(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 906 127**

(51) Int. CI.:

H04W 12/041 (2011.01)
H04W 92/10 (2009.01)
H04W 8/20 (2009.01)
H04W 12/0471 (2011.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.05.2008 E 19183523 (0)**

(97) Fecha y número de publicación de la concesión europea: **08.12.2021 EP 3598690**

(54) Título: **Método y disposición en un sistema de telecomunicaciones**

(30) Prioridad:

17.09.2007 US 97295507 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.04.2022

(73) Titular/es:

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

(72) Inventor/es:

BLOM, ROLF;
MILDH, GUNNAR y
NORRMAN, KARL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y disposición en un sistema de telecomunicaciones

Campo técnico

La presente invención se refiere a métodos y dispositivos en un sistema de telecomunicaciones, y en particular a una solución de seguridad en el EPS (Sistema de Paquetes Evolucionado), es decir, la E-UTRAN (la Red de Acceso de Radiocomunicaciones Terrestre UMTS Evolucionada) y la EPC (red Central de Paquetes Evolucionada), para solicitudes de servicio activadas por un UE. Más específicamente, la presente invención se refiere a un método y una disposición en una MME (Entidad de Gestión de Movilidad) y en un UE (Equipo de Usuario) para un EPS (Sistema de Paquetes Evolucionado) para establecer una clave de seguridad con el fin de proteger el tráfico de RRC/UP.

Antecedentes

En la arquitectura del EPS, la autenticación del abonado se realiza entre un UE y una MME (Entidad de Gestión de Movilidad), y la MME gestiona, por ejemplo, la movilidad, las identidades de UE y los parámetros de seguridad. El fundamento para definir el procedimiento de seguridad en el EPS es una clave de seguridad, K_ASME, que es compartida entre la MME y el UE, y se establece en la autenticación del UE. Una entidad funcional de la arquitectura del EPS denominada ASME (Entidad de Gestión de Seguridad de Acceso) puede, por ejemplo, estar ubicada conjuntamente con la MME, y la ASME recibe y almacena la clave de seguridad K_ASME derivada de las claves CK/IK confinadas en la red doméstica. A partir de la clave de seguridad, K_ASME, la ASME obtiene un contexto de seguridad NAS usado para proteger la señalización NAS, es decir, la señalización de Estrato Sin Acceso entre la MME de la red Central de Paquetes Evolucionada (EPC) y un UE. El contexto de seguridad NAS contiene parámetros para el cifrado y la protección de integridad de la señalización NAS, tales como K_NAS_enc, K_NAS_int, así como números de secuencias de enlace ascendente y enlace descendente, NAS_U_SEQ y NAS_D_SEQ, y los números de secuencia se usan para evitar la repetición de mensajes antiguos, y también como entradas en los procedimientos de cifrado y de protección de integridad. La ASME proporciona a la MME el contexto de seguridad NAS, y en la MME se mantiene un contexto de seguridad NAS, y en el UE se mantiene un contexto de seguridad NAS correspondiente, y la protección de repetición, la protección de integridad y el cifrado se basan en que los números de secuencia de los contextos de seguridad NAS de la MME y el UE no se reutilizan.

Preferentemente, el contexto de seguridad para la protección del tráfico de UP/RRC entre un UE y el NodoBe (es decir, una estación de base de radio en una arquitectura de EPS) de servicio se basa también en dicha clave de seguridad, K_ASME. El procedimiento para establecer el contexto de seguridad UP/RRC conlleva la obtención de una clave denominada K_eNB, a partir de la cual se obtiene la clave de cifrado K_eNB_UP_enc para proteger el UP (Plano de Usuario), es decir, los datos de usuario final transferidos a través de la EPC y la E-UTRAN, así como la clave de cifrado, K_eNB_RRC_enc, y la clave de protección de integridad, K_eNB_RRC_int, para proteger el RRC (Control de Recursos de Radiocomunicaciones).

La figura 1 ilustra un flujo de señalización ejemplificativo convencional para una transición del estado INACTIVO al ACTIVO iniciada por un UE, en una arquitectura de EPS. Un UE INACTIVO es solamente conocido por la EPC (Red Central de Paquetes Evolucionada) del EPS, y no existe ningún contexto de seguridad UP/RRC entre el Nodo Be y el UE. Un UE en el estado ACTIVO es conocido tanto en la EPC como en la EUTRAN, y se ha establecido un contexto de seguridad UP/RRC para la protección del tráfico de UP/RRC entre el UE y su NodoBe.

La figura 1 ilustra un UE 11, un NodoBe 12, una MME 13, una GW (Pasarela) 14 de servicio, una Pasarela 15 de PDN, y el HSS (Servidor de Abonados Domésticos) 16. La Pasarela 14 de Servicio es el nodo de la EPC con el que acaba la interfaz hacia la EUTRAN, y la Pasarela de PDN es el nodo de la EPC con el que acaba la interfaz hacia una PDN (Red de Datos por Paquetes). Si un UE accede a múltiples PDNs, puede haber múltiples Pasarelas de PDN para ese UE. En la señal S1 y la señal S2, se reenvía de manera transparente la Solicitud de Servicio NAS desde el UE a la MME, y la Solicitud de Servicio NAS está protegida en cuanto a integridad basándose en el NAS_U_SEQ. En la señal opcional S3, el UE es autenticado por la MME y se establece la K_ASME, usando datos de abonado almacenados en el HSS (Servidor de Abonados Domésticos), y la MME envía la Solicitud de Establecimiento de Contexto Inicial al NodoBe, en S4. En las señales S5 y S6, el NodoBe establece el portador de radiocomunicaciones con el UE y reenvía datos de enlaces ascendente, y devuelve un mensaje de Establecimiento de Contexto Inicial Completo a la MME en la señal S7. En la señal S8, la MME envía una solicitud de actualización de portador a la GW de Servicio, y la GW de Servicio responde en la señal S9.

En soluciones anteriores, la obtención de la K_eNB por parte del UE y la MME para el contexto de seguridad RRC/UP se basa, por ejemplo, en un mensaje ACEPTACIÓN DE SERVICIO NAS u otra información explícita enviada desde la MME al UE. No obstante, tal como se ilustra en el flujo de señalización EPS convencional ejemplificativo de la figura 1, la MME normalmente no enviará ninguna ACEPTACIÓN DE SERVICIO NAS tras recibir una SOLICITUD DE SERVICIO NAS desde un UE en un EPS. Por lo tanto, no será posible obtener la K_eNB a partir de la información de un mensaje ACEPTACIÓN DE SERVICIO NAS.

Según una solución conocida ejemplificativa, la K_eNB es obtenida por la MME a partir de la K_ASME y el NAS_D_SEQ usados por la MME en el mensaje ACEPTACIÓN DE SERVICIO NAS, y el UE obtiene la misma K_eNB recuperando el número de secuencia, NAS_D_SEQ, a partir del mensaje ACEPTACIÓN DE SERVICIO NAS y realizando el mismo procedimiento de obtención de K_eNB que la MME. La MME transfiere la K_eNB al NodoBe cuando establece la conexión de S1 con el NodoBe. No obstante, un inconveniente con esta solución conocida es que si no se define ningún mensaje explícito de ACEPTACIÓN DE SERVICIO NAS desde la MME al UE, tal como en el flujo de señalización EPS convencional ejemplificativo de la figura 1, no es posible para el UE obtener la misma K_eNB que la MME. Aun cuando es técnicamente posible para el UE realizar una estimación de un número de secuencia de enlace descendente NAS actual, NAS_D_SEQ, esta estimación podría ser errónea, puesto que la MME puede haber enviado mensajes NAS que se perdieron y no fueron recibidos nunca por el UE. En tal caso, la MME haría que se actualizase su NAS_D_SEQ, sin que el UE tuviera conocimiento de la actualización, lo cual conduce a un NAS_D_SEQ erróneo en el UE.

Según otra solución conocida ejemplificativa, la obtención de la K_eNB se basa en un número de secuencia independiente mantenido específicamente para la obtención de la K_eNB, y este número de secuencia se sincroniza explícitamente durante el procedimiento de Solicitud de Servicio NAS o bien mediante el envío del mismo a la MME por parte del UE, o bien mediante el envío del mismo hacia el UE por parte de la MME. No obstante, un inconveniente de esta solución es la complejidad adicional del número de secuencia independiente, puesto que el mismo se debe mantener tanto en el UE como en la MME para evitar ataques de repetición.

Compendio

El objetivo de la presente invención es afrontar el problema expuesto anteriormente en líneas generales, y este objetivo y otros se logran mediante el método y la disposición según las reivindicaciones independientes, y por medio de las realizaciones según las reivindicaciones dependientes.

La idea básica de la presente invención es que la K_eNB se obtiene a partir de la K_ASME y a partir del NAS_U_SEQ del mensaje SOLICITUD DE SERVICIO NAS del UE a la MME, activándose de este modo el establecimiento de un contexto de seguridad UP/RRC en el NodoBe.

Una de las ventajas de la presente invención es que no se requiere ningún mensaje ACEPTACIÓN DE SERVICIO NAS o número de secuencia de enlace descendente, explícito, desde la MME al UE, y que la funcionalidad de protección contra repeticiones del contexto de seguridad NAS se reutiliza en los contextos de seguridad de RRC y UP.

La invención se define mediante las reivindicaciones independientes. Mediante las reivindicaciones dependientes se definen realizaciones adicionales.

Breve descripción de los dibujos

A continuación se describirá más detalladamente la presente invención, y en referencia a los dibujos adjuntos, en los cuales:

- la Figura 1 es un diagrama de señalización que ilustra una Solicitud de Servicio activada por un UE, convencional, en un EPS;
- la Figura 2 es un diagrama de señalización que ilustra la primera realización de esta invención, según la cual el UE recuerda el NAS_U_SEQ enviado a la MME en un mensaje de SOLICITUD DE SERVICIO NAS;
- la Figura 3 es un diagrama de flujo que ilustra la obtención de la K_eNB por parte del UE y la MME;
- la Figura 4 es un diagrama de señalización que ilustra una segunda realización de esta invención, en la que la MME devuelve el NAS_U_SEQ recibido al UE;
- la Figura 5 es un diagrama de flujo que ilustra la segunda realización representada gráficamente en la figura 4; y
- la Figura 6a ilustra esquemáticamente una MME (Entidad de Gestión de Movilidad), y la figura 6b ilustra esquemáticamente un UE, ambos provistos de medios para obtener la clave de seguridad K_eNB.

Descripción detallada

En la siguiente descripción, se exponen detalles específicos, tales como una arquitectura particular y secuencias de etapas para proporcionar una comprensión exhaustiva de la presente invención. La presente invención se define mediante las reivindicaciones adjuntas.

Por otra parte, es evidente que las funciones descritas se pueden implementar usando software que funcione en combinación con un microprocesador programado o un ordenador de propósito general y/o usando un circuito integrado de aplicación específica. Cuando la invención se describe en forma de un método, la invención también se puede materializar en un producto de programa de ordenador, así como en un sistema que comprende un

procesador de ordenador y una memoria, en donde la memoria está codificada con uno o más programas que pueden ejecutar las funciones descritas.

El concepto de la invención es que la clave de seguridad, K_eNB, se obtiene a partir de la clave de Entidad de Gestión de Seguridad de acceso, K_ASME, y a partir del contador de secuencia de enlace ascendente, NAS_U_SEQ, del mensaje SOLICITUD DE SERVICIO NAS enviado desde el UE a la MME, activándose de este modo el establecimiento del contexto de seguridad UP/RRC en el NodoBe.

Cuando el UE se encuentra en modo INACTIVO, existe un contexto de seguridad NAS y el mismo comprende, por ejemplo, la K_NAS_enc, la K_NAS_int, el NAS_U_SEQ y el NAS_D_SEQ antes descritos, y los mensajes NAS están protegidos en cuanto a integridad y posiblemente en cuanto a confidencialidad. De este modo, el contexto de seguridad NAS contiene también las capacidades de seguridad del UE, en particular los algoritmos de cifrado e integridad.

La protección de los mensajes NAS se basa en las claves de seguridad NAS, K_NAS_enc, K_NAS_int, y los contadores de secuencia de enlace ascendente y enlace descendente, NAS_U_SEQ, o NAS_D_SEQ, para la dirección del mensaje. Normalmente, el contador de secuencia completo no se transmite con el mensaje NAS, solamente algunos de los bits de orden inferior, y el número de secuencia completo se reconstruirá en el extremo receptor a partir de una estimación local de los bits de orden superior y los bits de orden inferior recibidos

El concepto de la invención se puede explicar en el contexto del diagrama de señalización para solicitudes de servicio activadas por un UE, tal como se representa gráficamente en la figura 1 antes descrita:

En S1 y S2 del diagrama de señalización convencional de la figura 1, se reenvía una SOLICITUD DE SERVICIO NAS, que comprende un contador de secuencia de enlace ascendente, NAS_U_SEQ, desde el UE a la MME, y el mensaje de SOLICITUD DE SERVICIO NAS está protegido en cuanto a integridad sobre la base de dicho NAS_U_SEQ. La MME comprueba la integridad del mensaje y lo acepta si el mismo no es una repetición, y esto garantiza que el NAS_U_SEQ es nuevo y no ha sido usado anteriormente.

Después de esto, según esta invención, la MME obtiene la K_eNB basándose por lo menos en el contador de secuencia de enlace ascendente NAS_U_SEQ recibido y en la K_ASME, usando una función de obtención de claves convencional, y esto no se incluye en el diagrama de señalización convencional ilustrado en la figura 1. Consecuentemente, el contador de secuencia únicamente se puede reinicializar en la autenticación. La MME enviará la K_eNB obtenida, en sentido descendente hacia el NodoBe en el mensaje de la señal S4, la Solicitud de Establecimiento de Contexto inicial (S1-AP), o colgado del mismo.

En la señal S5, el NodoBe envía un Establecimiento de Portador de Radiocomunicaciones y un mensaje de configuración de seguridad (Orden de Modo de Seguridad) al UE. Estos mensajes se pueden enviar como dos mensajes independientes o combinados en un mensaje, tal como en la figura 1, y la recepción de estos mensajes por parte del UE será implícitamente una confirmación de la SOLICITUD DE SERVICIO NAS de UEs, en la señal S1. La Orden de Modo de Seguridad determinará, por ejemplo, cuándo debería comenzar la protección y qué algoritmo usar.

Según la presente invención, el UE obtiene la K_eNB basándose por lo menos en el NAS_U_SEQ y la K_ASME, usando una función de obtención de claves convencional, tras la recepción del mensaje en la señal S5, si es que no se ha realizado antes. Después de esto, el NodoBe y el UE establecerán los contextos de seguridad UP/RRC, y esto no se ilustra en el diagrama de señalización convencional de la figura 1.

Según una primera realización, el UE almacena el contador de secuencia de enlace ascendente, NAS_U_SEQ, incluido en la SOLICITUD DE SERVICIO NAS inicial en la señal S1, y usa el NAS_U_SEQ almacenado para la obtención de la K_eNB.

No obstante, de acuerdo con una segunda realización, la MME incluye el contador de secuencia de enlace ascendente, NAS_U_SEQ, o únicamente bits de orden inferior que indican el NAS_U_SEQ, en el mensaje de establecimiento de S1-AP, en la señal S4, enviado al NodoBe, en cuyo caso esta información se reenvía también al UE desde el NodoBe durante el establecimiento de contexto RRC/UP. En este caso, el UE podrá recuperar la indicación de NAS_U_SEQ desde el NodoBe para la obtención de la K_eNB, y no tiene que conservar el NAS_U_SEQ del mensaje de SOLICITUD DE SERVICIO NAS del NAS, enviado a la MME en las señales S1 y S2.

La figura 2 ilustra la primera realización, en la que el UE mantiene el NAS_U_SEQ del mensaje de SOLICITUD DE SERVICIO NAS inicial, en la señal S21, para la obtención de K_eNB en la señal S24. La MME recibirá el NAS_U_SEQ del UE en la señal S21, o únicamente bits de orden inferior que indican el NAS_U_SEQ, y obtendrá la K_eNB basándose en el NAS_U_SEQ y la K_ASME en S22. La MME reenvía la K_eNB obtenida hacia el NodoBe en la señal S23.

Después de esto, y no ilustrado en la figura 2, el NodoBe y el UE establecerán el contexto de seguridad UP/RRC usando la K_eNB, comprendiendo los contextos de seguridad de UP/RRC la clave de cifrado, K_eNB_UP_enc para proteger el tráfico de UP, así como la clave de cifrado y la clave de protección de integridad, K_eNB_RRC_enc y

K_eNB_RRC_int, respectivamente, para proteger el tráfico de RRC, lo cual posibilita un tráfico de UP/RRC seguro, en la señal S25.

La obtención de la K_eNB se realiza mediante una función de obtención de claves convencional, mediante una Función Seudo-Aleatoria; K_eNB = PRF (K_ASME, NAS_U_SEQ, ...).

Además, tal como se ilustra por medio de los puntos en la función PRF antes descrita, la función de obtención de K_eNB puede tener valores de entrada convencionales, adicionales, tales como, por ejemplo, la identidad de NodoBe.

La figura 3 es un diagrama de flujo que ilustra el método según la presente invención, y en la etapa 31, el UE 11 envía el mensaje de SOLICITUD DE SERVICIO NAS inicial a la MME 13, indicando el mensaje el contador de secuencia de enlace ascendente NAS, NAS_U_SEQ, normalmente solo mediante el envío de los bits de orden inferior del contador. En la etapa 32, la MME recibe el mensaje de SOLICITUD DE SERVICIO NAS desde el UE, obteniendo el NAS_U_SEQ, y reconstruyendo la secuencia completa a partir de los bits de orden inferior recibidos. En la etapa 33, la MME obtiene la clave de seguridad, K_eNB, a partir de por lo menos el NAS_U_SEQ recibido, y la K_ASME de la ASME (Entidad de Movilidad de Seguridad de Acceso), usando una función de obtención de claves, adecuada, por ejemplo, una Función Seudo-Aleatoria.

Después de esto, la MME reenvía la K_eNB obtenida al NodoBe 12, en la etapa 34, para que sea usada por el NodoBe con el fin de establecer el contexto de seguridad UP/RRC completo, compartido con el UE. En la etapa 35, dicho UE obtendrá la misma K_eNB a partir de por lo menos la K_ASME almacenada y a partir del NAS_U_SEQ del mensaje de SOLICITUD DE SERVICIO NAS inicial transmitido desde el UE a la MME en la etapa 31, y establecerá el contexto de seguridad de UP/RRC a partir de la K_eNB obtenida.

En la primera realización, el UE almacena el NAS_U_SEQ transmitido a la MME en el mensaje de SOLICITUD DE SERVICIO NAS del NAS inicial, y usa el número de secuencia almacenado para obtener la K_eNB.

La figura 4 es un diagrama de señalización que ilustra una segunda realización, en la que el UE no tiene que almacenar el NAS_U_SEQ. En su lugar, la MME devolverá una indicación del NAS_U_SEQ recibido, de vuelta al UE, a través del NodoBe. En la S41, correspondiente a la señal S21 de la figura 2, el UE 11 transmite una SOLICITUD DE SERVICIO NAS inicial a la MME 13, indicando un número de secuencia de enlace ascendente, NAS_U_SEQ, y la MME recibirá el NAS_U_SEQ y obtendrá la K_eNB basándose en por lo menos el NAS_U_SEQ y la K_ASME, en S42. No obstante, de acuerdo con esta segunda realización, la MME obtendrá una indicación de dicho NAS_U_SEQ recibido, en la señal S43 transmitida al NodoBe 12 junto con la K_eNB obtenida, y el NodoBe reenviará el NAS_U_SEQ al UE, en la señal S44. Después de esto, el UE obtendrá la K_eNB a partir de por lo menos la K_ASME y a partir del NAS_U_SEQ devuelto por la MME, en la señal S45. A partir de la clave de seguridad obtenida, K_eNB, el NodoBe y el UE establecerán el contexto de seguridad de UP/RRC, permitiendo de este modo un tráfico de UP/RRC seguro, en la señal S46.

La figura 5 es un diagrama de flujo que ilustra el método antes descrito de acuerdo con una segunda realización, en el que la MME devuelve al UE una indicación del NAS_U_SEQ. En la etapa 41, el UE 11 envía el mensaje de SOLICITUD DE SERVICIO NAS inicial a la MME 13, indicando el mensaje el contador de secuencia de enlace ascendente NAS, NAS_U_SEQ, normalmente los bits de orden inferior. En la etapa 52, la MME recibe el mensaje de SOLICITUD DE SERVICIO NAS del UE, obteniendo de este modo el NAS_U_SEQ, y, si fuera necesario, reconstruyendo el NAS_U_SEQ completo a partir de los bits de orden inferior recibidos. En la etapa 53, la MME obtiene la clave de seguridad, K_eNB, a partir de por lo menos el NAS_U_SEQ recibido y la K_ASME, usando una función de obtención de claves adecuada.

Después de esto, la MME incluye una indicación del contador de secuencia de enlace ascendente NAS, NAS_U_SEQ, en el mensaje que reenvía la K_eNB obtenida hacia el NodoBe 12, en la etapa 54, y el NodoBe usa la clave de seguridad recibida, K_eNB, para establecer un contexto de seguridad de UP/RRC. El NAS_U_SEQ recibido se reenvía al UE 11 por medio del NodoBe, en la etapa 55, y en la etapa 56, el UE obtiene la clave de seguridad, K_eNB, a partir de por lo menos la K_ASME y a partir de dicho NAS_U_SEQ recibido, con el fin de establecer el contexto de seguridad de UP/RRC compartido con el NodoBe.

La obtención de la K_eNB por parte de la MME, en la etapa 53, y por parte del UE, en la etapa 56, se realiza mediante una función de obtención de claves convencional adecuada, por ejemplo, una Función Seudo-Aleatoria; K_eNB = PRF (K_ASME, NAS_U_SEQ, ...). Normalmente, la función de obtención de claves tendrá valores de entrada convencionales, adicionales, por ejemplo, la identidad de NodoBe.

La figura 6a ilustra una MME 13 (Entidad de Gestión de Movilidad) para un EPS, según la presente invención, dispuesta para establecer una clave de seguridad, K_eNB, para un contexto de seguridad para la protección de tráfico de UP/RRC entre un UE y un NodoBe de servicio. La MME está provista de medios de comunicación convencionales, no ilustrados en la figura, para la comunicación con los nodos en el EPS, por ejemplo, con los NodosBe a través de una interfaz de S1-MME. Además, en la MME de la figura 1, se ilustra una ASME (Entidad de Gestión de Seguridad de Acceso) 61 por medio de líneas de trazos, puesto que esta entidad funcional de un EPS puede estar ubicada conjuntamente con la MME.

Los medios de la MME 13 ilustrada en la figura 6a para establecer la clave de seguridad, K_eNB, comprenden medios 62 de recepción para recibir un mensaje de SOLICITUD DE SERVICIO NAS que incluye un NAS_U_SEQ de un UE (a través de su NodoBe de servicio); medios 63 de obtención de claves para obtener una clave de seguridad, K_eNB basándose en por lo menos el NAS_U-SEQ recibido y una K_ASME almacenada, con el uso de una función de obtención de claves convencional; y medios 64 de envío para enviar la K_eNB obtenida al NodoBe que presta servicio al UE.

La figura 6b ilustra un UE 11 (Entidad de Usuario) según la presente invención, estando adaptado la UE para un EPS, y estando dispuesta además para establecer una clave de seguridad, K_eNB, para un contexto de seguridad para la protección de tráfico de UP/RRC intercambiado con su NodoBe de servicio. La UE está provista de medios de comunicación convencionales, no ilustrados en la figura, para comunicarse con los nodos en el EPS a través de una interfaz LTE-Uu hacia su NodoBe de servicio.

Los medios de la UE 11 ilustrada en la figura 6b para establecer la clave de seguridad, K_eNB, comprenden medios 66 de envío para enviar un mensaje de SOLICITUD DE SERVICIO NAS hacia la MME, a través del NodoBe, indicando la solicitud un número de secuencia de enlace ascendente, NAS_U-SEQ, y los medios para establecer una clave de seguridad, K_eNB, comprenden medios 67 de obtención de claves para obtener una clave de seguridad, K_eNB basándose en por lo menos el NAS_U-SEQ y una K_ASME almacenada, usando una función de obtención de claves convencional.

Los medios antes descritos de la MME y la UE, según se ilustra en las figuras 6a y 6b, implementan las funciones descritas usando una combinación adecuada de software y hardware, por ejemplo, un microprocesador programado o un circuito integrado de aplicación específica, así como transmisores y receptores convencionales de radiocomunicaciones.

Aunque la invención se ha descrito en referencia a realizaciones ejemplificativas específicas, la descripción en general está solamente destinada a ilustrar el concepto de la invención y no debe considerarse como limitativa del alcance de la misma.

REIVINDICACIONES

1. Método en una Entidad (13) de Gestión de Movilidad de un Sistema de Paquetes Evolucionado, EPS, para establecer una clave de seguridad para proteger tráfico de Control de Recursos de Radiocomunicaciones/Plano de Usuario entre un Equipo (11) de Usuario, UE, y una estación de base de radio (12) que presta servicio al UE, comprendiendo el método las siguientes etapas:

- Recibir (32, 52) un mensaje de Solicitud de Servicio de Estrato Sin Acceso, NAS, desde el UE, indicando el mensaje un número de secuencia de enlace ascendente de NAS;

- Obtener (33, 53) la clave de seguridad a partir de por lo menos dicho número de secuencia de enlace ascendente de NAS indicado y a partir de una clave de Entidad de Gestión de Seguridad de Acceso almacenada compartida con dicho UE, utilizando una función de obtención de claves que toma el número de secuencia de enlace ascendente de NAS y la clave de Entidad de Gestión de Seguridad de Acceso almacenada como entradas;

- Reenviar (34) dicha clave de seguridad obtenida hacia la estación de base de radio (12) que presta servicio a dicho UE.

2. Método en una Entidad de Gestión de Movilidad según la reivindicación 1, en el que la función de obtención de claves es una Función Seudo-Aleatoria.

3. Método en un Equipo (11) de Usuario, UE, de un Sistema de Paquetes Evolucionado, EPS, para establecer una clave de seguridad para proteger tráfico de Control de Recursos de Radiocomunicaciones/Plano de Usuario intercambiado con una estación de base de radio (12) de servicio, comprendiendo el método las siguientes etapas:

- Enviar (31, 51) un mensaje de Solicitud de Servicio de Estrato sin Acceso, NAS, a una Entidad de Gestión de Movilidad, indicando el mensaje un número de secuencia de enlace ascendente de NAS;

- Obtener (33, 53) la clave de seguridad a partir de por lo menos dicho número de secuencia de enlace ascendente de NAS indicado y a partir de una clave de Entidad de Gestión de Seguridad de Acceso almacenada compartida con dicha Entidad de Gestión de Movilidad, utilizando una función de obtención de claves que toma el número de secuencia de enlace ascendente de NAS y la clave de Entidad de Gestión de Seguridad de Acceso almacenada como entradas.

4. Método en un UE según la reivindicación 3, en el que la función de obtención de claves es una Función Seudo-Aleatoria.

5. Método en un UE según cualquiera de las reivindicaciones 3 - 4, que comprende la etapa adicional de proteger en cuanto a integridad la Solicitud de Servicio de NAS enviada a la Entidad de Gestión de Movilidad.

6. Método en un UE según cualquiera de las reivindicaciones 3 - 5, que comprende la etapa de almacenar el número de secuencia de enlace ascendente de NAS o la indicación del mismo de la Solicitud de Servicio de NAS enviada a la Entidad de Gestión de Movilidad.

7. Método en un UE según cualquiera de las reivindicaciones 3 - 6, en el que la clave de seguridad se obtiene a partir del número de secuencia de enlace ascendente de NAS y la clave de Entidad de Gestión de Seguridad de Acceso después de la recepción de un mensaje de configuración de seguridad desde la estación de base de radio.

8. Entidad (13) de Gestión de Movilidad de un Sistema de Paquetes Evolucionado, EPS, la Entidad de Gestión de Movilidad dispuesta para establecer una clave de seguridad para la protección de tráfico de Control de Recursos de Radiocomunicaciones/Plano de Usuario entre un UE (11) y una estación de base de radio (12) que presta servicio al UE, incluyendo la Entidad de Gestión de Movilidad:

- Medios (62) para recibir un mensaje de Solicitud de Servicio de Estrato sin Acceso, NAS, desde el UE, indicando el mensaje un número de secuencia de enlace ascendente de NAS;

- Medios (63) para obtener una clave de seguridad a partir de por lo menos dicho número de secuencia de enlace ascendente de NAS indicado y a partir de una clave de Entidad de Gestión de Seguridad de Acceso almacenada compartida con dicho UE, utilizando una función de obtención de claves que toma el número de secuencia de enlace ascendente de NAS y la clave de Entidad de Gestión de Seguridad de Acceso almacenada como entradas;

- Medios (64) para enviar la clave de seguridad obtenida hacia la estación de base de radio (12) que presta servicio a dicho UE.

9. Entidad de Gestión de Movilidad según la reivindicación 8, en la que la función de obtención de claves es una Función Seudo-Aleatoria.

10. Equipo (11) de usuario, UE, de un Sistema de Paquetes Evolucionado, EPS, el UE dispuesto para establecer una clave de seguridad para proteger tráfico de Control de Recursos de Radiocomunicaciones/Plano de Usuario intercambiado con una estación de base de radio (12) de servicio, incluyendo el UE:

- Medios (66) para enviar un mensaje de Solicitud de Servicio de Estrato sin Acceso, NAS, a una Entidad de Gestión de Movilidad, indicando el mensaje un número de secuencia de enlace ascendente de NAS;

- Medios (67) para obtener la clave de seguridad a partir de por lo menos dicho número de secuencia de enlace ascendente de NAS indicado y a partir de una clave de Entidad de Gestión de Seguridad de Acceso almacenada compartida con dicha Entidad de Gestión de Movilidad, utilizando una función de obtención de claves que toma el número de secuencia de enlace ascendente de NAS y la clave de Entidad de Gestión de Seguridad de Acceso almacenada como entradas.

11. UE (11) según la reivindicación 10, en el que la función de obtención de claves es una Función Seudo-Aleatoria.

12. UE (11) según cualquiera de las reivindicaciones 10 - 11, que comprende la etapa adicional de proteger en cuanto a integridad la Solicitud de Servicio de NAS enviada a la Entidad de Gestión de Movilidad.

13. UE (11) según cualquiera de las reivindicaciones 10 - 12, que comprende la etapa adicional de almacenar el número de secuencia de enlace ascendente de NAS o la indicación del mismo de la Solicitud de Servicio de NAS enviada a la Entidad de Gestión de Movilidad.

14. UE (11) según cualquiera de las reivindicaciones 10 - 13, en el que la clave de seguridad se obtiene a partir del número de secuencia de enlace ascendente de NAS y la clave de Entidad de Gestión de Seguridad de Acceso después de la recepción de un mensaje de configuración de seguridad desde la estación de base de radio.

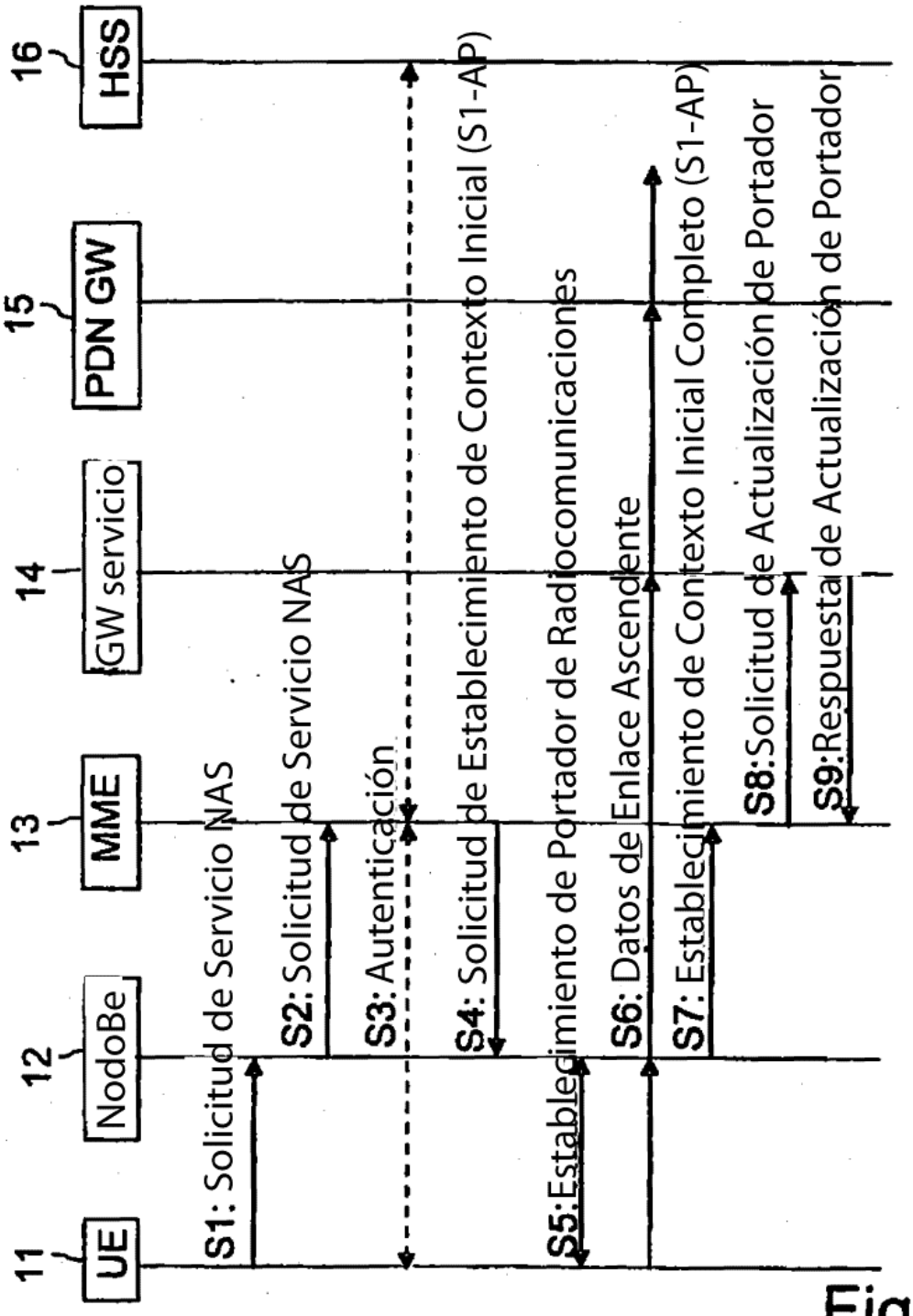
11
UE
12
NodoBe
13
MME
14
GW servicio
15
PDN GW
16
HSS
S1: Solicitud de Servicio NAS
S2: Solicitud de Servicio NAS
S3: Autenticación
S4: Solicitud de Establecimiento de Contexto Inicial (S1-AP)
S5: Establecimiento de Portador de Radiocomunicaciones
S6: Datos de Enlace Ascendente
S7: Establecimiento de Contexto Inicial Completo (S1-AP)
S8: Solicitud de Actualización de Portador
S9: Respuesta de Actualización de Portador

Fig. 1

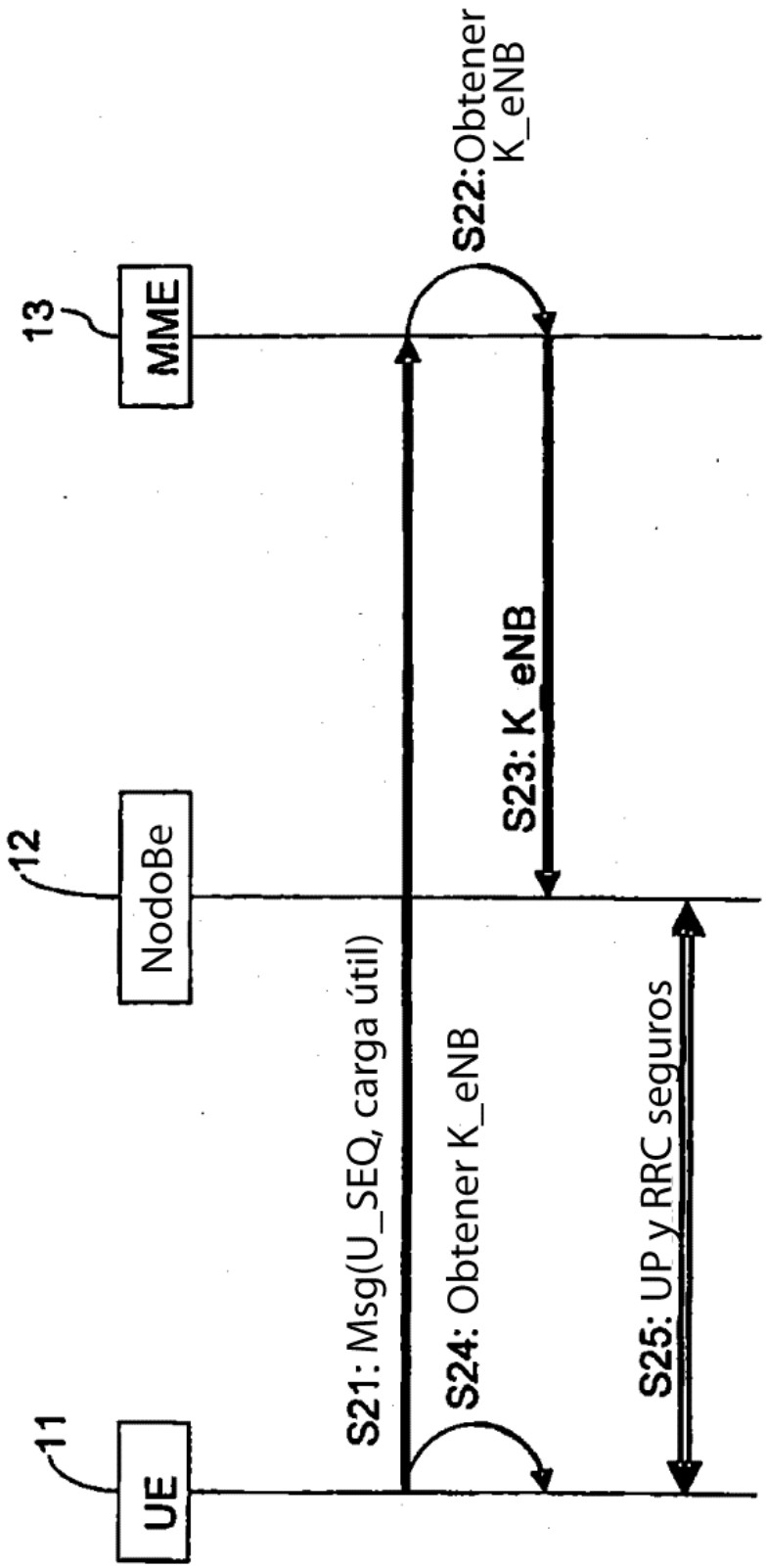
13
MME
S22: Obtener K_eNB
12
NodoBe
S23: K_eNB
S21: Msg(U_SEQ, carga útil)
S24: Obtener K_eNB
S25: UP y RRC seguros
11
UE

Fig. 2

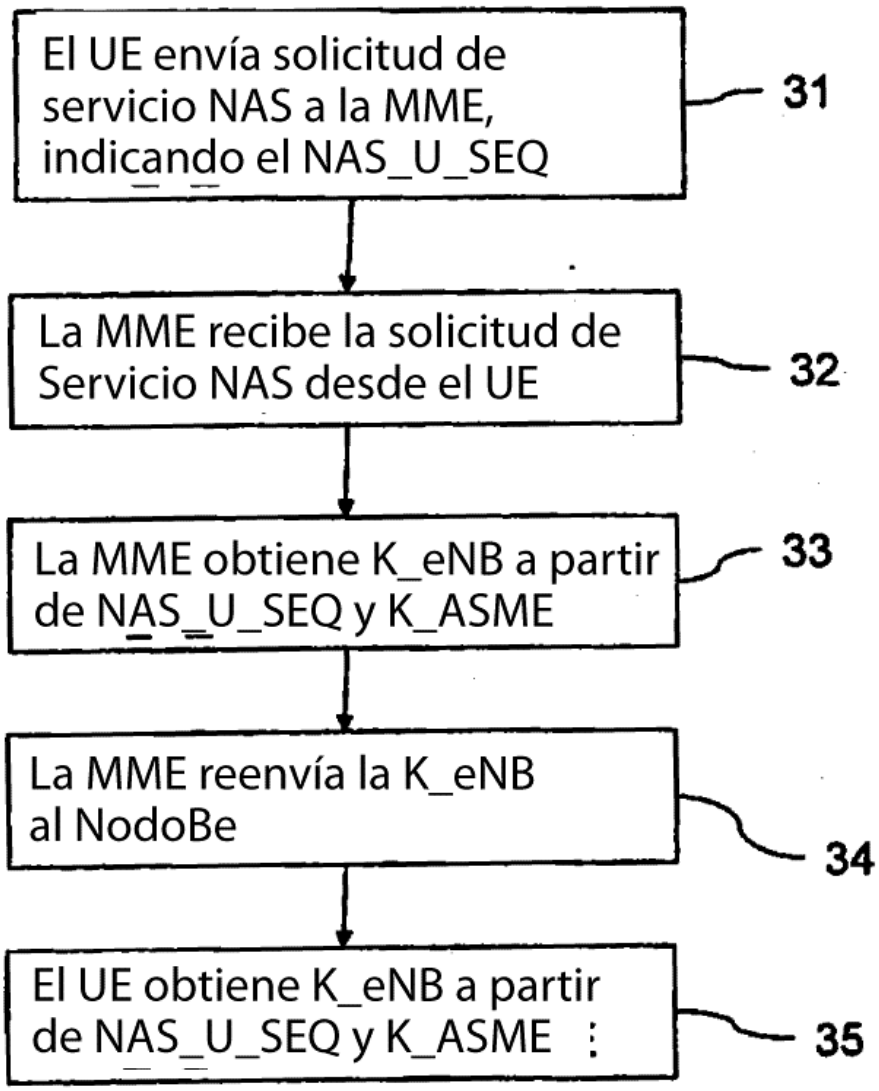
El UE envía solicitud de servicio NAS a la MME, indicando el NAS_U_SEQ
31
La MME recibe la solicitud de Servicio NAS desde el UE
32
La MME obtiene K_eNB a partir de NAS_U_SEQ y K_ASME
33
La MME reenvía la K_eNB al NodoBe
34
El UE obtiene K_eNB a partir de NAS_U_SEQ y K_ASME
35

Fig. 3

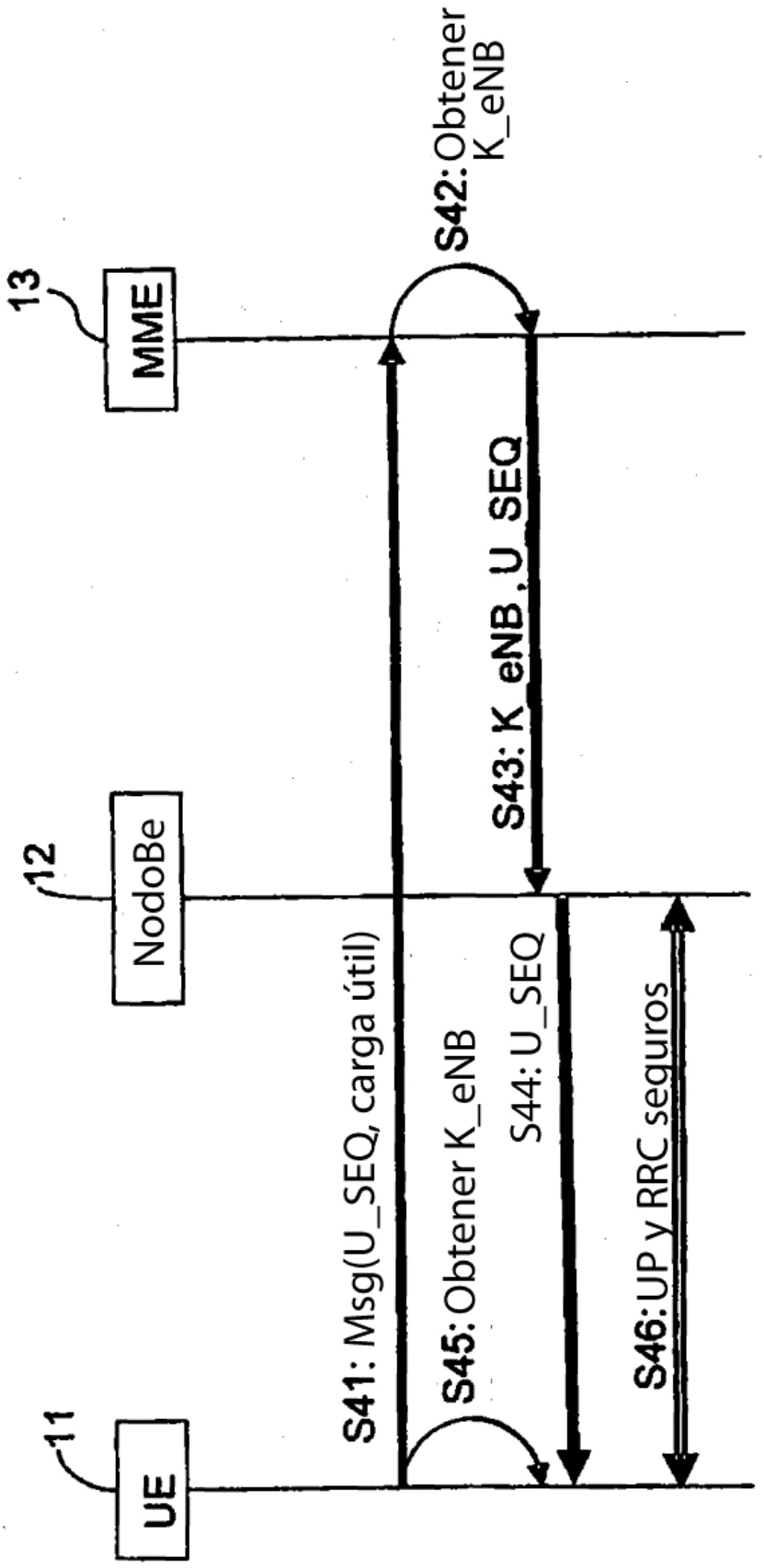
13
MME
S42: Obtener K_eNB
12
NodoBe
S43: K_eNB, U_SEQ
S41: Msg(U_SEQ, carga útil)
S45: Obtener K_eNB
S44: U_SEQ
S46: UP y RRC seguros
11
UE

Fig. 4

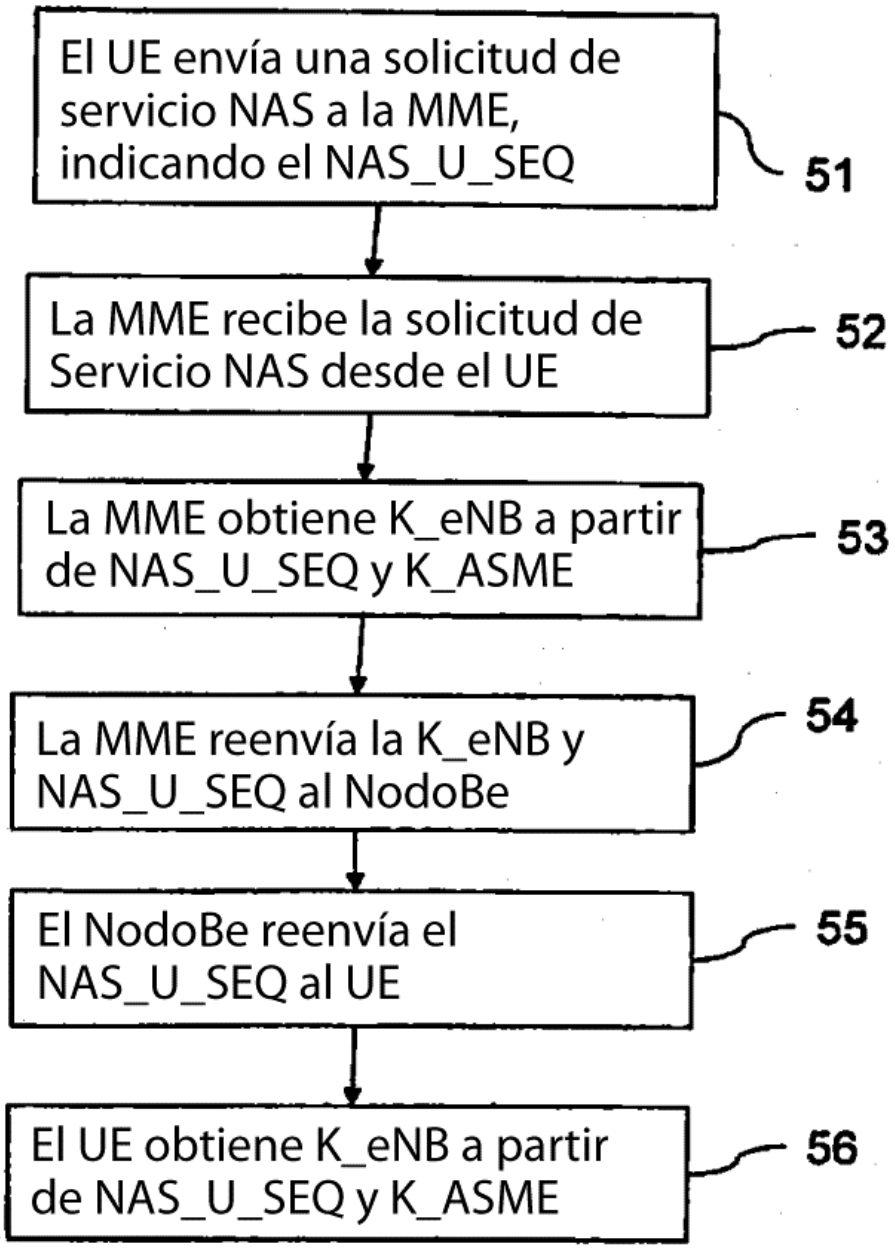
El UE envía una solicitud de servicio NAS a la MME, indicando el NAS_U_SEQ
51
La MME recibe la solicitud de Servicio NAS desde el UE
52
La MME obtiene K_eNB a partir de NAS_U_SEQ y K_ASME
53
La MME reenvía la K_eNB y NAS_U_SEQ al NodoBe
54
El NodoBe reenvía el NAS_U_SEQ al UE
55
El UE obtiene K_eNB a partir de NAS_U_SEQ y K_ASME
56

Fig. 5

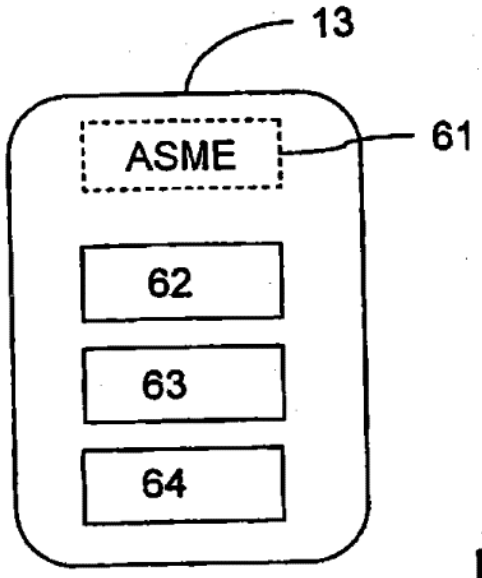

Fig. 6a

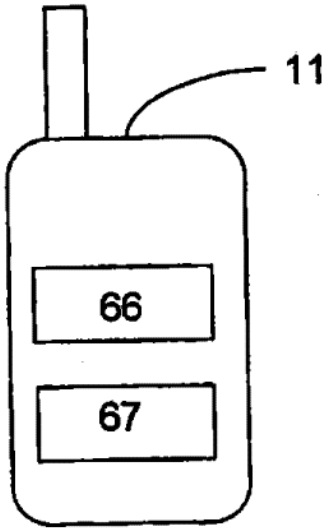

Fig. 6b