enseñanzas de los presentes conceptos de la invención. Los mismos números de referencia o los mismos designadores de referencia indican elementos iguales o similares en toda la especificación.

Como se usa en el presente documento, los términos "comprender", "que comprende", "comprende", "incluir", "que incluye", "incluye", "tener", "tiene", "que tiene" o variantes de los mismos son de final abierto, e incluyen una o más características, números enteros, elementos, pasos, componentes o funciones indicados, pero no excluye la presencia o adición de una o más características, números enteros, elementos, pasos, componentes, funciones o grupos de los mismos. Además, como se usa en el presente documento, la abreviatura común "e.g (por ejemplo)", que deriva de la frase latina "exempli gratia", puede usarse para introducir o especificar un ejemplo general o ejemplos de un elemento mencionado anteriormente, y no pretende ser una limitación de tal artículo. La abreviatura común "i.e (es decir)", que se deriva de la frase latina "id est", puede usarse para especificar un elemento particular de una recitación más general.

Las realizaciones de ejemplo se describen en el presente documento con referencia a los diagramas de bloques y/o las ilustraciones de los diagramas de flujo de métodos implementados por computadora, aparatos (sistemas y/o dispositivos) y/o productos de programas informáticos. Se entiende que un bloque de los diagramas de bloques y/o las ilustraciones de los diagramas de flujo, y las combinaciones de bloques en los diagramas de bloques y/o las ilustraciones de los diagramas de flujo pueden implementarse mediante instrucciones de programas informáticos que son realizadas por uno o más circuitos de computadora. Estas instrucciones del programa informático se pueden proporcionar a un circuito de procesador de un circuito de computadora de propósito general, circuito de computadora de propósito especial y/u otro circuito de procesamiento de datos programable para producir una máquina, de modo que las instrucciones, que se ejecutan a través del procesador de la computadora y/u otros aparatos de procesamiento de datos programables, transistores de transformación y control, valores almacenados en ubicaciones de memoria y otros componentes de hardware dentro de dicha circuitería para implementar las funciones/actos especificados en los diagramas de bloques y/o el bloque o bloques del diagrama de flujo, y así crear medios (funcionalidad) y/o estructura para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques del diagrama de flujo.

Estas instrucciones del programa informático también pueden almacenarse en un medio legible por computadora tangible que puede hacer que una computadora u otro aparato de procesamiento de datos programable funcione de una manera particular, de modo que las instrucciones almacenadas en el medio legible por computadora produzcan un artículo de fabricación que incluye instrucciones que implementan las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques del diagrama de flujo. En consecuencia, las realizaciones de los presentes conceptos de la invención pueden incorporarse en hardware y/o software (incluido firmware, software residente, microcódigo, etc.) que se ejecuta en un procesador, como un procesador de señales digitales, que se puede denominar colectivamente como "circuitería", "un módulo" o variantes de los mismos.

También debe tenerse en cuenta que en algunas implementaciones alternativas, las funciones/actos indicados en los bloques pueden ocurrir fuera del orden indicado en los diagramas de flujo. Por ejemplo, dos bloques mostrados en sucesión pueden de hecho ejecutarse sustancialmente al mismo tiempo o los bloques pueden ejecutarse a veces en el orden inverso, dependiendo de la funcionalidad/actos involucrados. Además, la funcionalidad de un bloque dado de los diagramas de flujo y/o los diagramas de bloques puede separarse en múltiples bloques y/o la funcionalidad de dos o más bloques de los diagramas de flujo y/o los diagramas de bloques puede integrarse al menos parcialmente. Finalmente, se pueden agregar/insertar otros bloques entre los bloques que se ilustran, y/o se pueden omitir bloques/operaciones sin apartarse del alcance de los conceptos de la invención. Además, aunque

algunos de los diagramas incluyen flechas en las rutas de comunicación para mostrar una dirección primaria de comunicación, debe entenderse que la comunicación puede ocurrir en la dirección opuesta a las flechas representadas.

Se pueden realizar muchas variaciones y modificaciones a las realizaciones sin apartarse sustancialmente de los principios de los presentes conceptos de la invención. Se pretende que todas estas variaciones y modificaciones se incluyan en el presente documento dentro del alcance de los presentes conceptos de la invención. En consecuencia, la materia descrita anteriormente debe considerarse ilustrativa y no restrictiva, y los ejemplos de las realizaciones están destinados a cubrir todas las modificaciones, mejoras y otras realizaciones que caen dentro del alcance de los presentes conceptos de la invención. Por lo tanto, en la medida máxima permitida por la ley, el alcance de los presentes conceptos de la invención se determinará mediante la interpretación más amplia permisible de la presente divulgación, incluidas las siguientes reivindicaciones y sus equivalentes, y no estará restringido o limitado por la descripción detallada anterior.

Las abreviaturas mencionadas anteriormente se analizan a continuación.

Abreviatura	Explicación
AMF	Función de gestión de acceso
CM	Gestión de conexión
CONN ID	Identificación de conexión
EEA	Algoritmo de encriptado EPS
EIA	Algoritmo de integridad EPS
eKSI	Identificador de conjunto de claves en E-UTRAN
EMM	Gestión de movilidad EPS
EPC	Núcleo de paquetes evolucionado
EPS	Sistema de paquetes evolucionado
IE	Elemento de información
KAMF	Clave específica de AMS
KASME	Entrada de gestión de seguridad de acceso de clave
KDF	Función de derivación de clave
KNAS	Clave de protección NAS
KNASenc	Encriptado KNAS
KNASint	Integridad KNAS
LTE	Evolución a largo plazo
MAC	Código de autenticación de mensaje
NAS	Estrato de acceso a red
PDU	Unidad de paquete de datos
SMC	Comando de modo de seguridad
SN	Número de secuencia
UE	Equipo de usuario
3GPP	Proyecto de asociación de tercera generación
5G	5ª generación

Las referencias mencionadas anteriormente se identifican a continuación.

Ref. [1] 3GPP TS 23.501 VO.4.0 (2017-04), servicios de grupo de especificaciones técnicas y aspectos del sistema; arquitectura del sistema para el sistema 5G; etapa 2 (versión 15)

Ref. [2] 3GPP TS 33.401 V14.2.0 (2017-03), servicios de grupo de especificaciones técnicas y aspectos del sistema; evolución de la arquitectura del sistema 3GPP (SAE); arquitectura de seguridad (versión 14)

Ref. [3] 3GPP TS 24.301 V14.3.0 (2017-03), terminales y red principal del grupo de especificaciones técnicas; protocolo de estrato de no acceso (NAS) para sistema de paquetes evolucionado (EPS); etapa 3 (versión 14)

Ref. [4] 3GPP TS 33.220 V14.0.0 (2016-12), servicios de grupo de especificaciones técnicas y aspectos del sistema; arquitectura de autenticación genérica (GAA); arquitectura de arranque genérico (GBA) (versión 14)

Ref. [5] Krawczyk, et al., "HMAC: hash de clave para autenticación de mensajes", RFC 2104, febrero de 1997

REIVINDICACIONES

1.- Un método en un primer nodo de comunicación que proporciona la comunicación de mensajes de estrato de acceso a red, NAS con un segundo nodo de comunicación, comprendiendo el método:

proporcionar (1711) una primera identificación de conexión de NAS para una primera conexión de NAS entre el primer y el segundo nodo de comunicación;

proporcionar (1713) una segunda identificación de conexión de NAS para una segunda conexión de NAS entre el primer y el segundo nodo de comunicación, en el que la primera y la segunda identificación de conexión de NAS son diferentes, y en el que la primera y la segunda conexión de NAS son diferentes y comparten una clave maestra de un contexto de seguridad de NAS;

comunicar (1717) un primer mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la primera conexión de NAS, en el que comunicar el primer mensaje de NAS comprende al menos uno de realizar protección de integridad y/o realizar protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS; y realizar la protección de integridad para el primer mensaje de NAS generando un primer código de autenticación de mensaje basándose en la primera identificación de conexión de NAS, la clave maestra, y el primer mensaje de NAS, y transmitir el primer mensaje de NAS con el primer código de autenticación de mensaje a través de la primera conexión de NAS al segundo nodo de comunicación;

comunicar (1719) un segundo mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la segunda conexión de NAS, en el que comunicar el segundo mensaje de NAS comprende al menos uno de realizar protección de integridad y/o realizar protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y realizar la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basándose en la segunda identificación de conexión de NAS, la clave maestra, y el segundo mensaje de NAS, y transmitir el segundo mensaje de NAS con el segundo código de autenticación de mensaje a través de la segunda conexión de NAS al segundo nodo de comunicación.

2.- El método de la reivindicación 1, en el que la primera identificación de conexión de NAS se proporciona como una entrada para generar el primer código de autenticación de mensaje, y en el que la segunda identificación de conexión de NAS se proporciona como una entrada para generar el segundo código de autenticación de mensaje.

3.- El método de cualquiera de las reivindicaciones 1 a 2, en el que realizar la protección de integridad para el primer mensaje de NAS comprende realizar la protección de integridad para el primer mensaje de NAS usando una interfaz de protección de integridad EIA compatible con 5G, y en el que realizar protección de integridad para el segundo mensaje de NAS comprende realizar protección de integridad para el segundo mensaje de NAS usando la interfaz de protección de integridad EIA compatible con 5G.

4.- El método de cualquiera de las reivindicaciones 1 a 3, en el que la primera conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación, o en el que la primera conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación.

5.- El método de la reivindicación 4, en el que el nodo de acceso 3GPP comprende una estación base de la red de acceso por radio, y en el que el nodo de acceso no 3GPP comprende al menos uno de un nodo de acceso WiFi y/o un nodo de acceso de satélite.

6.- El método de cualquiera de las reivindicaciones 1 a 5, en el que la primera y la segunda conexión de NAS se mantienen simultáneamente entre el primer y el segundo nodo de comunicación.

7.- El método de cualquiera de las reivindicaciones 1 a 6, en el que el primer nodo de comunicación comprende un nodo de red de una red de comunicación inalámbrica y el segundo nodo de comunicación comprende un terminal inalámbrico, o en el que el primer nodo de comunicación comprende un terminal inalámbrico y el segundo nodo de comunicación comprende un nodo de red de una red de comunicación inalámbrica.

8.- El método de cualquiera de las reivindicaciones 1 a 7, el método además comprende:

establecer una sesión de unidad de paquete de datos, PDU, basándose en el primer y el segundo mensaje de NAS para comunicar los datos de plano de usuario entre el primer y el segundo nodo de comunicación.

9.- Un primer nodo de comunicación adaptado para proporcionar comunicación de mensajes de estrato de acceso a red, NAS, con un segundo nodo de comunicación, en el que el primer nodo de comunicación se adapta para:

proporcionar una primera identificación de conexión de NAS para una primera conexión de NAS entre el primer y el segundo nodo de comunicación;

proporcionar una segunda identificación de conexión de NAS para una segunda conexión de NAS entre el primer y el segundo nodo de comunicación, en el que la primera y la segunda identificación de conexión de NAS son diferentes y en el que la primera y la segunda conexión de NAS son diferentes;

comunicar un primer mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la primera conexión de NAS, en el que comunicar el primer mensaje de NAS comprende al menos uno de realizar protección de integridad y/o realizar protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS; y realizar la protección de integridad para el primer mensaje de NAS generando un primer código de autenticación de mensaje basándose en la primera identificación de conexión de NAS, la clave maestra, y el primer mensaje de NAS, y transmitir el primer mensaje de NAS con el primer código de autenticación de mensaje a través de la primera conexión de NAS al segundo nodo de comunicación;

comunicar un segundo mensaje de NAS entre el primer y el segundo nodo de comunicación a través de la segunda conexión de NAS, en el que comunicar el segundo mensaje de NAS comprende al menos uno de realizar protección de integridad y/o realizar protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS, y realizar la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basándose en la segunda identificación de conexión de NAS, la clave maestra, y el segundo mensaje de NAS, y transmitir el segundo mensaje de NAS con el segundo código de autenticación de mensaje a través de la segunda conexión de NAS al segundo nodo de comunicación.

10.- El primer nodo de comunicación de la reivindicación 9, en el que la primera identificación de conexión de NAS se proporciona como una entrada para generar el primer código de autenticación de mensaje, y en el que la segunda identificación de conexión de NAS se proporciona como una entrada para generar el segundo código de autenticación de mensaje.

11.- El primer nodo de comunicación de cualquiera de las reivindicaciones 9 a 10, en el que realizar protección de integridad para el primer mensaje de NAS comprende realizar protección de integridad para el primer mensaje de NAS usando una interfaz de protección de integridad EIA compatible con 5G, y en el que realizar protección de integridad para el segundo mensaje de NAS comprende realizar la protección de integridad para el segundo mensaje de NAS usando la interfaz de protección de integridad EIA compatible con 5G.

12.- El primer nodo de comunicación de cualquiera de las reivindicaciones 9 a 11, en el que la primera conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación, o en el que la primera conexión de NAS se proporciona a través de un nodo de acceso no 3GPP entre el primer y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso 3GPP entre el primer y el segundo nodo de comunicación.

13.- El primer nodo de comunicación de la reivindicación 12, en el que el nodo de acceso 3GPP comprende una estación base de red de acceso por radio, y en el que el nodo de acceso no 3GPP comprende al menos uno de un nodo de acceso WiFi y/o un nodo de acceso de satélite.

14.- El primer nodo de comunicación de cualquiera de las reivindicaciones 9 a 13, en el que la primera y la segunda conexión de NAS se mantienen simultáneamente entre el primer y el segundo nodo de comunicación.

15.- El primer nodo de comunicación de cualquiera de las reivindicaciones 9 a 14, en el que el primer nodo de comunicación comprende un nodo de red de una red de comunicación inalámbrica y el segundo nodo de comunicación comprende un terminal inalámbrico, o en el que el primer nodo de comunicación comprende un terminal inalámbrico y el segundo nodo de comunicación comprende un nodo de red de una red de comunicación inalámbrica.

16.- El primer nodo de comunicación de cualquiera de las reivindicaciones 9 a 15, en el que el primer nodo de comunicación está además adaptado para:

establecer una sesión de unidad de paquete de datos, PDU, basándose en el primer y el segundo mensaje de NAS para comunicar los datos de plano de usuario entre el primer y el segundo nodo de comunicación.

Figura 1

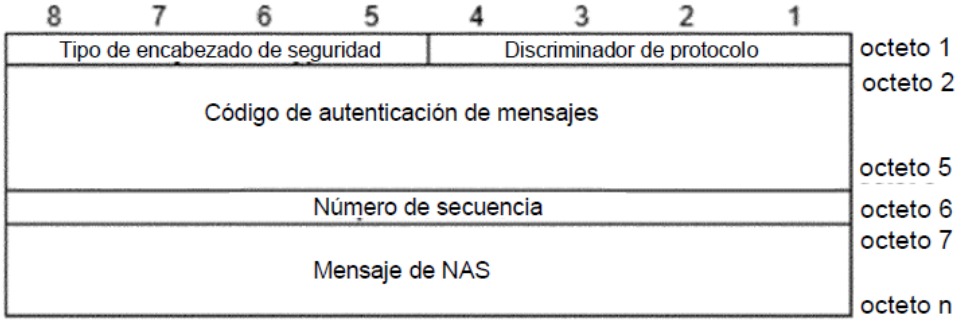


Figura 2

Tipo de encabezado de seguridad (octeto 1)

8	7	6	5	
0	0	0	0	Mensaje de NAS sencillo, no protegido por
				Mensaje de NAS protegido por
0	0	0	1	Protegido por integridad
0	0	1	0	Protegido por integridad y cifrado
0	0	1	1	Protegido por integridad con nuevo contexto de seguridad EPS (NOTA 1)
0	1	0	0	Protegido por integridad y cifrado con nuevo contexto de seguridad EPS (NOTA 2)
0	1	0	1	Mensaje de NAS protegido por integridad y parcialmente cifrado (NOTA 4)
				Mensaje L3 no estándar:
1	1	0	0	Encabezado de seguridad para el MENSAJE DE SOLICITUD
1	1	0	1	Estos valores no se usan en esta versión del protocolo.
	a			Si se reciben se interpretarán como '1100'. (NOTA 3)
1	1	1	1	

Todos los otros valores están reservados.

Figura 3A

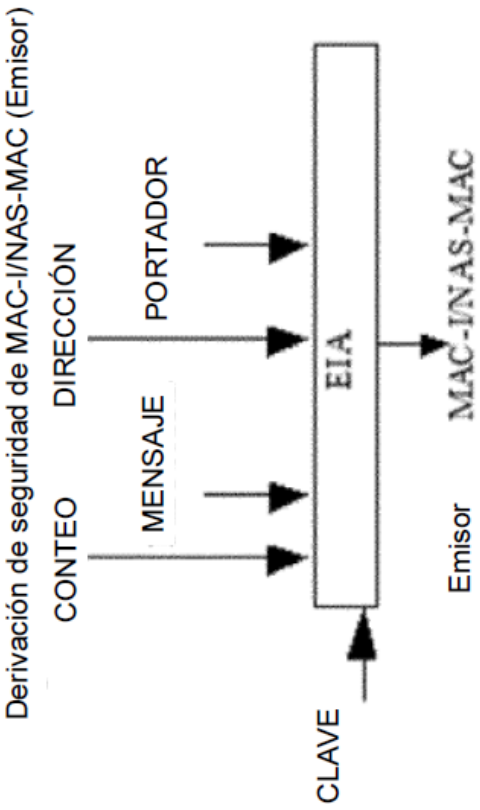
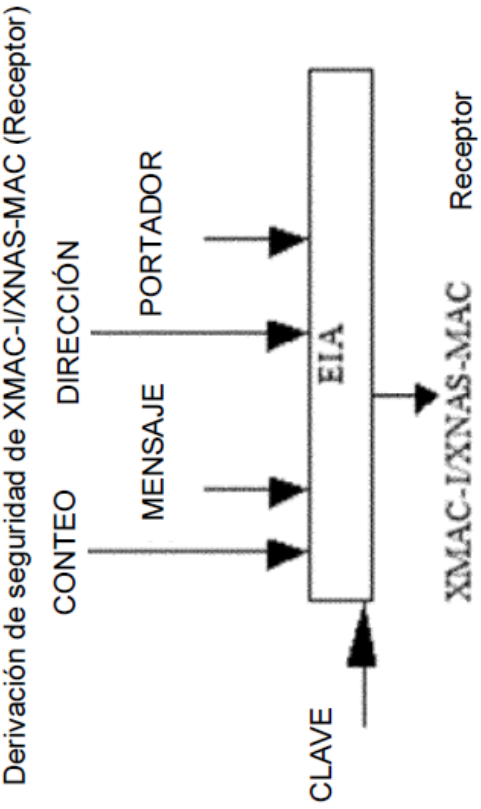


Figura 3B



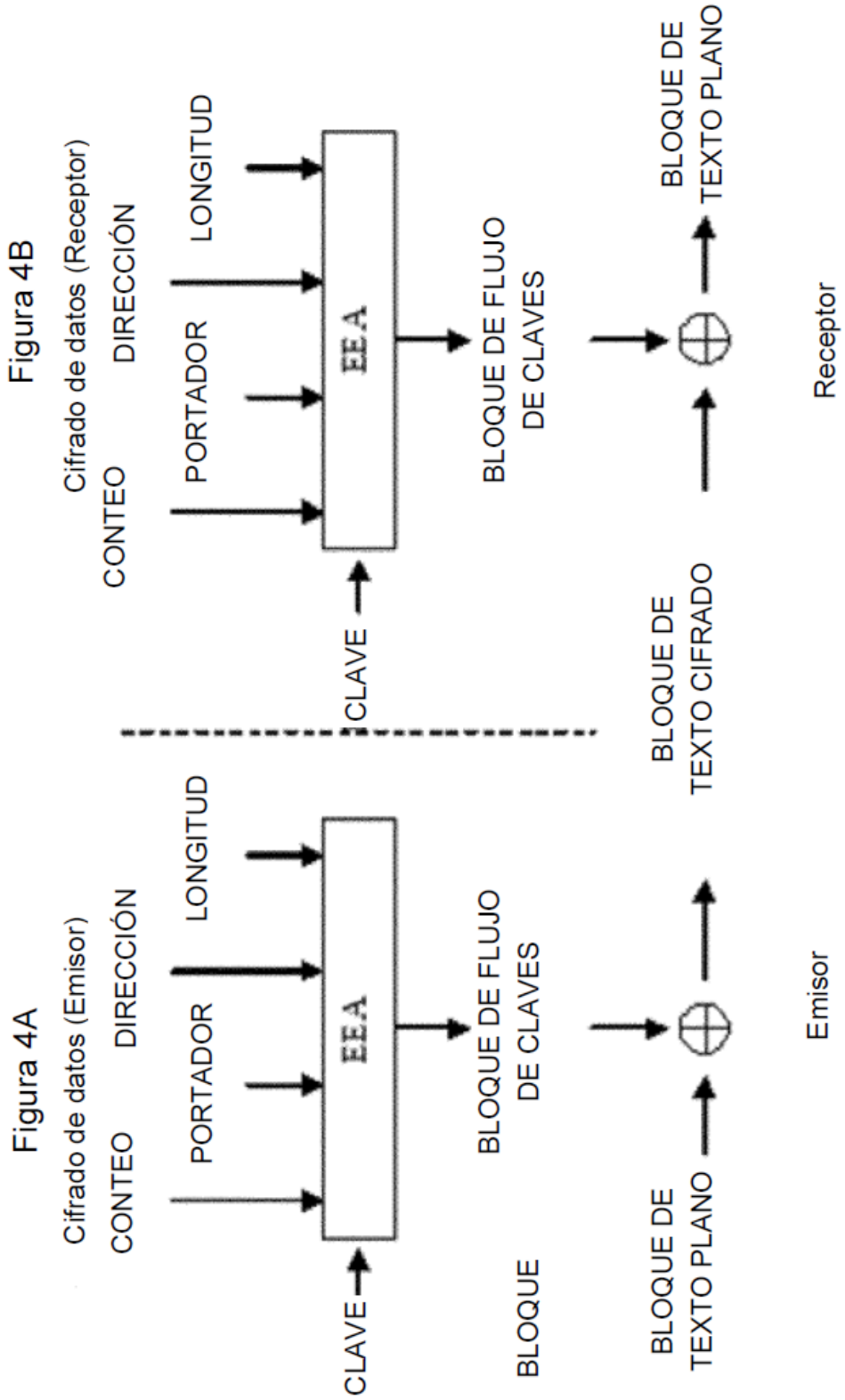


Figura 4A
Cifrado de datos (Emisor)
CONTEO
DIRECCIÓN
PORTADOR
LONGITUD
EEA
CLAVE
BLOQUE DE FLUJO DE CLAVES
BLOQUE
BLOQUE DE TEXTO PLANO
BLOQUE DE TEXTO CIFRADO
Emisor
Figura 4B
Cifrado de datos (Receptor)
CONTEO
DIRECCIÓN
PORTADOR
LONGITUD
EEA
CLAVE
BLOQUE DE FLUJO DE CLAVES
BLOQUE DE TEXTO PLANO
Receptor

Figura 5

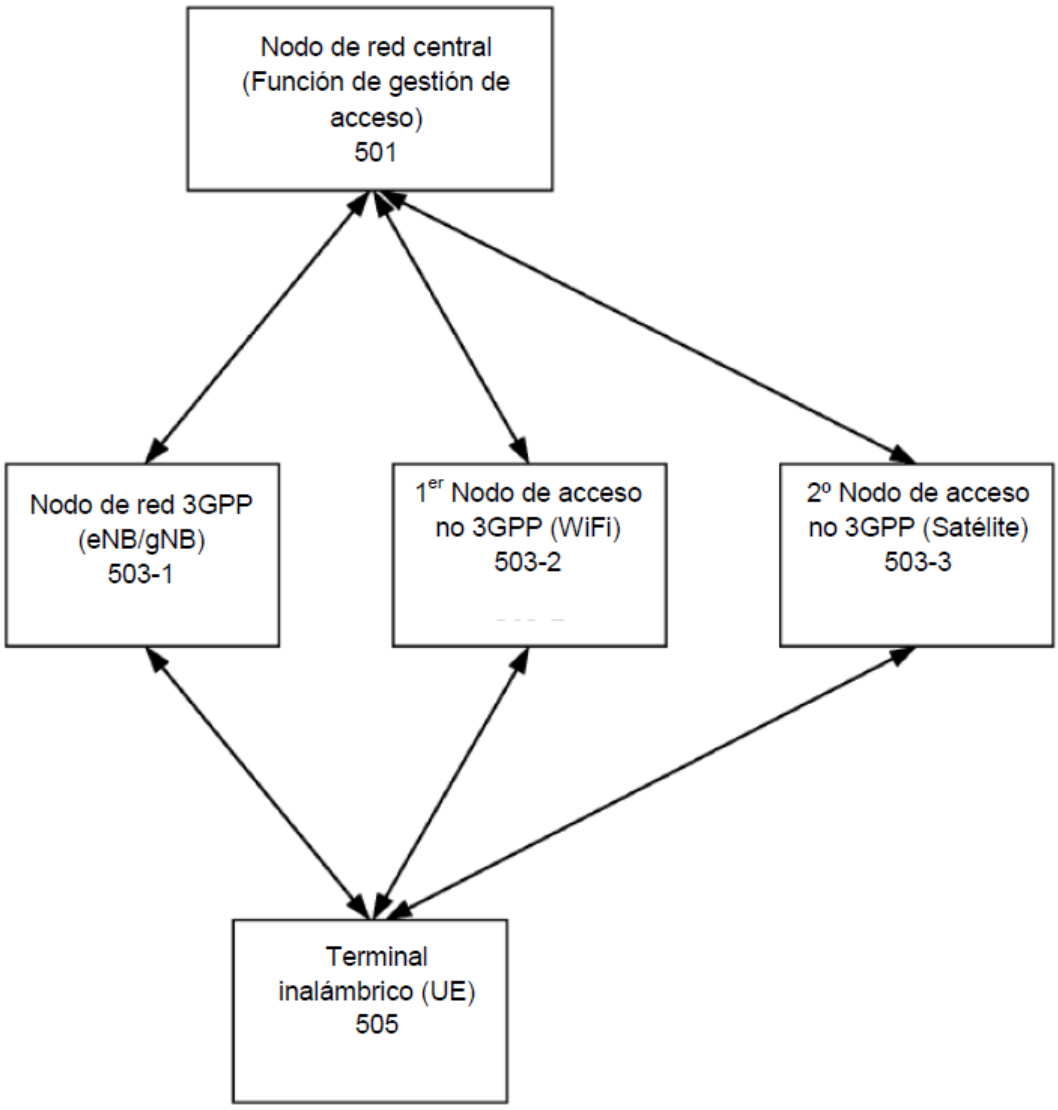

Nodo de red central
(Función de gestión de acceso)
501
Nodo de red 3GPP
(eNB/gNB)
503-1
1er Nodo de acceso no 3GPP (WiFi)
503-2
2º Nodo de acceso no 3GPP (Satélite)
503-3
Terminal inalámbrico (UE)
505

Figura 6

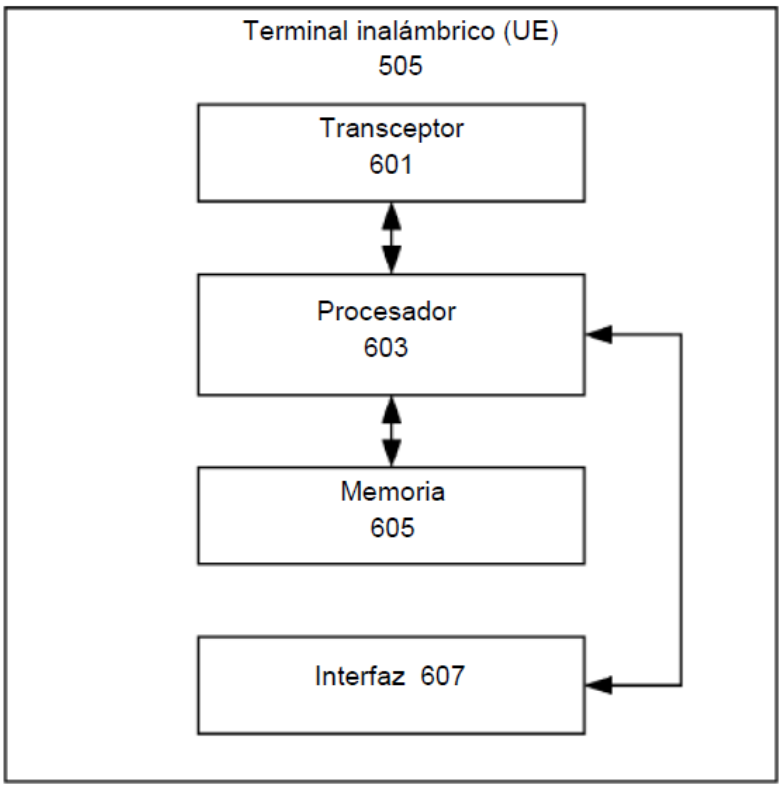


Figura 7

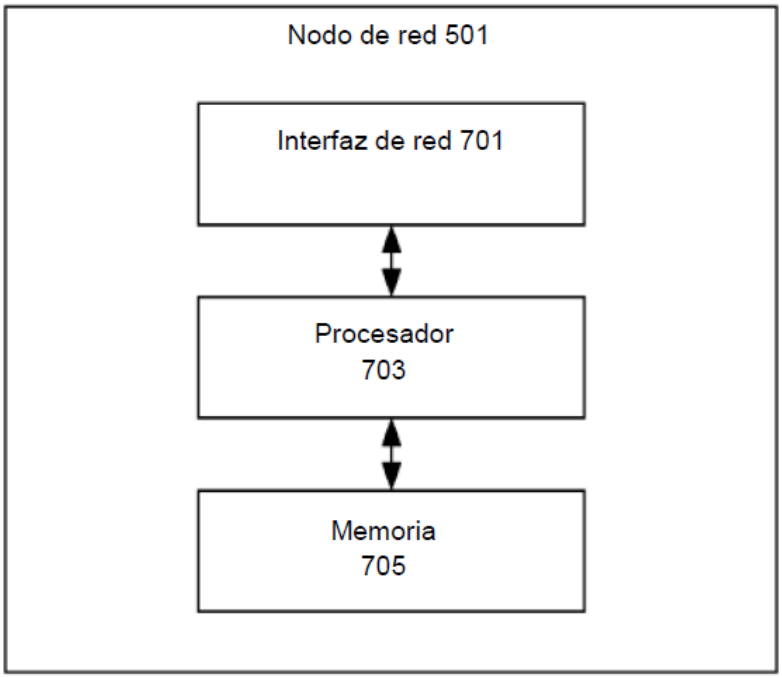


Figura 8

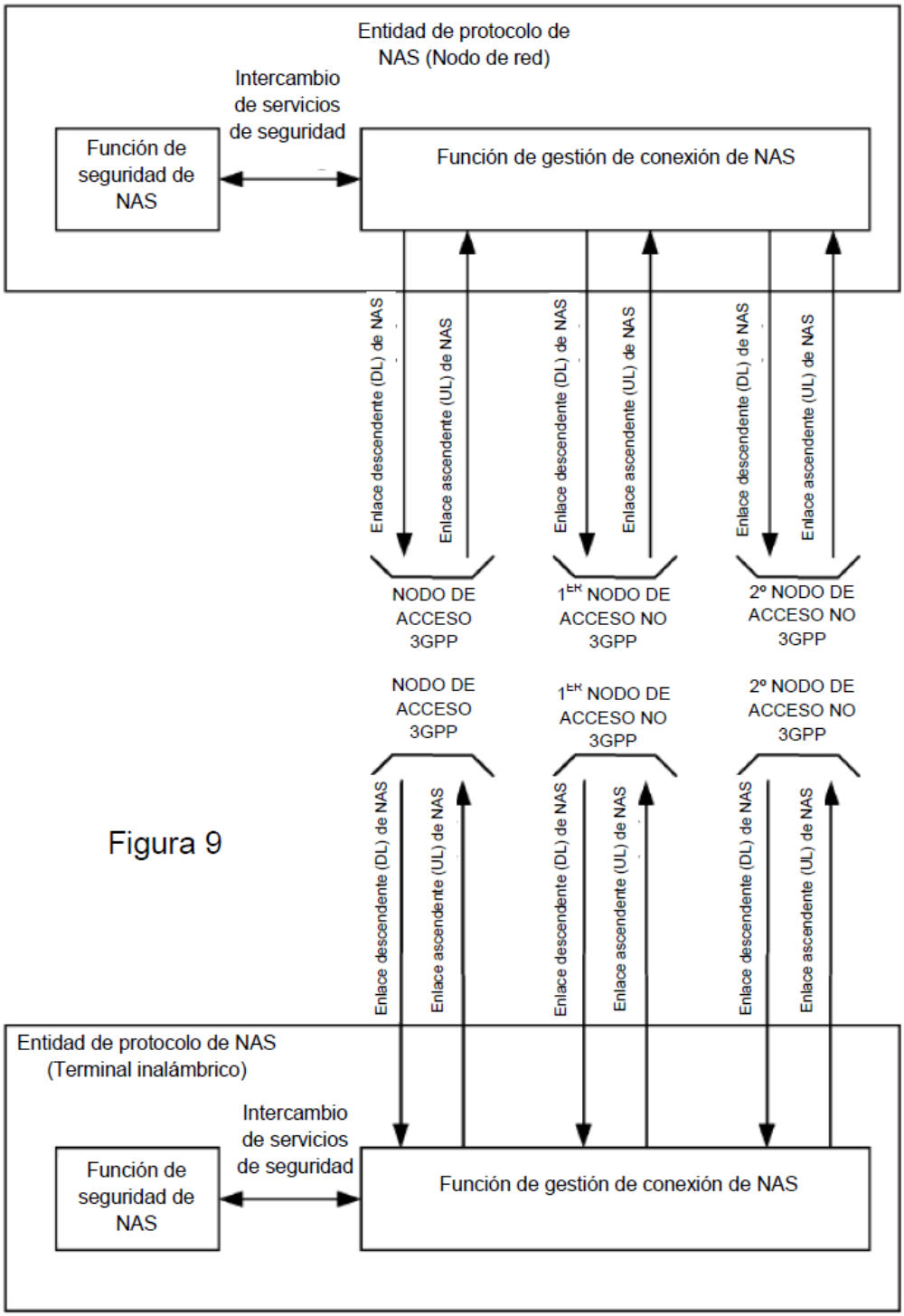


Figura 9

Figura 10A

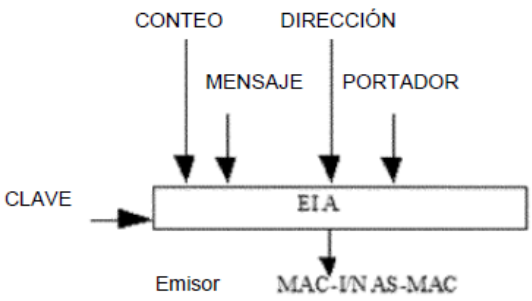


Figura 10B

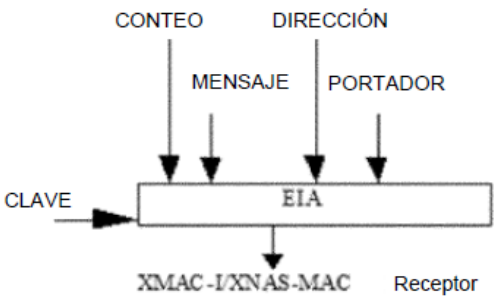


Figura 11A

Figura 11B

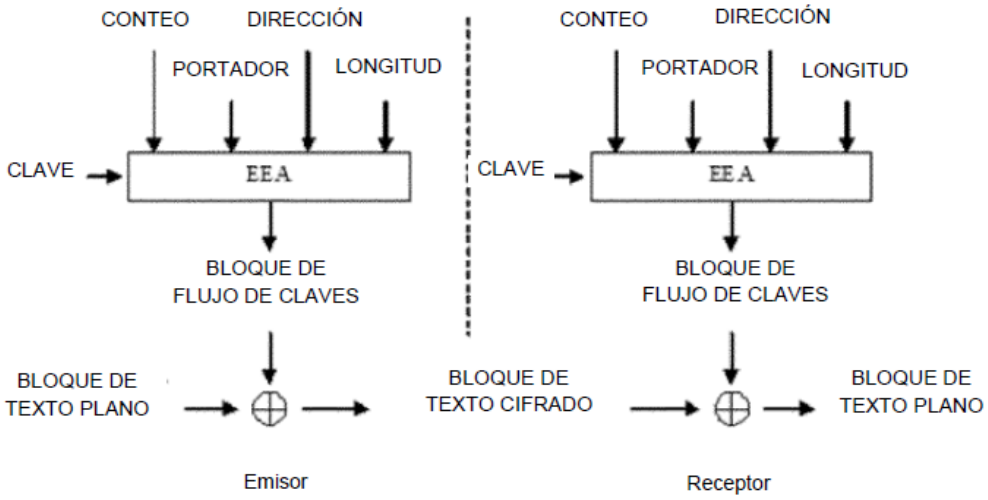


Figura 12A

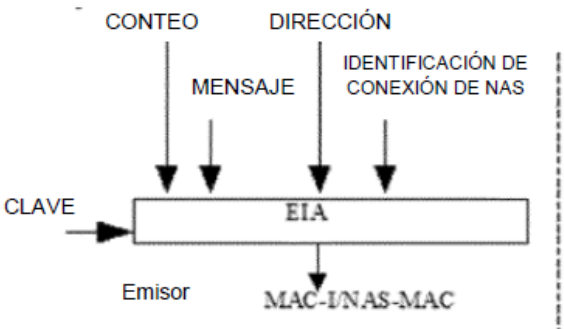


Figura 12B

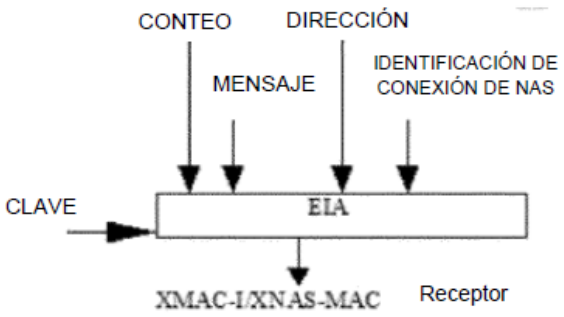


Figura 13A

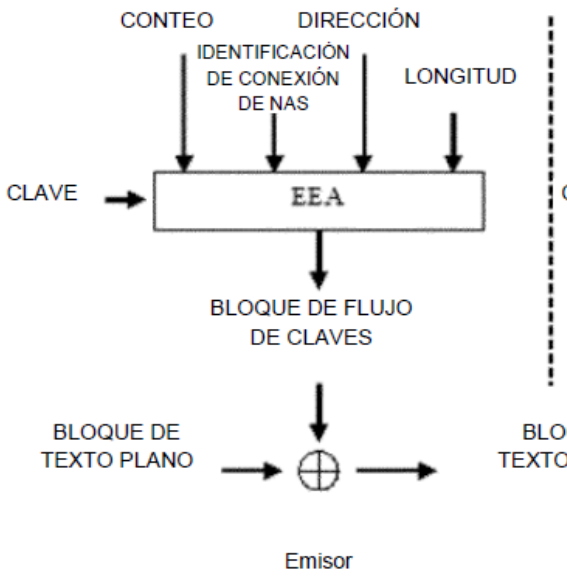


Figura 13B

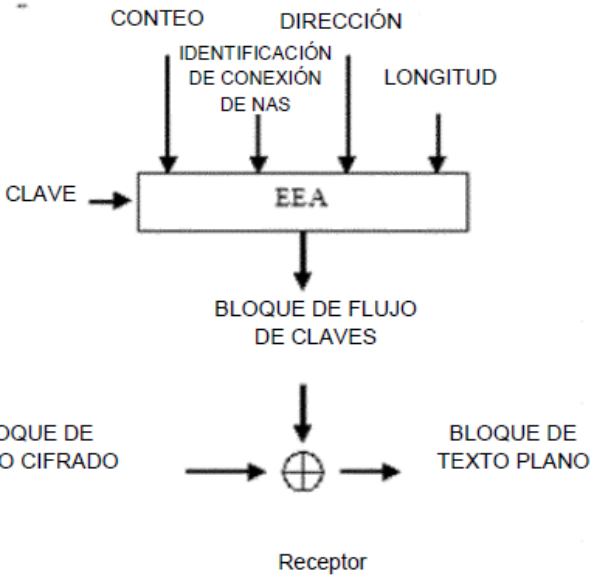


Figura 14

Diferenciador de proceso	Valor
NAS-enc-alg	0x01
NAS-int-alg	0x02

Figura 15

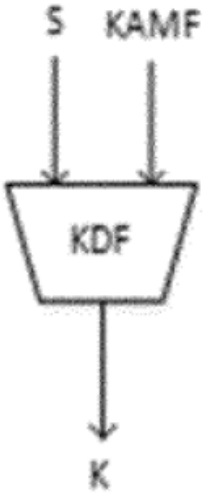


Figura 16

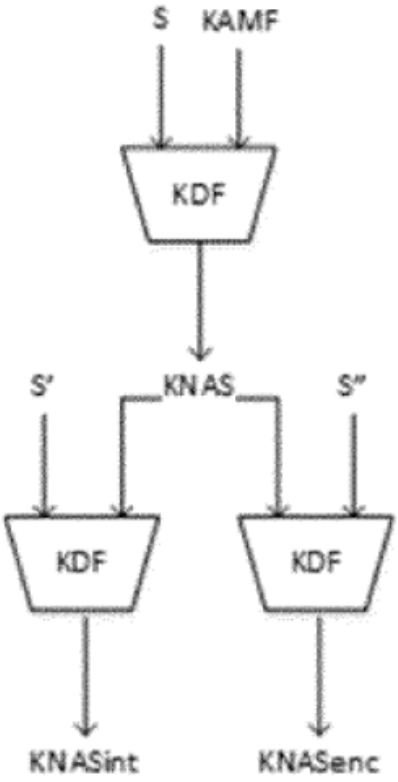


Figura 17A

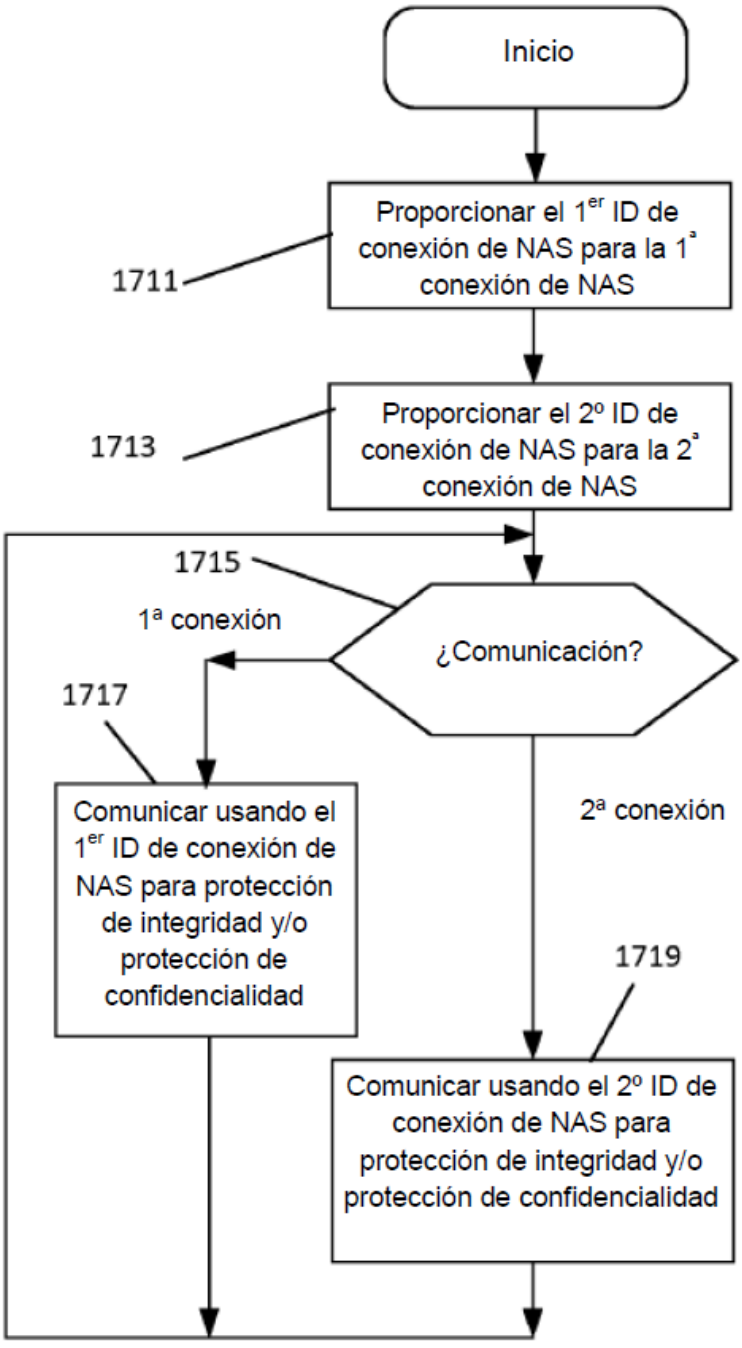


Figura 17B

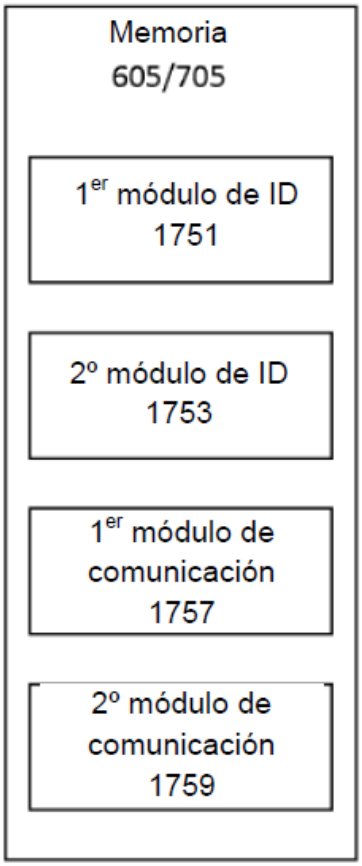


Figura 18A

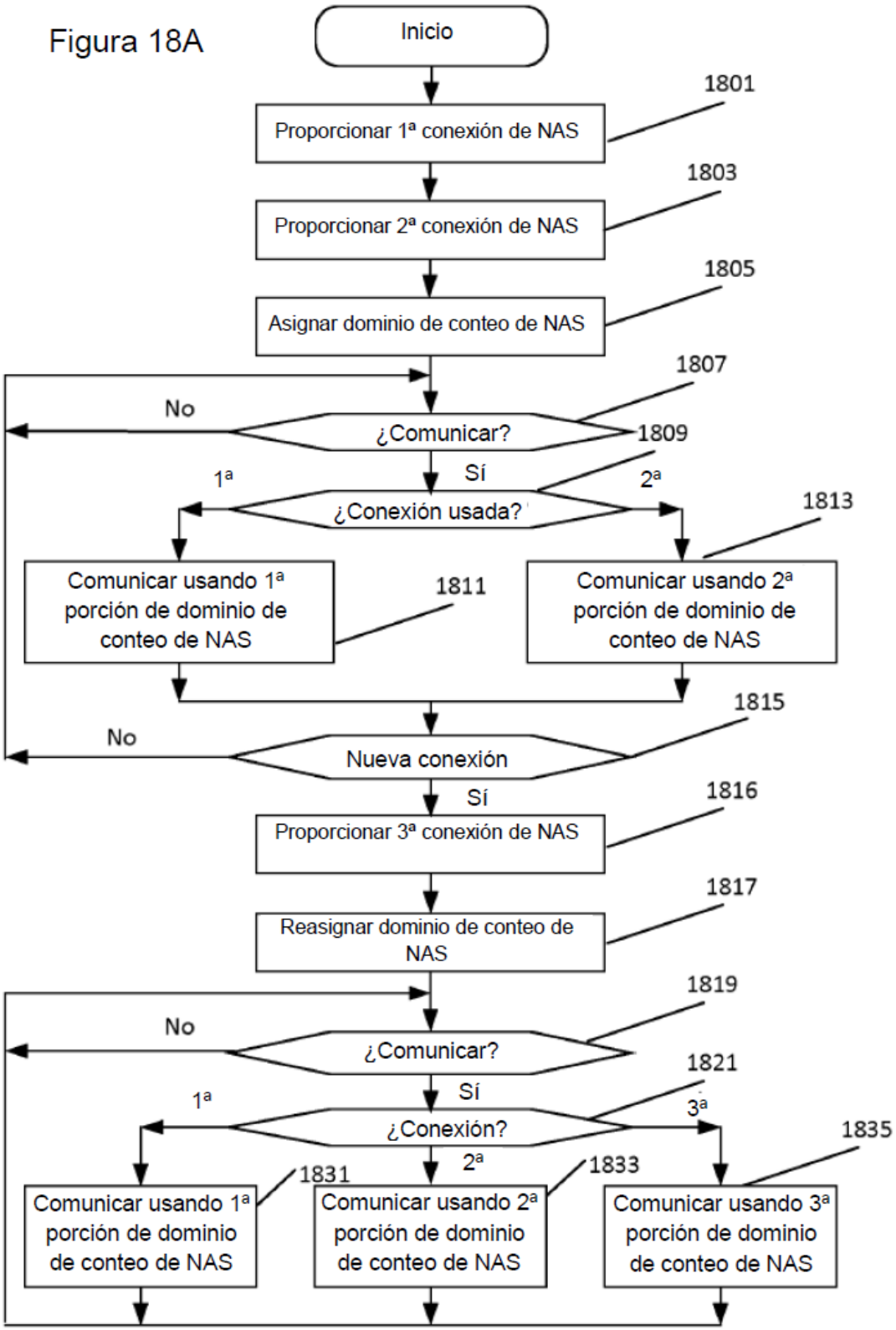
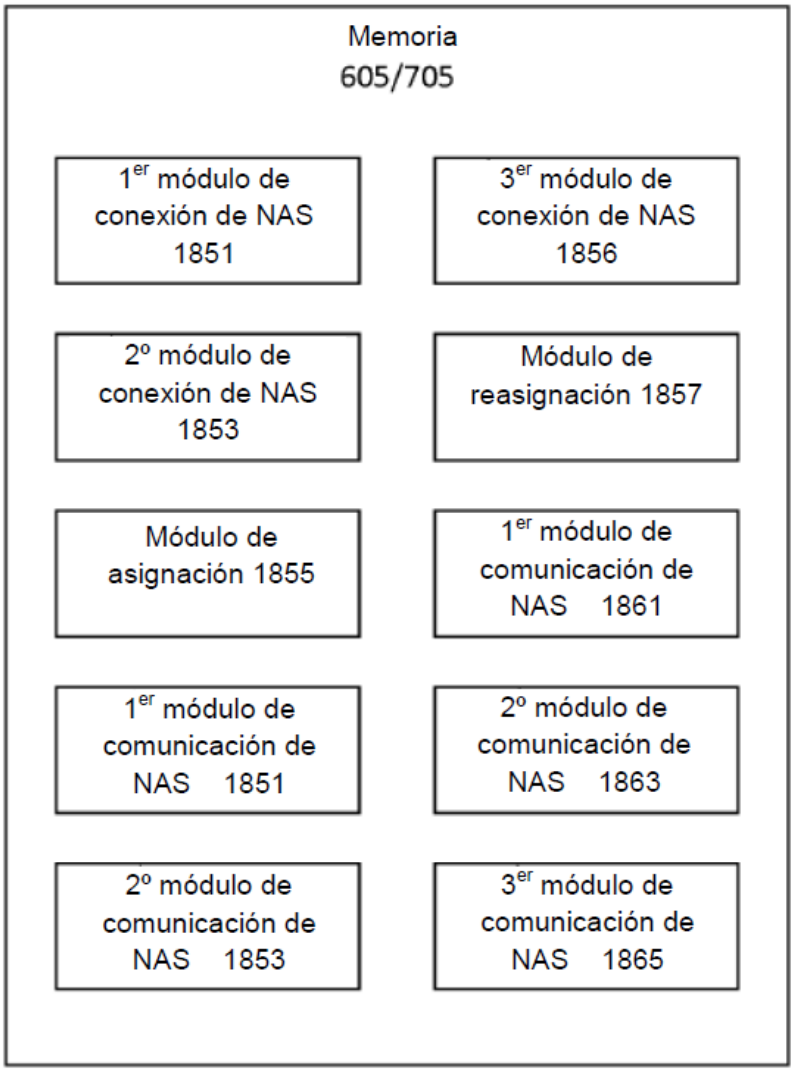

Inicio
1801
Proporcionar 1ª conexión de NAS
1803
Proporcionar 2ª conexión de NAS
1805
Asignar dominio de conteo de NAS
1807
No
¿Comunicar?
1809
Sí
1ª
¿Conexión usada?
2ª
1813
Comunicar usando 1ª porción de dominio de conteo de NAS
1811
Comunicar usando 2ª porción de dominio de conteo de NAS
1815
No
Nueva conexión
Sí
1816
Proporcionar 3ª conexión de NAS
1817
Reasignar dominio de conteo de NAS
1819
No
¿Comunicar?
1821
Sí
1ª
¿Conexión?
3ª
2ª
1835
1831
1833
Comunicar usando 1ª porción de dominio de conteo de NAS
Comunicar usando 2ª porción de dominio de conteo de NAS
Comunicar usando 3ª porción de dominio de conteo de NAS

Figura 18B


Memoria
605/705
1er módulo de conexión de NAS 1851
3er módulo de conexión de NAS 1856
2º módulo de conexión de NAS 1853
Módulo de reasignación 1857
Módulo de asignación 1855
1er módulo de comunicación de NAS 1861
1er módulo de comunicación de NAS 1851
2º módulo de comunicación de NAS 1863
2º módulo de comunicación de NAS 1853
3er módulo de comunicación de NAS 1865