

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 984 699**

51 Int. Cl.:

H04L 9/32 (2006.01)

H04L 9/40 (2012.01)

H04W 12/03 (2011.01)

H04W 12/033 (2011.01)

H04W 12/041 (2011.01)

H04W 12/0431 (2011.01)

H04W 12/069 (2011.01)

H04W 12/106 (2011.01)

H04W 88/06 (2009.01)

H04W 88/10 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **07.05.2018** **E 23157253 (8)**

97 Fecha y número de publicación de la concesión europea: **03.07.2024** **EP 4203384**

54 Título: **Métodos que proporcionan seguridad para múltiples conexiones de NAS utilizando contajes independientes 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:
30.10.2024

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:

ELZABURU, S.L.P

ES 2 984 699 T3

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

DESCRIPCIÓN

Métodos que proporcionan seguridad para múltiples conexiones de NAS utilizando contajes independientes y nodos de red y terminales inalámbricos relacionados

Campo técnico

- 5 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

- 10 En los Sistemas 5G, un UE puede registrarse simultáneamente en la misma PLMN a través de un acceso del 3GPP (por ejemplo, utilizando un nodo de acceso del LTE ó 5G, también denominado estación base, eNB, gNB, etc.) y de un acceso que no sea del 3GPP (por ejemplo, usando un nodo de WiFi ó por satélite). Para este propósito, se espera que el terminal inalámbrico UE y la AMF (Función de Gestión del Acceso) de la red mantengan una conexión para cada tipo de acceso (es decir, una conexión para el acceso del 3GPP y una conexión para la conexión de NAS que no es 3GPP). En tales escenarios, la TS 23.501 (a la que se denomina 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 de Gestión de Registro, uno por tipo de acceso. Por otro lado, se puede utilizar un identificador temporal común.

- 15 Como se describe en la TS 33.401 [2], los mecanismos de seguridad en sistemas heredados pueden proporcionar protección de integridad, de confidencialidad y contra repeticiones para 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 NAS COUNTs, uno para cada dirección (enlace ascendente y enlace descendente). Estos parámetros de seguridad pueden proporcionarse para una conexión de NAS y pueden actualizarse tras la creación de una nueva KASME, por ejemplo tras un procedimiento de autenticación.

- 20 Además, uno de los mecanismos de protección contra repeticiones, materializado en parte por los NAS COUNTs, puede basarse en suposiciones de que el protocolo es fiable y que los procedimientos de 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 ordenada de los mensajes de NAS, de modo que tanto el UE como la MME solo necesitan almacenar dos valores de los NAS COUNTs, uno por dirección (es decir, un NAS COUNT para el enlace ascendente y un NAS COUNT para el enlace descendente). Estos serían los siguientes valores y los únicos esperados/aceptados.

- 25 Sin embargo, con múltiples conexiones a través de accesos del 3GPP y de accesos que no son del 3GPP, la entrega ordenada de mensajes de NAS a través de las diferentes conexiones puede no ser fiable.

Compendio

La invención se define en las reivindicaciones independientes adjuntas.

- 35 Según algunas realizaciones de conceptos inventivos, un método en un primer nodo de comunicación puede proporcionar la comunicación de mensajes de Estrato de Acceso a la 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 nodos de comunicación, y puede proporcionarse una segunda identificación de conexión de NAS para una segunda conexión de NAS entre el primer y el segundo nodos de comunicación. Además, la primera y la segunda identificaciones de conexión de NAS pueden ser diferentes, y la primera y la segunda conexiones de NAS pueden ser diferentes. Se puede comunicar un primer mensaje de NAS entre el primer y el segundo nodos de comunicación a través de la primera conexión de NAS, y la comunicación del primer mensaje de NAS puede incluir llevar a cabo al menos una de generar un código de autenticación de mensaje para la autenticación de integridad del primer mensaje de NAS usando la primera identificación de conexión NAS y/o cifrar/descifrar el primer mensaje de NAS utilizando la primera identificación de conexión de NAS. Se puede comunicar un segundo mensaje de NAS entre el primer y el segundo nodos de comunicación a través de la segunda conexión de NAS, y la comunicación del segundo mensaje de NAS puede incluir llevar a cabo al menos una 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 utilizando la segunda identificación de conexión de NAS.

- 40 Según algunas otras realizaciones de conceptos inventivos, un método en un primer nodo de comunicación puede proporcionar la comunicación de mensajes de Estrato de Acceso a la Red (NAS) con un segundo nodo de comunicación. Puede proporcionarse una primera conexión de NAS entre el primer y el segundo nodos de comunicación, y puede proporcionarse una segunda conexión de NAS entre el primer y el segundo nodos de comunicación. Además, la primera y la segunda conexiones de NAS pueden ser diferentes. Se puede asignar un dominio de contajes de NAS de modo que una primera parte del dominio de contajes de NAS se asigne para mensajes de NAS comunicados a través de la primera conexión de NAS y de modo que una segunda parte del dominio de

contajes de NAS se asigne para mensajes de NAS comunicados a través de la segunda conexión de NAS. Además, la primera y la segunda partes del dominio de contajes de NAS pueden ser mutuamente excluyentes. Los mensajes de NAS pueden producirse a través de la primera conexión de NAS utilizando el valor de contaje de NAS más bajo de la primera parte del dominio de contajes de NAS que no se haya utilizado 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 utilizando el valor de contaje de NAS más bajo de la segunda parte del dominio de contajes de NAS que no se haya utilizado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS.

De acuerdo con algunas realizaciones de conceptos inventivos descritos en este 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 mayor comprensión de la divulgación y se incorporan a esta solicitud y constituyen una parte de la misma, ilustran ciertas realizaciones no limitativas de conceptos inventivos. En los dibujos:

la Figura 1 es un diagrama que ilustra un ejemplo de organización de mensajes para un mensaje de NAS protegido en cuanto a seguridad;

la Figura 2 es una tabla que ilustra tipos de encabezamientos de seguridad del mensaje de NAS protegido en cuanto a seguridad de la Figura 1;

las Figuras 3A y 3B ilustran el uso de un proceso EIA de integridad de 128 bits para autenticar la integridad de 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 múltiples conexiones de NAS entre un nodo de red central y un terminal inalámbrico según algunas realizaciones de conceptos inventivos;

la Figura 6 es un diagrama de bloques que ilustra elementos de un terminal inalámbrico UE según algunas realizaciones de conceptos inventivos;

la Figura 7 es un diagrama de bloques que ilustra elementos de un nodo de red según algunas realizaciones de conceptos inventivos;

las Figuras 8 y 9 son diagramas de bloques que ilustran 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 inventivos;

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

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 inventivos;

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

las Figuras 15 y 16 ilustran derivaciones de clave que pueden usarse de acuerdo con algunas realizaciones de conceptos inventivos;

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

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

Descripción detallada

A continuación se describirán en la presente conceptos inventivos más exhaustivamente con referencia a los dibujos adjuntos, en los que se muestran ejemplos de realizaciones de conceptos inventivos. Sin embargo, los conceptos de inventivos pueden incorporarse 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 resulte minuciosa y completa, y transmita completamente el alcance de los presentes conceptos inventivos 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 utilizan en otra realización.

La siguiente descripción presenta varias realizaciones de la materia en cuestión dada a conocer. Estas realizaciones se presentan como ejemplos didácticos y no deben interpretarse como limitativas del alcance de la materia en cuestión dada a conocer. Por ejemplo, ciertos detalles de las realizaciones descritas pueden modificarse, omitirse o ampliarse sin desviarse del alcance de la materia en cuestión descrita.

5 La Figura 5 es un diagrama de bloques que ilustra múltiples conexiones de NAS entre el nodo 501 de red central (que proporciona gestión de acceso) y un terminal inalámbrico UE 505 según algunas realizaciones de conceptos inventivos. Como se muestra, se puede proporcionar una primera conexión de NAS a través de un nodo de acceso del 3GPP (por ejemplo, una estación base, eNB, eNodeB, gNB, gNodeB), se puede proporcionar una segunda conexión de NAS a través de un primer nodo de acceso que no es 3GPP (por ejemplo, un nodo de acceso de WiFi),
10 y se puede proporcionar una tercera conexión de NAS a través de un segundo nodo de acceso que no sea 3GPP (por ejemplo, un nodo por satélite). Con diferentes conexiones de NAS proporcionadas a través de diferentes nodos de acceso de diferentes tecnologías, se puede reducir la probabilidad de que el nodo receptor (ya sea 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.

15 La Figura 6 es un diagrama de bloques que ilustra 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 según realizaciones de conceptos inventivos. Como se muestra, el terminal inalámbrico UE puede incluir un circuito 601 de transceptor (también denominado transceptor) que incluye un transmisor y un receptor configurados para
20 proporcionar radiocomunicaciones de enlace ascendente y de enlace descendente con una estación o estaciones base de una red de acceso por radiocomunicaciones. 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 código de programa legible por ordenador que cuando es ejecutado por el circuito 603 de procesador hace que el circuito de
25 procesador realice operaciones de acuerdo con realizaciones dadas a conocer en este documento. Según otras realizaciones, el circuito 603 de procesador puede definirse para incluir memoria de modo que no se requiera un circuito de memoria aparte. 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 proporcione una
30 salida visual, un altavoz que proporcione una salida de audio y/o un dispositivo de entrada de usuario (por ejemplo, una pantalla táctil, un teclado, un botón(es), etc.) que acepte la entrada del usuario.

Como se analiza en este 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
35 transmitir comunicaciones a través del transceptor 601 sobre una interfaz de radiocomunicaciones a un nodo de acceso y/o para recibir comunicaciones a través del transceptor 601 desde un nodo de acceso sobre una interfaz de radiocomunicaciones. Además, pueden almacenarse módulos en la memoria 605, y estos módulos pueden proporcionar instrucciones de modo que cuando el procesador 603 ejecute instrucciones de un módulo, el procesador 603 realice operaciones respectivas (por ejemplo, operaciones que se describen más adelante con respecto a Realizaciones de Ejemplo).

40 La Figura 7 es un diagrama de bloques que ilustra elementos de un nodo de red (también denominado nodo de red central, estación base, eNB, eNodeB, gNB, gNodeB, etc.) de una Red de Acceso por Radiocomunicaciones (RAN) configurada para admitir comunicaciones inalámbricas de acuerdo con realizaciones de conceptos inventivos. Como se muestra, el nodo de red puede incluir un circuito 701 de interfaz de red (también denominado interfaz de red) que incluye un transmisor y un receptor configurados para proporcionar radiocomunicaciones de enlace ascendente y de
45 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 código de programa legible por ordenador que cuando es ejecutado por el circuito 703 de procesador hace que el circuito de procesador realice operaciones de acuerdo con
50 realizaciones dadas a conocer en este documento. Según otras realizaciones, el circuito 703 de procesador puede definirse para incluir memoria de modo que no se requiera un circuito de memoria aparte.

Como se analiza en este 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
55 comunicaciones a través de la interfaz 701 de red a uno o más nodos de acceso y/o recibir comunicaciones a través de la interfaz de red desde uno o más nodos de acceso como se muestra en la Figura 5. Además, pueden almacenarse módulos en la memoria 705, y estos módulos pueden proporcionar instrucciones para que cuando el procesador 703 ejecute instrucciones de un módulo, el procesador 703 realice operaciones respectivas (por ejemplo, operaciones discutidas más adelante con respecto a Realizaciones de Ejemplo). Aunque no se muestra en las Figuras 5 y 7, las operaciones del nodo 503-1 de acceso del 3GPP y el nodo 501 de red pueden combinarse proporcionando un
60 transceptor en el nodo 501 de red. En tales realizaciones, el transceptor del nodo 501 de red puede proporcionar la conexión de NAS del 3GPP a través de una interfaz directa del 3GPP con el terminal inalámbrico 505. Según tales realizaciones, el procesador 703 puede controlar el transceptor para transmitir una comunicación a través del

transceptor sobre una interfaz de radiocomunicaciones al terminal inalámbrico 505 y/o para recibir comunicaciones a través del transceptor desde el terminal inalámbrico 505.

A continuación se analizará un formato de mensaje general y la codificación de elementos de información para los mensajes de NAS en el EPC.

- 5 Para sistemas EPC/LTE heredados, la TS 24.301 (a la que también se denomina referencia [3]) describe un formato de mensaje general y una codificación de elementos de información para mensajes de NAS. Si el mensaje de NAS es un mensaje de NAS protegido en cuanto a seguridad, el mensaje incluye las siguientes partes:

- a) discriminador de protocolo;
- b) tipo de encabezamiento de seguridad;
- 10 c) código de autenticación de mensaje (MAC);
- d) número de secuencia; y
- e) mensaje de NAS en claro.

La organización de un mensaje de NAS protegido en cuanto a 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 en cuanto a seguridad.

- 15 Los bits 5 a 8 del primer octeto de cada mensaje de Gestión de Movilidad de EPS (EMM) contienen el IE Tipo de encabezamiento de seguridad. Este IE incluye información de control relacionada con la protección de seguridad de un mensaje de NAS. El tamaño total del IE Tipo de encabezamiento de seguridad es de 4 bits. El IE Tipo de encabezamiento de seguridad puede adoptar los valores que se muestran en la tabla de la Figura 2, que ilustra tipos de encabezamiento de seguridad del mensaje de NAS protegido en cuanto a seguridad de la Figura 1.

- 20 El elemento de información Código de autenticación del mensaje (MAC) de la Figura 1 incluye/contiene la información de protección de integridad del mensaje. El IE MAC se incluye en el mensaje de NAS protegido en cuanto a seguridad si existe un contexto de seguridad de EPS válido y se inician funciones de seguridad.

El IE Número de secuencia en la Figura 1 incluye el número de secuencia (SN) del mensaje de NAS que consiste en los ocho bits menos significativos del NAS COUNT para un mensaje de NAS protegido en cuanto a seguridad.

- 25 Cuando un mensaje de NAS se va a enviar tanto cifrado como protegido en cuanto a integridad, primero se cifra el mensaje de NAS y a continuación el mensaje de NAS cifrado y el número de secuencia de NAS (NAS COUNT) se protegen en cuanto a integridad calculando el MAC.

Cuando se va a enviar un mensaje de NAS solo con protección de integridad y sin cifrar, el mensaje de NAS sin cifrar y el número de secuencia de NAS se protegen en cuanto a integridad mediante el cálculo del MAC.

- 30 La TS 33.401 (a la que se denomina también referencia [2]) y la TS 24.301 (a la que se denomina también referencia [3]) describen que cada KASME independiente tiene, asociado a la misma, un par distinto de NAS COUNTs, un NAS COUNT para el enlace ascendente y un NAS COUNT para el enlace descendente.

- 35 Los NAS COUNTs para una KASME en particular no se restablecen a los valores iniciales (es decir, los NAS COUNTs solo tienen su valor inicial cuando se crea una nueva KASME). Esto reduce/evita el problema de seguridad de usar los mismos NAS COUNTs con las mismas claves de NAS, p. ej. reutilización del flujo de claves.

- La TS 24.301 (a la que se denomina también referencia [3]) describe que el remitente utiliza su NAS COUNT almacenado localmente como entrada para el proceso de protección/verificación de integridad (también conocido como algoritmo de verificación/protección de integridad) que se utiliza 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 NAS COUNT para el proceso de verificación de integridad.

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

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

Se puede utilizar un proceso de integridad de 128 bits en el EPC/LTE. De acuerdo con la TS 33.401 (a la que se denomina también referencia [2]), los parámetros de entrada para el proceso de integridad de 128 bits son una clave de integridad de 128 bits llamada KEY, un COUNT de 32 bits (es decir, NAS COUNT), una identidad del portador de 5 bits denominada BEARER, la dirección de la transmisión de 1 bit (es decir, DIRECTION) y el propio mensaje (es decir, MESSAGE). El bit de DIRECTION puede ser/será 0 para el enlace ascendente y 1 para el enlace descendente. La longitud en bits del MESSAGE es LENGTH. Las Figuras 3A y 3B ilustran el uso del proceso de integridad de 128 bits EIA para autenticar la integridad de mensajes. Como se muestra en la Figura 3A, el remitente 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 remitente calcula un código de autenticación de mensaje de 32 bits (MAC-I/NAS-MAC) utilizando el proceso de integridad EIA (también denominado algoritmo de integridad EIA) de la Figura 3A. El código de autenticación de mensaje (MAC) se añade entonces 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) sobre el mensaje recibido (usando el proceso de integridad EIA de la Figura 3B, también denominado algoritmo de integridad) de la misma manera en que el remitente calculó su código de autenticación de mensaje sobre el mensaje enviado y verifica la integridad de los datos del mensaje comparando el MAC calculado con el código de autenticación de mensaje recibido, es decir, MAC-I/NAS-MAC.

La TS 24.301 (a la que se denomina también referencia [3]) describe que el remitente usa su NAS COUNT 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 del contador de desbordamiento de NAS para formar la entrada NAS COUNT para el algoritmo de descifrado.

Puede utilizarse un algoritmo de cifrado de 128 bits. Según la TS 33.401 (a la que se denomina también referencia [2]), los parámetros de entrada para el proceso de cifrado (también conocido como algoritmo de cifrado) son una clave de cifrado de 128 bits llamada KEY, un COUNT de 32 bits (es decir, NAS COUNT), una identidad de portador de 5 bits BEARER, la dirección de la transmisión de 1 bit (es decir, DIRECTION) y la longitud del flujo de claves requerida (es decir, LENGTH). El bit de DIRECTION será 0 para el enlace ascendente y 1 para el 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 KEYSTREAM que se utiliza para cifrar el bloque de texto en claro de entrada PLAINTEXT para producir el bloque de texto cifrado de salida CIPHERTEXT.

El soporte de múltiples conexiones de NAS terminadas en la misma AMF puede dar lugar a nuevos problemas que incluyen compatibilidad a futuro, simultaneidad, indiferencia tecnológica y/o flexibilidad.

Con respecto a la compatibilidad a futuro, la clasificación de tipos de accesos en 3GPP y no 3GPP es, de hecho, compatible a futuro y se puede aplicar a cualquier nueva tecnología de acceso futura. Aunque parece que puede que no sea necesario admitir 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 sobre 3GPP y dos sobre accesos que no sean del 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 admita de manera eficiente un número arbitrario (hasta un límite) de conexiones simultáneas.

Con respecto a la simultaneidad, la introducción de múltiples conexiones de NAS puede causar problemas de simultaneidad, ya que ahora puede ser posible que el sistema se ejecute en múltiples procedimientos de NAS paralelos en los diferentes tramos de NAS. Es concebible forzar que la AMF ejecute los procedimientos de NAS de uno en uno, independientemente de la conexión de NAS, de modo que se conserven las suposiciones subyacentes del mecanismo de seguridad heredado. Esto no es lo esperable. Por ejemplo, un procedimiento de NAS que falla 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 fallos. Esta puede ser una elección de diseño no deseable. Por lo tanto, puede ser mejor que el nuevo mecanismo de seguridad admita la ejecución paralela de procedimientos de NAS en las diferentes conexiones.

En cuanto a la indiferencia tecnológica, 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 contra repeticiones. Los servicios de seguridad deben proporcionarse de manera transparente ante el tipo de acceso, de acuerdo con el principio de diseño general de una arquitectura de 5G indiferente al acceso.

En cuanto a la flexibilidad, la nueva característica de múltiples conexiones de NAS puede dar lugar a nuevos escenarios que no eran posibles en 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. De forma más precisa, el UE puede registrarse en un tramo de 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 admitir tales escenarios de movilidad.

De acuerdo con algunas realizaciones de conceptos inventivos, se pueden proporcionar métodos para proteger conexiones de NAS paralelas. Dichos métodos pueden basarse en compartir parcialmente el contexto de seguridad para 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 un par independiente dedicado de NAS COUNTs basados en el uso de un parámetro de NAS llamado NAS CONN ID (Identificación de Conexión de NAS) para identificar cada conexión de NAS con el mismo terminal inalámbrico.

De acuerdo con algunas realizaciones, los métodos/dispositivos dados a conocer pueden abordar problemas relacionados con la compatibilidad a futuro, la simultaneidad, la indiferencia tecnológica y la flexibilidad, al tiempo que brindando un nivel similar/idéntico de servicios de seguridad y protección en relación con la conexión de NAS en comparación con sistemas heredados.

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

Primero, puede haber una clave específica de la AMF, indicada por KAMF que es el equivalente de KASME en los Sistemas del 5G. Esta clave se establece mediante una autenticación exitosa y se utiliza 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 ordenada de los mensajes de NAS en cada tramo (conexión). Más particularmente, los supuestos de transporte de NAS subyacentes de sistemas heredados pueden seguir aplicándose, pero según cada conexión de NAS, aunque esto no excluye las ejecuciones paralelas de procedimientos de 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 cada conexión de NAS. Se espera que la negociación tenga lugar una vez durante el establecimiento y activación de la clave de AMF, por ejemplo el equivalente del procedimiento SMC de NAS en 5G. El procedimiento SMC (Orden de Modo de Seguridad) de NAS se describe en detalle en la TS 33.401 (a la que se denomina también referencia [2]).

También se puede suponer que la seguridad de NAS es una función adicional de 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 criterio de 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 (incluida 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 (incluyendo la Función de Seguridad de NAS y la Función de Gestión de Conexión de NAS) de la Figura 9 pueden ser realizadas por 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 interactúe 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 la cual realiza las comprobaciones y operaciones criptográficas y devuelve el resultado (por ejemplo, si la comprobación de integridad falla o es superada, y/o si el mensaje está descifrado, etc.). Cuando un mensaje debe protegerse en el enlace descendente, la función de gestión de la conexión de NAS proporciona la carga útil a la función de seguridad la cual realiza las operaciones necesarias y devuelve el mensaje protegido.

Las Figuras 8 y 9 ilustran Funciones de Seguridad de NAS en un nodo de red central y en un terminal inalámbrico, respectivamente.

Para el 5G, se espera que el contexto de seguridad de NAS pueda incluir la clave de AMF KAMF, las claves de protección derivadas KNASint y KNASenc, y el equivalente del identificador de conjunto de claves eKSI en el 5G. Según algunas realizaciones de la presente divulgación, se puede usar un par independiente de NAS COUNTs para cada conexión de NAS con un terminal inalámbrico en este contexto de seguridad de NAS.

Como se ha descrito anteriormente, para cada conexión de NAS, se puede usar/mantener un par independiente de NAS COUNTs, 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, puede introducirse un parámetro específico de la conexión de NAS, y este parámetro específico de la conexión de NAS puede denominarse identificador de conexión de NAS e indicarse como NAS CONN ID.

El NAS CONN ID es un número que se incrementa cada vez que se establece una nueva conexión de NAS para un terminal inalámbrico. En el contexto de seguridad, cada par de NAS COUNT está asociado a un valor de NAS CONN ID único. El nuevo parámetro se utiliza como diferenciador cuando se interactúa con la función de seguridad de NAS para indicar a qué conexión de NAS pertenece cada mensaje. Para realizar un seguimiento de valores de NAS CONN ID no asignados, se puede usar/necesitar un parámetro adicional. Este nuevo parámetro, indicado por NEXT NAS

CONN ID también puede ser parte del contexto de seguridad. El parámetro NEXT NAS CONN ID se fija inicialmente a 0 y se incrementa cada vez que se establece 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 NEXT NAS CONN ID. Más particularmente, se crea un nuevo par de NAS COUNT y el mismo se asocia a un NAS CONN ID cuyo valor se fija a el valor actual de NEXT NAS CONN ID. A continuación, se incrementa el valor de NEXT NAS CONN ID. De este modo, la Identificación de Conexión de NAS NAS CONN ID se puede utilizar como entrada (directa o indirectamente) para procesos de autenticación y/o cifrado/descifrado.

De acuerdo con algunas realizaciones de conceptos inventivos, cuando se crea un nuevo par de NAS COUNT, los valores de los contadores se fijan a 0. El NAS CONN ID puede ser un valor de 8 bits que se utiliza para rellenar la representación interna de 24 bits de NAS COUNT cuando se construye la entrada para los procesos de cifrado/descifrado y/o integridad de NAS. En sistemas heredados, el relleno siempre se puede fijar a 0 como se describe en la TS 24.301 (a la que se denomina también referencia [3]). Dado que cada conexión de NAS se identifica mediante una NAS CONN ID única, el relleno proporciona/garantiza la separación criptográfica para 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 mensajes usando la NAS CONN ID en los lados del remitente y del receptor. Al incorporar la Identificación de Conexión de NAS NAS CONN ID en la entrada COUNT, se puede proporcionar una separación para la autenticación de diferentes conexiones de NAS para el mismo terminal inalámbrico. La entrada COUNT, por ejemplo, puede ser un valor de 32 bits generado como una concatenación del NAS CONN ID de 8 bits para la conexión de NAS y el NAS COUNT de 24 bits para la conexión de NAS (es decir, COUNT (32 bits) = NAS CONN ID (8 bits) || NAS COUNT (24 bits)). La Figura 10A ilustra así el uso del NAS CONN ID para derivar MAC-I/NAS-MAC en el lado del transmisor, y la Figura 10B ilustra el uso del NAS CONN ID 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 el NAS CONN ID en los lados del remitente y del receptor. Al incorporar la Identificación de Conexión de NAS NAS CONN ID en la entrada COUNT, se puede proporcionar una separación para cifrar/descifrar diferentes conexiones de NAS para el mismo terminal inalámbrico. La entrada COUNT, por ejemplo, puede ser un valor de 32 bits generado como una concatenación del NAS CONN ID de 8 bits para la conexión de NAS y el NAS COUNT de 24 bits para la conexión de NAS (es decir, COUNT (32 bits) = NAS CONN ID (8 bits) || NAS COUNT (24 bits)). La Figura 11A ilustra así el uso del NAS CONN ID para cifrar el texto en claro en el lado del transmisor, y la Figura 11B ilustra el uso del NAS CONN ID para descifrar el texto cifrado en el lado del receptor.

Según algunas otras realizaciones, el NAS CONN ID puede ser un valor de 5 bits que se usa como entrada BEARER 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 mensajes usando el NAS CONN ID en los lados del remitente y del receptor. Al utilizar la Identificación de Conexión de NAS NAS CONN ID como entrada BEARER, se puede proporcionar una separación para la autenticación de diferentes conexiones de NAS para el mismo terminal inalámbrico. La Figura 12A ilustra así el uso del NAS CONN ID como entrada BEARER para derivar MAC-I/NAS-MAC en el lado del transmisor, y la Figura 12B ilustra el uso del NAS CONN ID como entrada BEARER 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 el NAS CONN ID en los lados del remitente y del receptor. Al utilizar la Identificación de Conexión de NAS NAS CONN ID como entrada BEARER, se puede proporcionar una separación para cifrar/descifrar diferentes conexiones de NAS para el mismo terminal inalámbrico. La Figura 13A ilustra así el uso del NAS CONN ID como entrada BEARER para cifrar el texto en claro en el lado del transmisor, y la Figura 13B ilustra el uso de NAS CONN ID como entrada BEARER para descifrar el texto cifrado en el lado del receptor.

Se analizarán a continuación operaciones que proporcionan autenticación de integridad y/o cifrado/descifrado de las Figuras 10A-B, 11A-B, 12A-B y/o 13A-B con respecto al diagrama de flujo de las Figuras 17A y 17B.

Se analizarán a continuación operaciones de un nodo de comunicación 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 de terminal inalámbrico de la Figura 6 si el nodo de comunicación es un terminal inalámbrico, o la memoria 705 de 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 del 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 lleva a cabo operaciones respectivas del diagrama de flujo de la Figura 17A.

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

Para una comunicación a través de la primera conexión de NAS en el bloque 1717, el procesador del nodo de comunicación puede comunicar un primer mensaje de NAS entre el primer y el segundo nodos de comunicación a través de la primera conexión de NAS (por ejemplo, usando el primer módulo 1757 de comunicación). Más particularmente, la comunicación del primer mensaje de NAS puede incluir al menos una de llevar a cabo una protección de integridad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y/o llevar a cabo una 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 del nodo de comunicación puede comunicar un segundo mensaje de NAS entre el primer y el segundo nodos de comunicación a través de la segunda conexión de NAS (por ejemplo, usando el segundo módulo 1759 de comunicación). Más particularmente, la comunicación del segundo mensaje de NAS puede incluir al menos una de llevar a cabo al menos una de llevar a cabo una protección de integridad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y/o llevar a cabo una protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS.

La primera y la segunda conexiones de NAS comparten una clave maestra de un contexto de seguridad de NAS. Además, la comunicación del primer mensaje de NAS puede incluir al menos una de llevar a cabo una protección de integridad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra y/o llevar a cabo una protección de confidencialidad para el primer mensaje de NAS usando la primera identificación de conexión de NAS y la clave maestra. De manera similar, la comunicación del segundo mensaje de NAS puede incluir al menos una de llevar a cabo una protección de integridad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave maestra y/o llevar a cabo una protección de confidencialidad para el segundo mensaje de NAS usando la segunda identificación de conexión de NAS y la clave 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 ha descrito anteriormente, la primera y la segunda conexiones 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 llevar a cabo una protección de integridad generando un primer código de autenticación de mensaje basado 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, la comunicación del segundo mensaje de NAS puede incluir llevar a cabo una protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basado 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.

Según algunas realizaciones para el nodo transmisor, 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 puede 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 puede proporcionarse como entrada para generar el segundo código de autenticación de mensaje. Según algunas otras realizaciones para el nodo transmisor, 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. Según otras realizaciones más para el nodo transmisor, 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 utilizada para generar el segundo código de autenticación de mensaje. Además, la aplicación de la protección de integridad para el primer mensaje de NAS puede incluir llevar a cabo una protección de integridad para el primer mensaje de NAS utilizando una interfaz de protección de integridad de EIA compatible con el 5G, y llevar a cabo la protección de integridad para el segundo mensaje de NAS puede incluir llevar a cabo una protección de integridad para el segundo mensaje de NAS utilizando la interfaz de protección de integridad de EIA compatible con el 5G.

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 ha descrito anteriormente, la primera y la segunda conexiones 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 llevar a cabo una protección de confidencialidad para el primer mensaje de NAS mediante el cifrado del primer mensaje de NAS utilizando 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 llevar a cabo una protección de confidencialidad para el segundo mensaje de NAS mediante el cifrado del segundo mensaje de NAS utilizando 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.

Según algunas realizaciones para el nodo transmisor, 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 puede 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 puede proporcionarse como entrada para generar el segundo mensaje de NAS cifrado. Según algunas otras realizaciones del nodo transmisor, 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. Según otras realizaciones más del nodo transmisor, 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 utilizarse para derivar una segunda clave de cifrado que se utiliza para generar el segundo mensaje de NAS cifrado. El cifrado del primer mensaje de NAS puede incluir cifrar el primer mensaje de NAS utilizando el cifrado de EEA, y el cifrado del segundo mensaje de NAS comprende cifrar el segundo mensaje de NAS utilizando el cifrado de EEA. Además, la aplicación de la protección de confidencialidad para el primer mensaje de NAS puede incluir llevar a cabo una protección de confidencialidad para el primer mensaje de NAS utilizando una interfaz de cifrado de EEA compatible con el 5G, y la aplicación de la protección de confidencialidad para el segundo mensaje de NAS puede incluir llevar a cabo una protección de confidencialidad para el segundo mensaje de NAS utilizando la interfaz de cifrado de EEA compatible con el 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 ha descrito anteriormente, la primera y la segunda conexiones de NAS pueden compartir una clave maestra de un contexto de seguridad de NAS. En el bloque 1715, la comunicación del 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, llevar a cabo 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 a la coincidencia del primer código de autenticación de mensaje y el primer código de autenticación de mensaje derivado. En el bloque 1719, la comunicación del 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, llevar a cabo 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 a la coincidencia del segundo código de autenticación de mensaje y el segundo código de autenticación de mensaje derivado.

Según algunas realizaciones para el nodo receptor, 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 puede proporcionarse como 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 puede proporcionarse como entrada para generar el segundo código de autenticación de mensaje derivado. Según algunas otras realizaciones para el nodo receptor, 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. Según otras realizaciones más para el nodo receptor, 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 utilizarse para derivar una segunda clave de protección de integridad utilizada para generar el segundo código de autenticación de mensaje derivado. Además, la aplicación de la protección de integridad para el primer mensaje de NAS puede incluir llevar a cabo una protección de integridad para el primer mensaje de NAS utilizando una interfaz de protección de integridad de EIA compatible con el

5G, y la aplicación de la protección de integridad para el segundo mensaje de NAS puede incluir llevar a cabo una protección de integridad para el segundo mensaje de NAS utilizando la interfaz de protección de integridad de EIA compatible con el 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 ha descrito anteriormente, la primera y la segunda conexiones 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 recibir un primer mensaje de NAS cifrado a través de la primera conexión de NAS desde el segundo nodo de comunicación, llevar a cabo una protección de confidencialidad para el primer mensaje de NAS mediante el descifrado del primer mensaje de NAS cifrado utilizando 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, la comunicación del 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, llevar a cabo una protección de confidencialidad para el segundo mensaje de NAS mediante el descifrado del segundo mensaje de NAS cifrado utilizando 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.

Según algunas realizaciones para el nodo receptor, 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 puede proporcionarse como 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 puede proporcionarse como entrada para generar el segundo mensaje de NAS cifrado. Según algunas otras realizaciones para el nodo receptor, 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. Según otras realizaciones más para el nodo receptor, 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 utilizada para generar el segundo mensaje de NAS descifrado. Además, la aplicación de la protección de confidencialidad para el primer mensaje de NAS puede incluir llevar a cabo una protección de confidencialidad para el primer mensaje de NAS utilizando una interfaz de descifrado de EEA compatible con el 5G, y la aplicación de la protección de confidencialidad para el segundo mensaje de NAS puede incluir llevar a cabo una protección de confidencialidad para el segundo mensaje de NAS utilizando la interfaz de descifrado de EEA compatible con el 5G.

En realizaciones de la Figura 17A, la primera conexión de NAS puede proporcionarse a través de un nodo de acceso del 3GPP entre el primer y el segundo nodos de comunicación, y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso que no sea del 3GPP entre el primer y el segundo nodos de comunicación; o la primera conexión de NAS puede proporcionarse a través de un nodo de acceso que no sea del 3GPP entre el primer y el segundo nodos de comunicación y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso del 3GPP entre el primer y el segundo nodos de comunicación. Por ejemplo, el nodo de acceso del 3GPP puede incluir una estación base de la red de acceso por radiocomunicaciones, y el nodo de acceso que no es del 3GPP puede incluir al menos uno de un nodo de acceso de WiFi y/o un nodo de acceso satelital.

Además, la primera y la segunda conexiones de NAS de la Figura 17A pueden mantenerse simultáneamente entre el primer y el segundo nodos de comunicación. Además, se puede establecer una sesión de Unidades de Datos por Paquetes (PDU) sobre la base del primer y el segundo mensajes de NAS para comunicar datos del plano de usuario entre el primer y el segundo nodos 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 de ejemplo 1 (que se expone a continuación), por ejemplo, las operaciones del bloque 1715 de la Figura 17B pueden ser opcionales.

Según algunas otras realizaciones, el dominio de NAS COUNT se puede dividir dependiendo del número de conexiones de NAS en ejecución como se describe a continuación.

Una de las diferencias en relación con realizaciones descritas anteriormente con respecto a las Figuras 10A-B, 11A-B, 12A-B y 13A-B es que el NAS CONN ID 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 de NAS CONN ID.

En tales realizaciones, se puede usar un nuevo parámetro indicado por NAS CONN NUM para realizar un seguimiento del número de conexiones de NAS en ejecución para un terminal inalámbrico. Además, se puede utilizar un par especial de NAS COUNTs para realizar un seguimiento de los valores máximos de los COUNTs en el enlace ascendente y el enlace descendente en todos los pares de NAS COUNT disponibles. Este parámetro puede denominarse par de MAX NAS COUNTs. Inicialmente, todos los parámetros se fijan a 0. Cuando se establece una

nueva conexión de NAS para un terminal inalámbrico, a la nueva conexión de NAS se le asigna el valor de NAS CONN NUM actual como NAS CONN ID. Se crea un nuevo par de NAS COUNTs con su valor fijado a los valores actuales de NAS COUNT MAX añadidos al NAS CONN ID de la conexión. Para todas las conexiones existentes, los valores de NAS COUNT se ajustan a los valores actuales de NAS COUNT MAX añadidos al valor de NAS CONN ID correspondiente. Finalmente, se incrementa NAS CONN NUM.

En caso de que una conexión de NAS termine, entonces el NAS CONN NUM se decrementa, todas las conexiones con un identificador por encima del de la conexión eliminada se decrementan y todos los NAS COUNTs se ajustan como en el caso de adición de conexión. Siempre que un mensaje de NAS se procesa exitosamente (para su transmisión o tras una recepción), entonces para esa conexión de NAS, el valor de NAS COUNT se incrementa en NAS COUNT NUM. Intuitivamente, el NAS CONN NUM se utiliza como incremento para todos los NAS COUNTs. Sin embargo, para reducir/prevenir el solapamiento, cada vez que se establece o elimina una conexión, los NAS COUNTs se reajustan en función de los valores de NAS COUNT MAX actuales y los correspondientes NAS CONN IDs (posiblemente reajustados).

Es posible que esta realización no proporcione/garantice un uso eficiente/buena del dominio de NAS COUNT. En caso de que una conexión de NAS esté más activa que las otras (impulsando los valores de MAX NAS COUNT), entonces la terminación de la conexión de NAS más activa puede provocar un salto adelante en los valores de NAS COUNT de las conexiones restantes y, por lo tanto, un desperdicio de valores de NAS COUNT.

Se analizarán a continuación operaciones de un nodo de comunicación con referencia al diagrama de flujo de la Figura 18A y los módulos de la Figura 18B. Por ejemplo, los módulos de la Figura 18B 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 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 del 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 operaciones respectivas 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 nodos 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 nodos de comunicación en el bloque 1803 (por ejemplo, usando el segundo módulo 1853 de conexión de NAS). Además, la primera y la segunda conexiones de NAS pueden ser diferentes.

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

Para una comunicación de 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 el valor de contaje de NAS más bajo de la primera parte del Dominio de contajes de NAS que no se ha utilizado previamente para cada mensaje de NAS comunicado a través de la primera conexión de NAS (p. ej., utilizando el primer módulo 1851 de comunicación de NAS). El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la segunda conexión de NAS en el bloque 1813 utilizando el valor de contaje de NAS más bajo de la segunda parte del dominio de contajes de NAS que no se ha utilizado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS (p. ej., utilizando el segundo módulo 1853 de comunicación de NAS).

Los valores de contaje de NAS de la primera y la segunda partes del dominio de contajes de NAS pueden estar intercalados. Con dos conexiones de NAS, la primera parte del dominio de contajes de NAS puede incluir valores de contaje de NAS pares, y la segunda parte del dominio de contajes de NAS puede incluir valores de contaje de NAS impares. Con esta división del dominio de contaje 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 parte del dominio de Contaje de NAS, y a los mensajes de NAS comunicados a través de la segunda conexión de NAS se les pueden asignar números de secuencia 1, 3, 5, 7, etc. de la segunda parte del dominio de contajes de NAS. Además, si una de las conexiones de NAS está más activa, se pueden asignar más números de secuencia de una parte del dominio de Contaje de NAS que de la otra parte del dominio de contaje 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 NAS Count Max 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 nodos de comunicación (por ejemplo, utilizando el tercer módulo 1856 de conexión de NAS). La primera y la tercera conexiones de NAS son diferentes, y la segunda y la tercera conexiones de NAS son diferentes. Además, el procesador de nodo de comunicación puede reasignar el dominio de contajes de NAS en el bloque 1817 (por ejemplo, usando el módulo 1857 de reasignación). Tras la reasignación, una primera parte del dominio de contajes de NAS puede asignarse para mensajes de NAS comunicados a través de la primera conexión de NAS, una segunda parte del dominio de contajes de NAS puede asignarse para mensajes de NAS comunicados a través de la segunda conexión de NAS, y una tercera parte del dominio de contajes de NAS puede asignarse para mensajes de NAS comunicados a través de la tercera conexión de NAS, siendo la primera, segunda y tercera partes del dominio de contajes de NAS mutuamente excluyentes.

Continuando con el ejemplo anterior, si el valor de NAS Count Max es 18, la reasignación puede ocurrir para los valores de NAS Count superiores a 14, por lo que los valores de NAS Count 7, 9, 11 y 13 no se utilizan. Según dicho ejemplo, después de la reasignación, la primera parte del dominio de contajes de NAS puede incluir valores de contaje de NAS mayores de 14 que son divisibles por 3 (por ejemplo, 15, 18, 21, 24, etc.), la segunda parte del dominio de contajes de NAS puede incluir valores de contaje 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 parte del dominio de contajes de NAS puede incluir valores de contaje de NAS mayores de 14 para los cuales la división por 3 proporciona un resto de 2 (por ejemplo, 17, 20, 23, 26, etc.).

Para una comunicación de 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 el valor de contaje de NAS más bajo de la primera parte del Dominio de contajes de NAS que no se ha utilizado previamente para cada mensaje de NAS comunicado a través de la primera conexión de NAS (p. ej., utilizando el primer módulo 1861 de comunicación de NAS). El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la segunda conexión de NAS en el bloque 1833 utilizando el valor de contaje de NAS más bajo de la segunda parte del dominio de contajes de NAS que no se ha utilizado previamente para cada mensaje de NAS comunicado a través de la segunda conexión de NAS (p. ej., utilizando el segundo módulo 1863 de comunicación de NAS). El procesador de nodo de comunicación puede comunicar mensajes de NAS a través de la tercera conexión de NAS en el bloque 1835 utilizando el valor de contaje de NAS más bajo de la tercera parte del dominio de contajes de NAS que no se ha utilizado previamente para cada mensaje de NAS comunicado a través de la tercera conexión de NAS (p. ej., utilizando el segundo módulo 1865 de comunicación de NAS).

Según 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 de contajes de NAS puede ser un dominio de contajes de NAS de enlace ascendente. Por consiguiente, la comunicación de 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 la comunicación de 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.

Según 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 de contajes de NAS puede ser un dominio de contajes de NAS de enlace descendente. Por consiguiente, la comunicación de mensajes de NAS a través de la primera conexión de NAS puede incluir transmitir mensajes de NAS a través de la primera conexión de NAS, y la comunicación de 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.

Según 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 de contajes de NAS es un dominio de contajes de NAS de enlace ascendente. Por consiguiente, la comunicación de mensajes de NAS a través de la primera conexión de NAS puede incluir transmitir mensajes de NAS a través de la primera conexión de NAS, y la comunicación de 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.

Según 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 de contajes de NAS puede ser un dominio de contajes de NAS de enlace descendente. Por consiguiente, la comunicación de 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 la comunicación de 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 realizaciones de la Figura 18A, la primera conexión de NAS puede proporcionarse a través de un nodo de acceso del 3GPP entre el primer y el segundo nodos de comunicación y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso que no sea del 3GPP entre el primer y el segundo nodos de comunicación, o la primera conexión de NAS puede proporcionarse a través de un nodo de acceso que no sea del 3GPP entre el primer y el

segundo nodos de comunicación y la segunda conexión de NAS puede proporcionarse a través de un nodo de acceso del 3GPP entre el primer y el segundo nodos de comunicación.

Además, la comunicación de mensajes de NAS a través de la primera conexión de NAS puede incluir al menos una de llevar a cabo una protección de integridad mediante la generación de códigos de autenticación de mensaje utilizando valores de contaje de NAS respectivos de la primera parte del dominio de contajes de NAS y/o llevar a cabo una protección de confidencialidad utilizando valores de contaje de NAS respectivos de la primera parte del dominio de contajes de NAS. De manera similar, la comunicación de mensajes de NAS a través de la segunda conexión de NAS puede incluir al menos una de llevar a cabo una protección de integridad mediante la generación de códigos de autenticación de mensaje utilizando valores de contaje de NAS respectivos de la segunda parte del dominio de contajes de NAS y/o llevar a cabo una protección de confidencialidad utilizando valores de contaje de NAS respectivos de la segunda parte del dominio de contajes de NAS.

Además, la primera y la segunda conexiones de NAS de la Figura 18A pueden mantenerse simultáneamente entre el primer y el segundo nodos de comunicación. Además, se puede establecer una sesión de Unidades de Datos por Paquetes (PDU) sobre la base del primer y el segundo mensajes de NAS para comunicar datos del plano de usuario entre el primer y el segundo nodos 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 de ejemplo 1 (que se expone más adelante), 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.

Según algunas otras realizaciones de conceptos inventivos, puede proporcionarse separación criptográfica en el nivel de las claves. En sistemas heredados pueden derivarse claves de protección de NAS como se describe en la TS 33.401 (a la que se denomina también referencia [2]).

En general, todas las derivaciones de claves (incluida la codificación de parámetros de entrada) para el LTE se pueden realizar utilizando la función de derivación de clave (KDF) especificada en la TS 33.220 (a la que se denomina también 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, al que también se denomina 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: $S = FC || P_0 || L_0 || P_1 || L_1 || P_2 || L_2 || P_3 || L_3 || \dots || P_n || L_n$, donde P_i (i de 0 a n) es un parámetro y L_i es su longitud en octetos.

De acuerdo con la cláusula A.7 de la TS 33.401 (a la que se denomina también referencia [2]), cuando se derivan claves para procesos (también denominados algoritmos) de integridad de NAS y de cifrado de NAS a partir de la KASME y los IDs y tipos de proceso/algoritmo, pueden/deberán usarse los siguientes parámetros 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 del proceso
- L1 = longitud de la identidad del proceso (es decir, 0x00 0x01)

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

La identidad del proceso (como se especifica en la cláusula 5 de la TS 33.401, a la que se denomina también 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 un uso futuro, y los dos bits más significativos del cuarteto más significativo pueden reservarse para un uso privado. La totalidad de los cuatro bits más significativos pueden/deberán fijarse a todos ceros.

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

Como se ha descrito anteriormente con respecto a las Figuras 10A-B, 11A-B, 12A-B y 13A-B, el Identificador de Conexión de NAS NAS CONN ID puede usarse en los procesos de autenticación y/o cifrado/descifrado para proporcionar separación para diferentes conexiones de NAS utilizadas por un mismo terminal inalámbrico.

Según algunas realizaciones, el NAS CONN ID puede usarse en la derivación de las claves de protección de 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 utilizadas 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 el NAS CONN ID y su longitud L2 sería cualquier longitud que tenga el NAS CONN ID (en octetos). Por ejemplo, si el NAS CONN ID tiene una longitud de 8 bits, entonces L2 es 1 (de un octeto). Si se especifica que el NAS CONN ID tiene un valor de longitud de 32 bits, entonces L2 se fijaría a la constante 4 (de cuatro octetos). Todos los demás parámetros (P0, P1) pueden permanecer iguales o pueden basarse en los equivalentes del 5G.

La Figura 15 ilustra la Derivación de claves basada en la cadena S donde el NAS CONN ID se usa en la derivación de la cadena S. Aquí, la clave maestra KAMF y S se proporcionan como entradas para la función de derivación de clave KDF con el fin de generar la KEY K que se utiliza para la autenticación de EIA y/o el cifrado/descifrado de EEA. En la Figura 15:

- KAMF es el equivalente de KASME en el 5G;
- S se construye como la concatenación FC||P0||L0||P1||L1||P2||L2 donde:

- FC es potencialmente un diferenciador nuevo para la derivación de la clave de protección de NAS,
- P0, P1, L0 y L1 se basan en parámetros potencialmente nuevos y valores equivalentes a los utilizados en el LTE. De hecho, los algoritmos en el 5G potencialmente podrían tener otros nombres y otros valores de diferenciador de tipo, etc.
- P2 y L2 son los nuevos parámetros basados en el NAS CONN ID.

Dependiendo del valor de FC, se utiliza el mismo procedimiento para derivar una clave de protección de integridad de NAS ó una clave de cifrado de NAS. Dado que el NAS CONN ID se utiliza en la función de derivación, esas claves serían entonces específicas de la conexión de NAS.

Según algunas otras realizaciones, el NAS CONN ID puede usarse para derivar una clave KNAS de nivel nuevo a partir de la clave KAMF que a continuación se usa para derivar las otras claves de protección de nivel inferior. Por tanto, la KNAS y las claves de protección derivadas pueden ser específicas de la conexión de NAS.

Por ejemplo, una nueva clave llamada KNAS puede derivarse a partir de la KAMF como se muestra en la Figura 16, donde S se fija a FC||P0||L0, teniendo FC un nuevo valor y correspondiéndose P0, L0 con el NAS CONN ID. De hecho, P0 y L0 se definen de manera similar a P2 y L2 como se ha descrito anteriormente con respecto a la Figura 15. Debido a que el NAS CONN ID se usa en la derivación de esta nueva clave intermedia, la misma es por lo tanto específica de la conexión de NAS. Todo lo que se derive posteriormente de la clave KNAS sería también específico de la conexión de NAS. Por lo tanto, se propone derivar la clave de protección de NAS KNASint y KNASenc a partir de la KNAS de manera similar a como se hace en sistemas heredados cuando estas se derivan de la KASME.

Por tanto, el esquema general de derivación de claves que produce las claves de protección de NAS puede proporcionarse como se ilustra en la Figura 16. En realizaciones en las que se proporciona derivación de claves basadas en el NAS CONN ID, se puede usar/necesitar un mayor número de parámetros específicos de la conexión en comparación con realizaciones analizadas anteriormente con respecto a las Figuras 10A-B, 11A-B, 12A-B y 13A-B.

En la descripción anterior de varias realizaciones de los presentes conceptos inventivos, debe entenderse que la terminología utilizada en este documento tiene el propósito de describir realizaciones particulares únicamente y no pretende ser limitativa de los presentes conceptos inventivos. A menos que se defina de otro modo, todos los términos (incluidos términos técnicos y científicos) usados en este documento tienen el mismo significado que el comúnmente entendido por un experto en la técnica a la que pertenecen los presentes conceptos inventivos. Se entenderá además que los términos, como los definidos en diccionarios de uso común, deben interpretarse como si tuvieran un significado que sea consistente con su significado en el contexto de esta memoria descriptiva y la técnica relevante y no se interpretarán en un sentido idealizado o excesivamente formal a menos que se defina así expresamente en este documento.

Cuando se hace referencia a un elemento como "conectado", "acoplado", "sensible" o variantes de estos con respecto a otro elemento, el mismo puede conectarse, acoplarse o ser sensible directamente al otro elemento o pueden estar presentes elementos intermedios. Por el contrario, cuando se hace referencia a un elemento como "directamente conectado", "directamente acoplado", "directamente sensible" o variantes de estos con respecto a otro elemento, no hay elementos intermedios presentes. Los números iguales se refieren a elementos iguales en todas partes. Además, "acoplado", "conectado", "sensible" o variantes de los mismos, según se usan en este documento, pueden incluir acoplado, conectado o sensible de forma inalámbrica. Como se usa en este documento, las formas singulares "un", "una" y "el/la" pretenden incluir las formas plurales también, a menos que el contexto indique claramente lo contrario. Es posible que las funciones o construcciones ampliamente conocidas no se describan en detalle por motivos 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 la presente para describir varios elementos/operaciones, estos elementos/operaciones no deberían estar limitados por estos términos. Estos términos solo se utilizan para distinguir un elemento/operación de otro elemento/operación. Por tanto, un primer elemento/operación en algunas realizaciones podría denominarse segundo elemento/operación en otras realizaciones sin desviarse de las enseñanzas de los presentes conceptos inventivos. Los números de referencia iguales o los indicadores de referencia iguales señalan elementos iguales o similares en toda la memoria descriptiva.

Según se usan en el presente documento, los términos "comprender", "comprendiendo", "comprende", "incluir", "incluyendo", "incluye", "tener", "tiene", "teniendo", o variantes de los mismos son de interpretación abierta, e incluyen una o más características, números enteros, elementos, pasos, componentes o funciones indicados, pero no excluye la presencia o adición de otra u otras características, números enteros, elementos, pasos, componentes, funciones o grupos de los mismos. Además, como se usa en este documento, la abreviatura común "e.g." ["p. ej." en español], que se deriva de la expresión latina "exempli gratia", puede usarse para introducir o especificar un ejemplo o ejemplos generales de un elemento mencionado anteriormente, y no pretende ser limitativa de tal artículo. La abreviatura común "i.e." ["es decir" en español], que se deriva de la expresión latina "id est", puede usarse para especificar un elemento particular de una relación de elementos más general.

En este documento se describen realizaciones de ejemplo con referencia a diagramas de bloques y/o ilustraciones de diagramas de flujo de métodos implementados por ordenador, aparatos (sistemas y/o dispositivos) y/o productos de programa de ordenador. 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 de ordenador que son ejecutadas por uno o más circuitos de ordenador. Estas instrucciones de programa de ordenador se pueden proporcionar a un circuito de procesador de un circuito de ordenador de propósito general, circuito de ordenador de propósito especial y/u otro circuito de procesamiento de datos programable para crear una máquina, de modo que las instrucciones, que se ejecutan a través del procesador del ordenador y/u otros aparatos de procesamiento de datos programables, transforman y controlan transistores, valores almacenados en posiciones de memoria y otros componentes de *hardware* dentro de dicha circuitería para implementar las funciones/acciones especificadas en los diagramas de bloques y/o el bloque o bloques de los diagramas de flujo, y de ese modo crear medios (funcionalidad) y/o estructura para implementar las funciones/acciones especificadas en los diagramas de bloques y/o el(los) bloque(s) de los diagramas de flujo.

Estas instrucciones de programa de ordenador también pueden almacenarse en un soporte tangible legible por ordenador que puede hacer que un ordenador u otro aparato de procesamiento de datos programable funcione de una manera particular, de modo que las instrucciones almacenadas en el soporte legible por ordenador creen un artículo de fabricación que incluye instrucciones que implementan las funciones/acciones especificadas en los diagramas de bloques y/o bloque o bloques de los diagramas de flujo. En consecuencia, las realizaciones de los conceptos de la presente invención pueden incorporarse en *hardware* y/o en *software* (incluido *firmware*, *software* residente, microcódigo, etc.) que se ejecuta en un procesador, como un procesador de señal digital, que puede denominarse en conjunto "circuitería", "un módulo" o variantes de los mismos.

También debe tenerse en cuenta que en algunas implementaciones alternativas, las funciones/acciones señaladas en los bloques pueden producirse en otro orden al señalado 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 en ocasiones en el orden inverso, dependiendo de la funcionalidad/acciones involucradas. Además, la funcionalidad de un bloque dado de los diagramas de flujo y/o diagramas de bloques puede separarse en múltiples bloques y/o la funcionalidad de dos o más bloques de los diagramas de flujo y/o diagramas de bloques puede integrarse al menos parcialmente. Finalmente, se pueden añadir/insertar otros bloques entre los bloques que se ilustran, y/o se pueden omitir bloques/operaciones sin desviarse del alcance de los conceptos inventivos. Además, aunque algunos de los diagramas incluyen flechas en las rutas de comunicación para mostrar una dirección principal de comunicación, debe entenderse que la comunicación puede producirse en la dirección opuesta a las flechas representadas.

Se pueden aplicar muchas variaciones y modificaciones en las realizaciones sin desviarse sustancialmente de los principios de los presentes conceptos inventivos. Se pretende que todas estas variaciones y modificaciones se incluyan en el presente documento dentro del alcance de los presentes conceptos inventivos. Por consiguiente, la materia en cuestión dada a conocer anteriormente debe considerarse ilustrativa, y no restrictiva, y los ejemplos de realizaciones pretenden cubrir todas esas modificaciones, mejoras y otras realizaciones, que se sitúan dentro del espíritu y alcance de los presentes conceptos inventivos. Por lo tanto, en la máxima medida permitida por la ley, el alcance de los presentes conceptos inventivos se determinará mediante la interpretación más amplia permisible de la presente divulgación, incluidas las siguientes reivindicaciones, y no estará restringido o limitado por la descripción detallada anterior.

Se exponen a continuación abreviaturas mencionadas anteriormente.

Abreviatura	Explicación
AMF	Función de Gestión de Acceso
CM	Gestión de Conexión
5 ID CONN	Identificación de Conexión
EEA	Algoritmo de Cifrado de EPS
EIA	Algoritmo de Integridad de EPS
eKSI	Identificador de Conjunto de Claves en E-UTRAN
EMM	Gestión de Movilidad de EPS
10 EPC	Red Central por Paquetes Evolucionada
EPS	Sistema por Paquetes Evolucionado
IE	Elemento de información
KAMF	Clave específica de AMS
KASME	Clave de Entrada de Gestión de Seguridad de Acceso
15 KDF	Función de Derivación de Clave
KNAS	Clave de protección de NAS
KNASenc	Cifrado de KNAS
KNASint	Integridad de KNAS
LTE	Evolución a Largo Plazo
20 MAC	Código de Autenticación de Mensaje
NAS	Estrato de Acceso a la Red
PDU	Unidad de Datos por Paquetes
SMC	Orden de Modo de Seguridad
SN	Número de secuencia
25 UE	Equipo de Usuario
3GPP	Proyecto de Asociación de 3ª Generación
5G	5ª Generación

Las referencias mencionadas anteriormente se identifican a continuación.

30	Ref. [1]	3GPP TS 23.501 V0.4.0 (2017-04), Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Etapa 2 (versión 15)
	Ref. [2]	3GPP TS 33.401 V14.2.0 (2017-03), Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture; (versión 14)
	Ref. [3]	3GPP TS 24.301 V14.3.0 (2017-03), Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Etapa 3 (versión 14)
35	Ref. [4]	3GPP TS 33.220 V14.0.0 (2016-12), Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (versión 14)
	Ref. [5]	Krawczyk, et al., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, febrero de 1997

REIVINDICACIONES

1. Un método en un primer nodo de comunicación que proporciona comunicación de mensajes de Estrato de Acceso a la Red, NAS, con un segundo nodo de comunicación de una red de comunicación inalámbrica, comprendiendo el método:

5 comunicar (1717) un primer mensaje de NAS entre el primer nodo de comunicación y el segundo nodo de comunicación a través de una primera conexión de NAS, en donde la comunicación del primer mensaje de NAS comprende llevar a cabo una protección de integridad para el primer mensaje de NAS utilizando una primera identificación de conexión de NAS; y llevar a cabo la protección de integridad para el primer mensaje de NAS generando un primer código de autenticación de mensaje basado en la primera identificación de conexión de NAS, una clave maestra de un contexto de seguridad de NAS 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;

10 comunicar (1719) un segundo mensaje de NAS entre el primer nodo de comunicación y el segundo nodo de comunicación a través de una segunda conexión de NAS, en donde la comunicación del segundo mensaje de NAS comprende llevar a cabo una protección de integridad para el segundo mensaje de NAS usando una segunda identificación de conexión de NAS, en donde la primera y segundas conexiones de NAS son diferentes y comparten la clave maestra, y llevar a cabo la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basado 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 entrada para generar el primer código de autenticación de mensaje, y en el que la segunda identificación de conexión de NAS se proporciona como entrada para generar el segundo código de autenticación de mensaje.

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

30 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 del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso que no es del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación, o en el que la primera conexión de NAS se proporciona a través de un nodo de acceso que no es del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación.

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

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

7. El método de cualquiera de las reivindicaciones 1 a 6, método que comprende además:

establecer una sesión de Unidades de Datos por Paquetes, PDU, basada en el primer y segundo mensajes de NAS para comunicar datos del plano de usuario entre el terminal inalámbrico y el nodo de red.

45 8. Un primer nodo de comunicación adaptado para proporcionar comunicación de mensajes de Estrato de Acceso a la Red, NAS, con un segundo nodo de comunicación de una red de comunicación inalámbrica, en donde la primera y segunda conexiones de NAS entre el primer nodo de comunicación y el segundo nodo de comunicación comparten una clave maestra de un contexto de seguridad de NAS, y en donde el primer nodo de comunicación está adaptado para:

50 comunicar un primer mensaje de NAS entre el primer nodo de comunicación y el segundo nodo de comunicación a través de la primera conexión de NAS, en donde la comunicación del primer mensaje de NAS comprende llevar a cabo una protección de integridad para el primer mensaje de NAS utilizando la primera identificación de conexión de NAS; y llevar a cabo la protección de integridad para el primer mensaje de NAS generando un primer código de autenticación de mensaje basado 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;

- 5 comunicar un segundo mensaje de NAS entre el primer nodo de comunicación y el segundo nodo de comunicación a través de la segunda conexión de NAS, en donde la comunicación del segundo mensaje de NAS comprende llevar a cabo una protección de integridad para el segundo mensaje de NAS utilizando una segunda identificación de conexión de NAS, y llevar a cabo la protección de integridad para el segundo mensaje de NAS generando un segundo código de autenticación de mensaje basado 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 9. El primer nodo de comunicación de la reivindicación 8, en el que la primera identificación de conexión de NAS se proporciona como entrada para generar el primer código de autenticación de mensaje, y en el que la segunda identificación de conexión de NAS se proporciona como entrada para generar el segundo código de autenticación de mensaje.
- 15 10. El primer nodo de comunicación de cualquiera de las reivindicaciones 8 a 9, en el que la aplicación de la protección de integridad para el primer mensaje de NAS comprende llevar a cabo una protección de integridad para el primer mensaje de NAS utilizando una interfaz de protección de integridad de EIA compatible con el 5G, y en el que la aplicación de la protección de integridad para el segundo mensaje de NAS comprende llevar a cabo una protección de integridad para el segundo mensaje de NAS utilizando la interfaz de protección de integridad de EIA compatible con el 5G.
- 20 11. El primer nodo de comunicación de cualquiera de las reivindicaciones 8 a 10, en el que la primera conexión de NAS se proporciona a través de un nodo de acceso del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso que no es del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación, o en el que la primera conexión de NAS se proporciona a través de un nodo de acceso que no es del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación y la segunda conexión de NAS se proporciona a través de un nodo de acceso del 3GPP entre el primer nodo de comunicación y el segundo nodo de comunicación.
- 25 12. El primer nodo de comunicación de la reivindicación 11, en el que el nodo de acceso del 3GPP comprende una estación base de red de acceso por radiocomunicaciones, y en el que el nodo de acceso que no es del 3GPP comprende al menos uno de un nodo de acceso de WiFi y/o un nodo de acceso satelital.
- 30 13. El primer nodo de comunicación de cualquiera de las reivindicaciones 8 a 12, en el que la primera y la segunda conexiones de NAS se mantienen simultáneamente entre el primer nodo de comunicación y el segundo nodo de comunicación.
14. El primer nodo de comunicación de cualquiera de las reivindicaciones 8 a 13, en el que el primer nodo de comunicación está además adaptado para:
- 35 establecer una sesión de Unidades de Datos por Paquetes, PDU, basada en el primer y segundo mensajes de NAS para comunicar datos del plano de usuario entre el primer nodo de comunicación y el segundo nodo de comunicación.

Figura 1

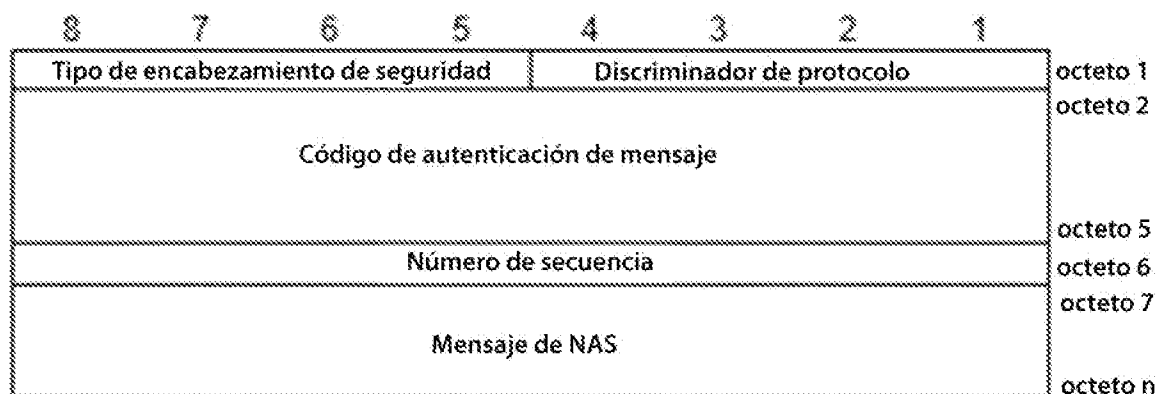


Figura 2

Tipo de encabezamiento de seguridad (octeto 1)				
8	7	6	5	
0	0	0	0	Mensaje de NAS en claro, sin protección en cuanto a seguridad
Mensaje de NAS protegido en cuanto a seguridad:				
0	0	0	1	Protegido en cuanto a integridad
0	0	1	0	Protegido en cuanto a integridad y cifrado
0	0	1	1	Protegido en integ. con nuevo contexto de segur. EPS (NOTA 1)
0	1	0	0	Protegido en integ. y cifrado con nuevo cont. de seg. EPS (NOTA 2)
0	1	0	1	Mensaje NAS trotegido en integ. y cifrado parcialmente (NOTA 4)
Mensaje de L3 no estándar:				
1	1	0	0	Encabezamiento de seguridad para el mensaje SERVICE REQUEST
1	1	0	1	Estos valores no se usan en esta versión del protocolo. Si se reciben se interpretarán como "1100". (NOTA 3)
1	1	1	1	

La totalidad del resto de valores está reservada.

Figura 3A

Deriv. de Seguridad de MAC-I/NAS-MAC (Remitente)

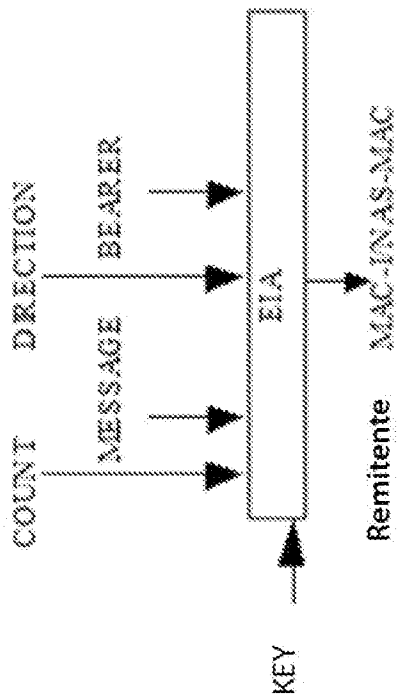


Figura 3B

Deriv. de Seguridad de XMAC-I/XNAS-MAC (Receptor)

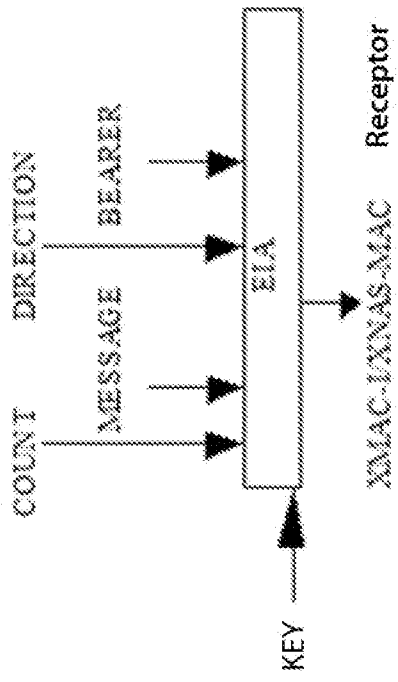


Figura 4A

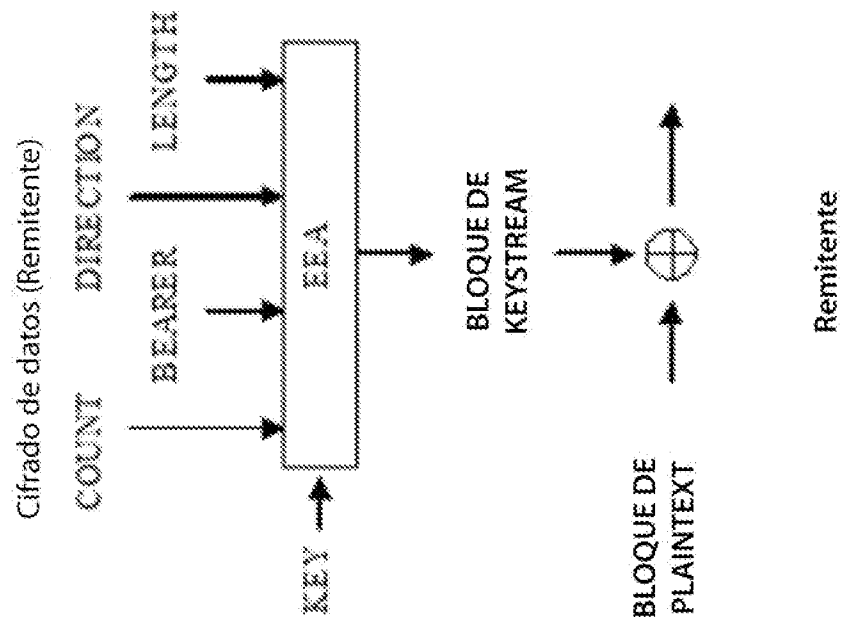


Figura 4B

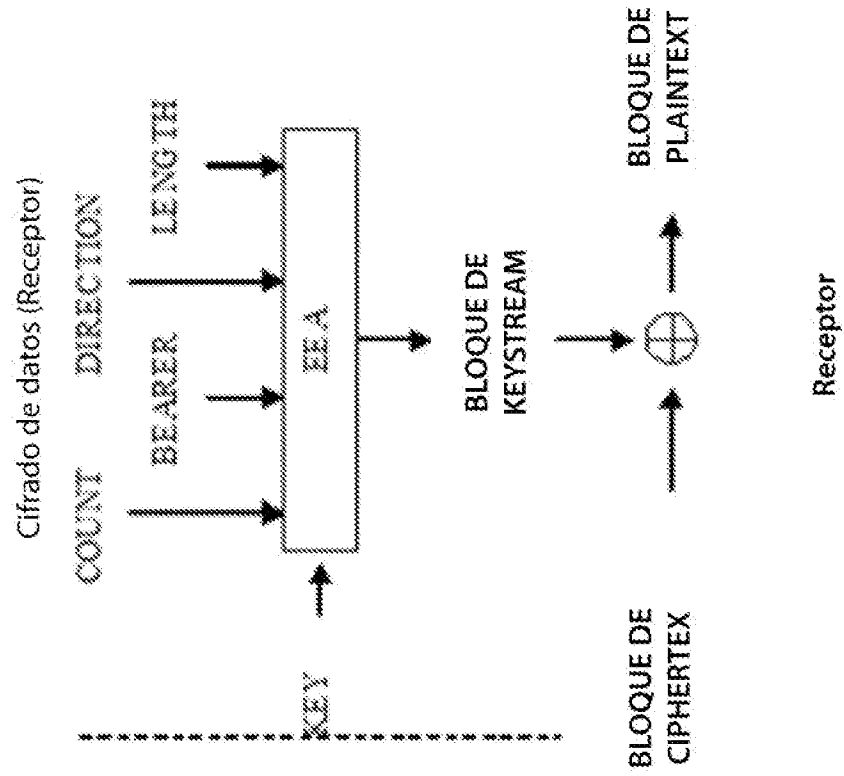


Figura 5

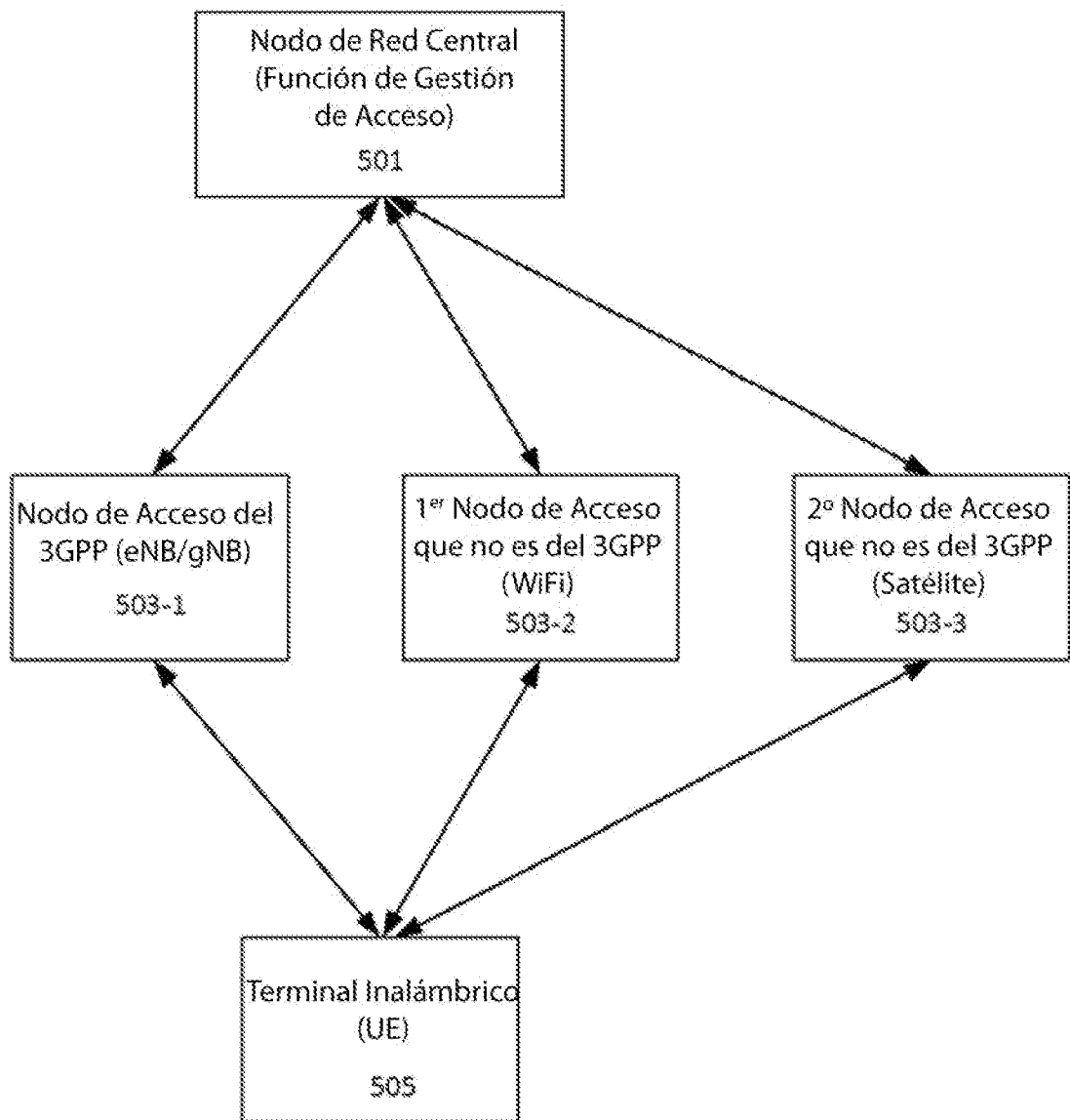


Figura 6

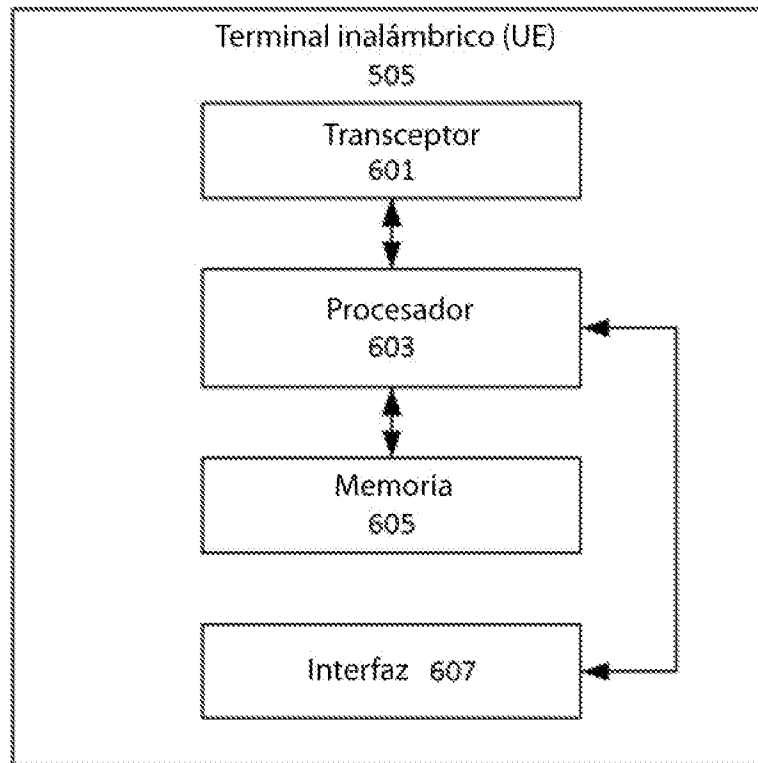


Figura 7

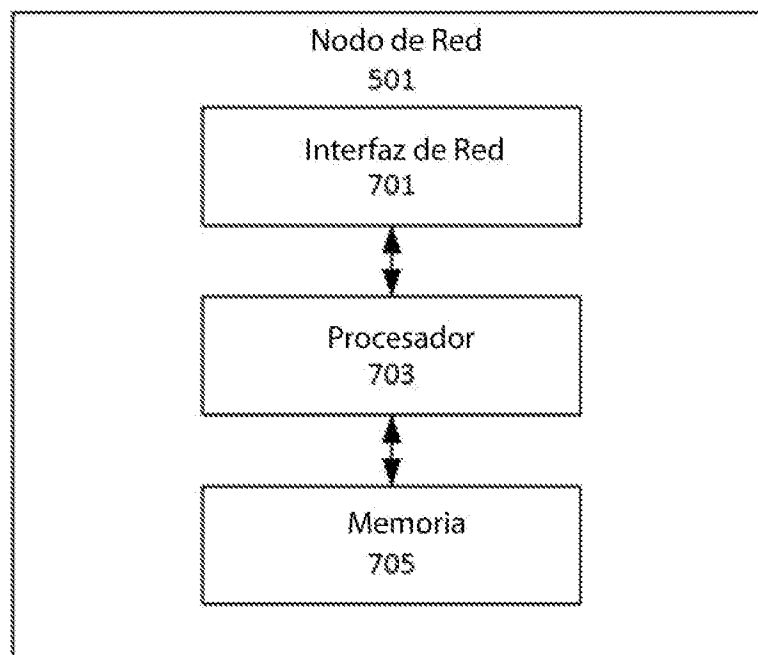


Figura 8

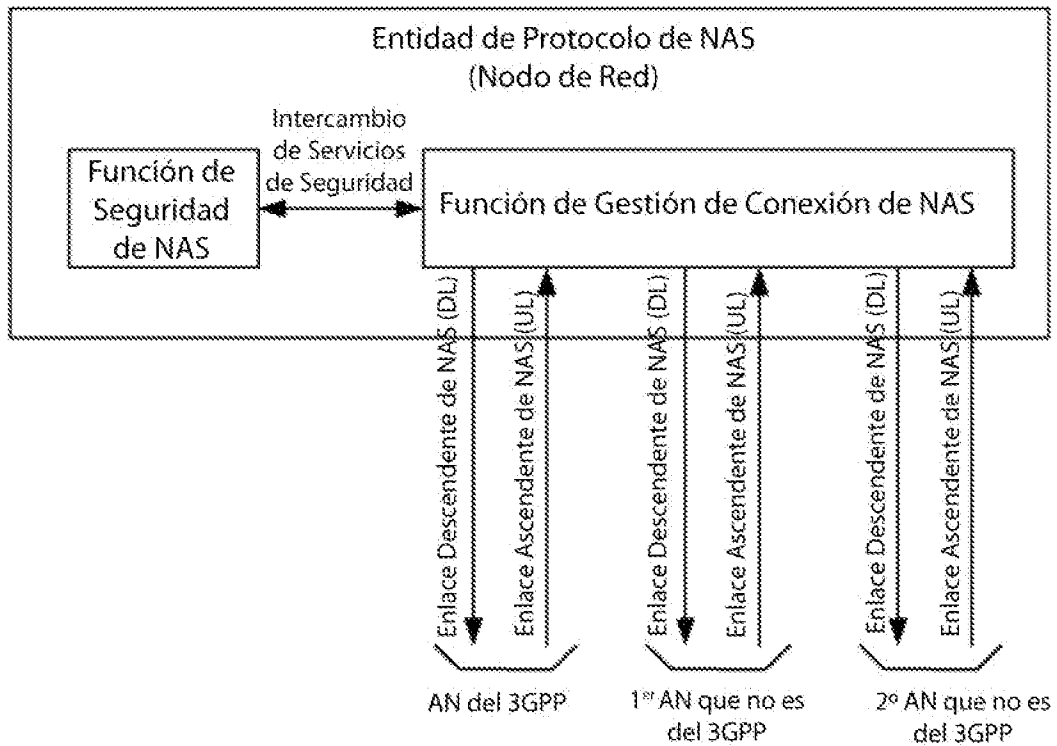


Figura 9

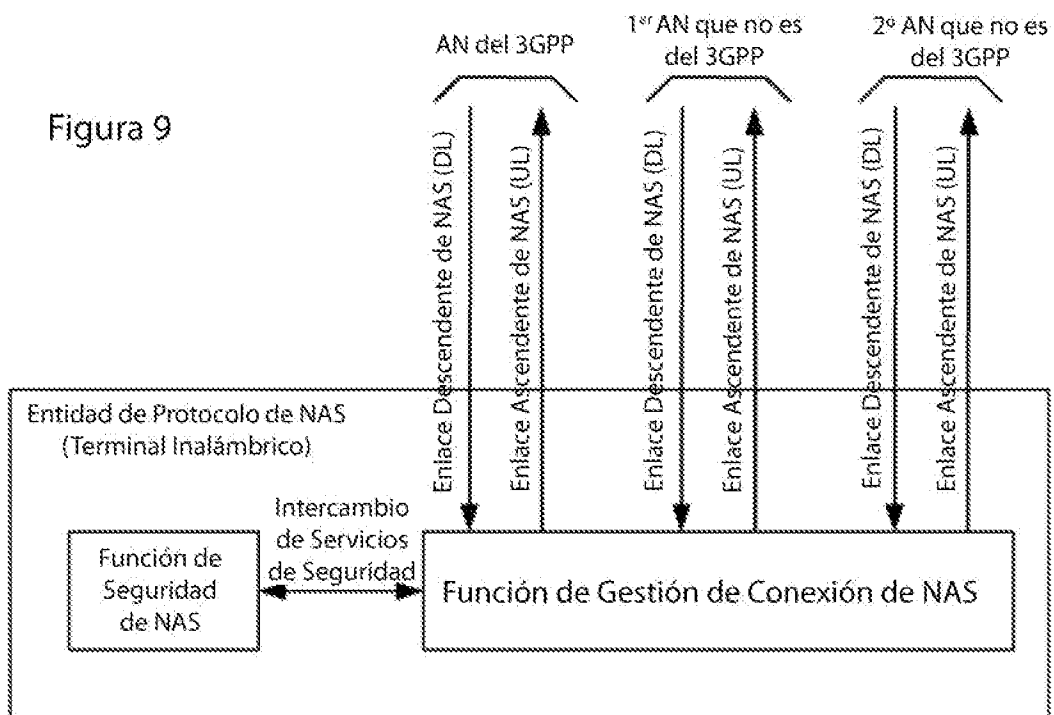


Figura 10A

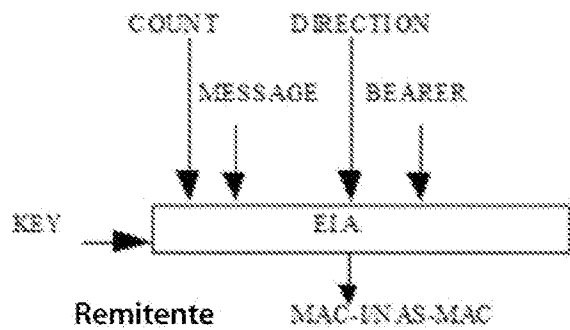


Figura 10B

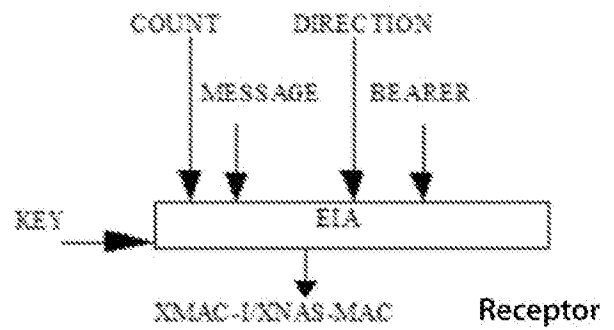


Figura 11A

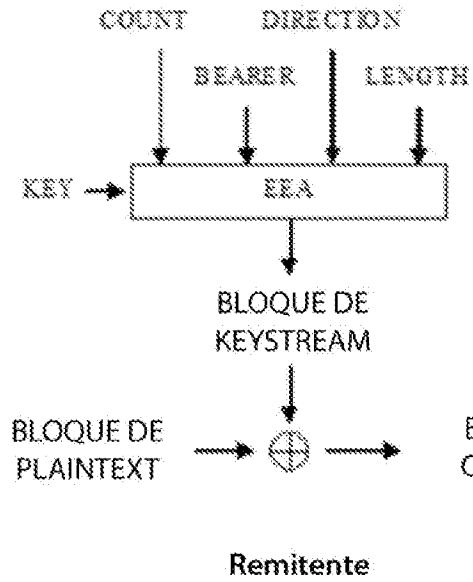


Figura 11B

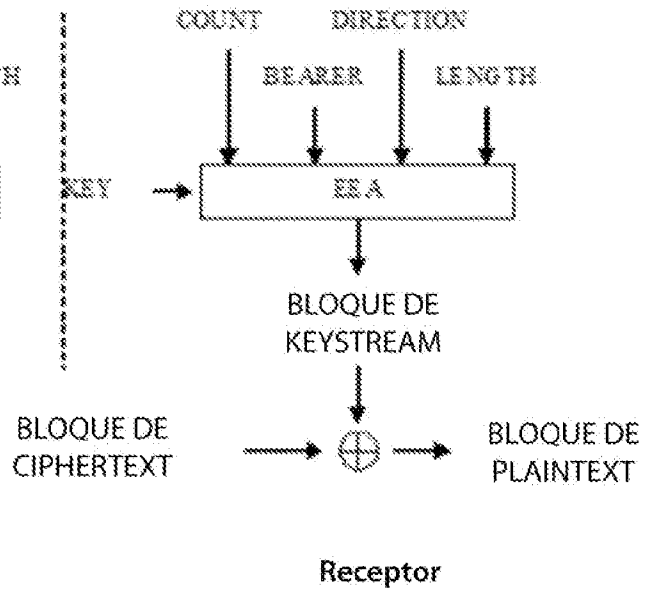


Figura 12A

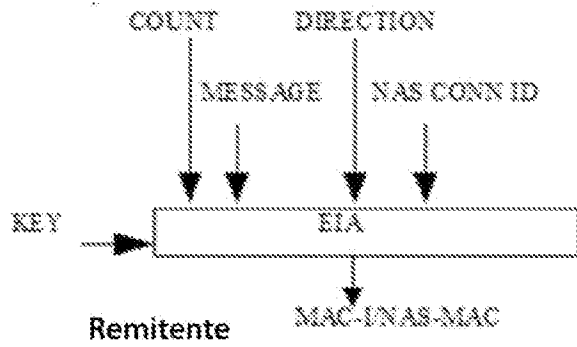


Figura 12B

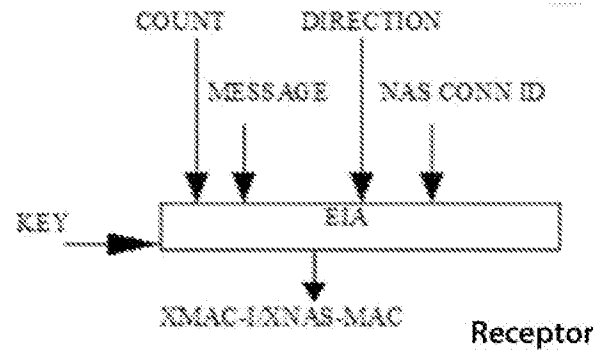


Figura 13A

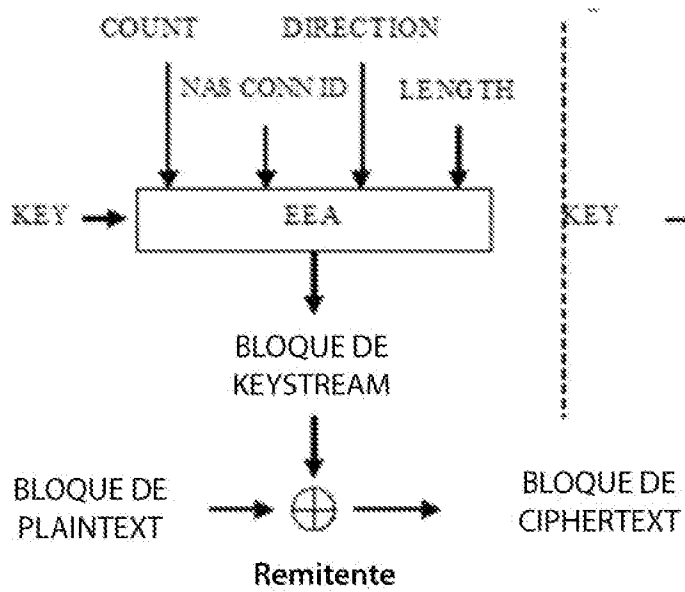


Figura 13B

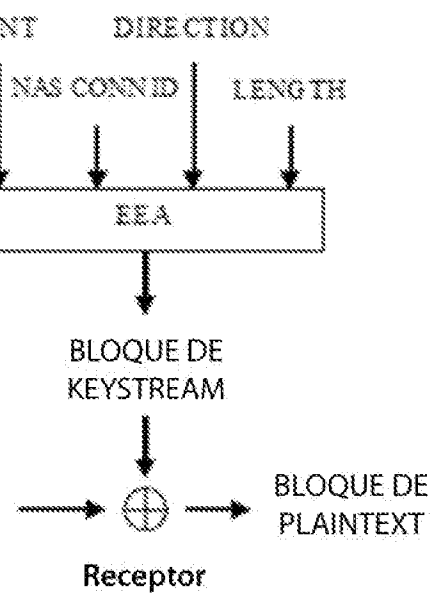


Figura 14

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

Figura 15

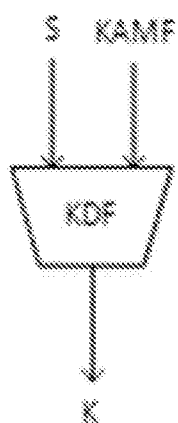


Figura 16

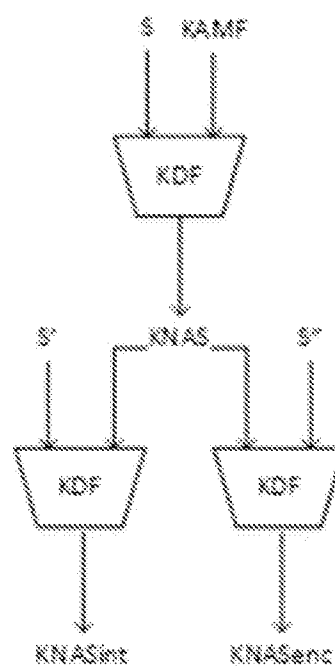


Figura 17A

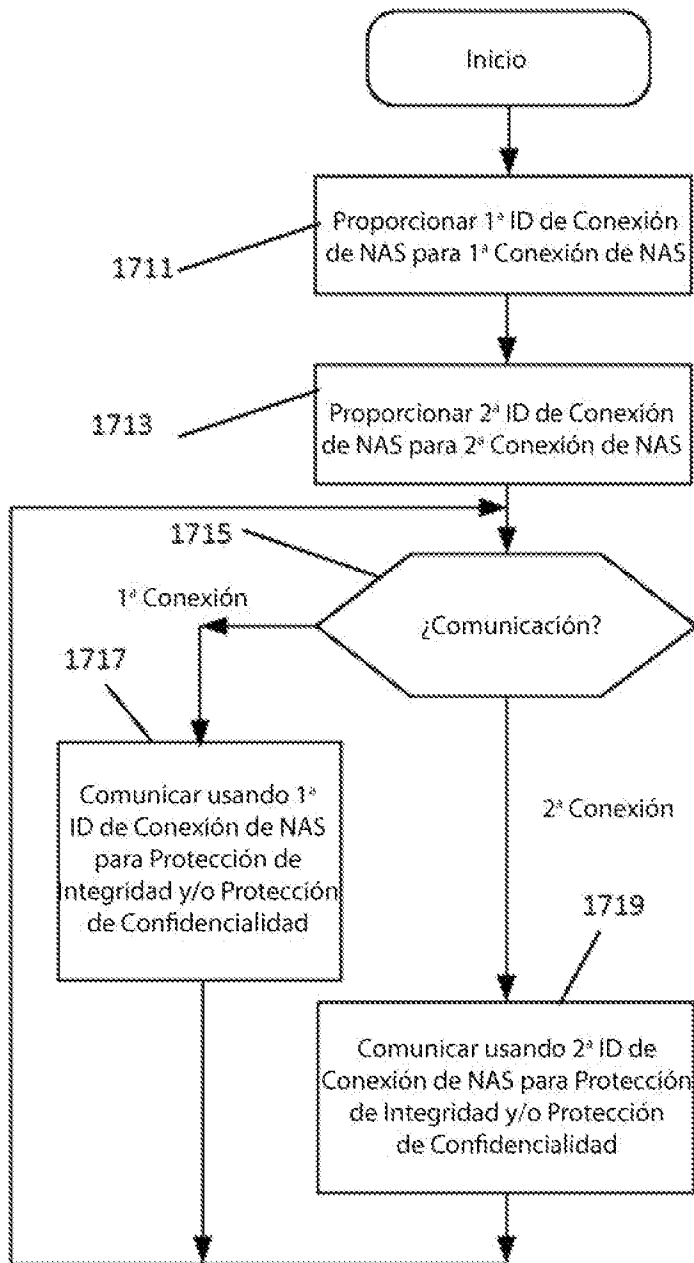


Figura 17B

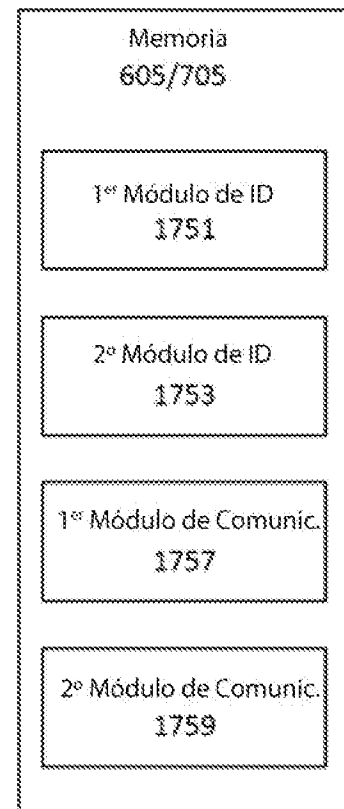


Figura 18A

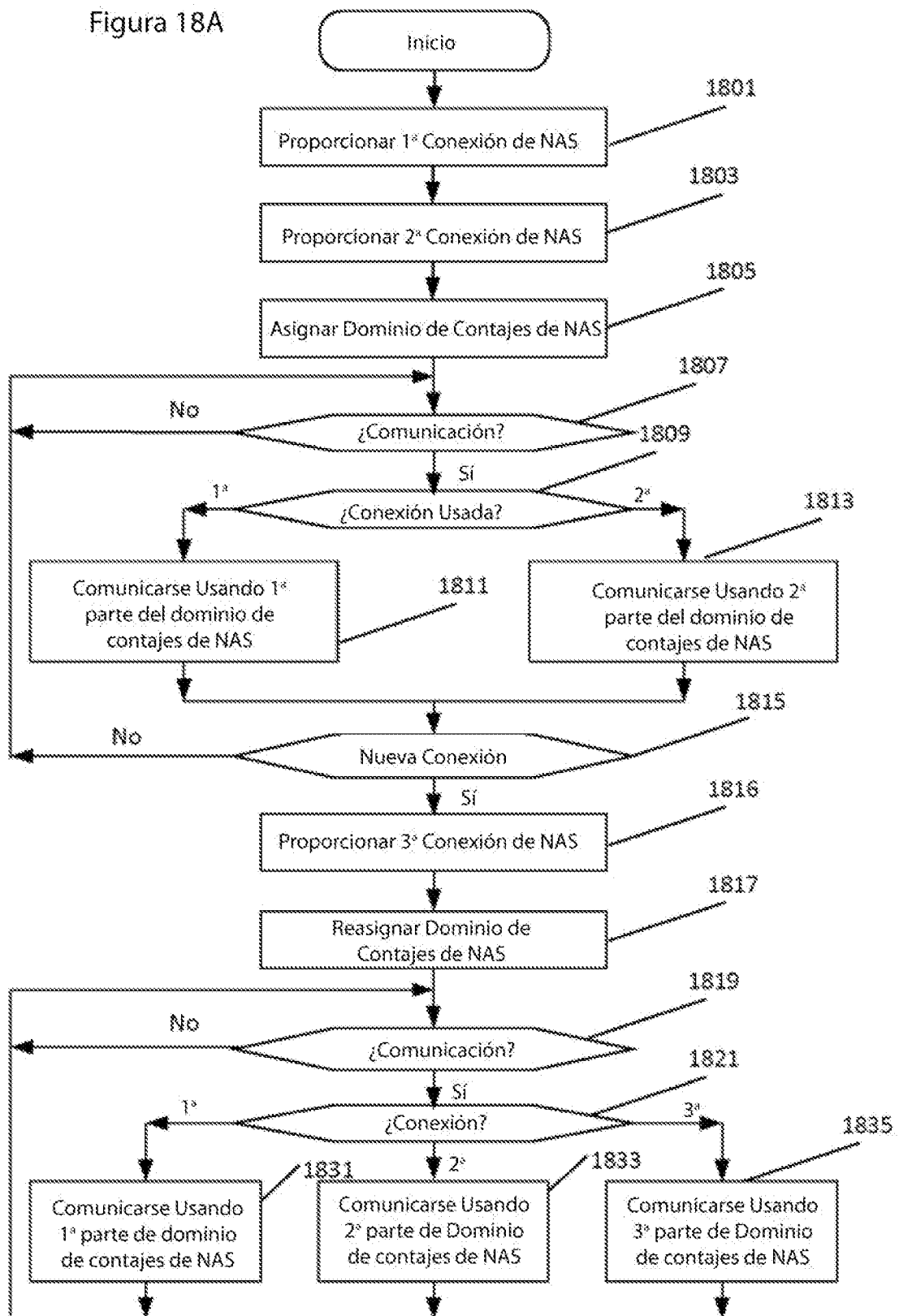


Figura 18B

