

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 845 874**

51 Int. Cl.:

H04W 12/06 (2009.01)

H04W 36/00 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **29.01.2018** **E 19196520 (1)**

97 Fecha y número de publicación de la concesión europea: **18.11.2020** **EP 3599784**

54 Título: **Métodos y aparatos para restablecer una conexión de control de recurso de radio (RRC)**

30 Prioridad:

30.01.2017 US 201762451866 P

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
28.07.2021

73 Titular/es:

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

72 Inventor/es:

LEHTOVIRTA, VESA;
WIFVESSON, MONICA y
NAKARMI, PRAJWOL KUMAR

74 Agente/Representante:

LINAGE GONZÁLEZ, Rafael

ES 2 845 874 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 y aparatos para restablecer una conexión de control de recurso de radio (RRC)

5 Campo técnico

La invención se refiere a métodos, equipo de usuario, nodo B de destino y entidad de gestión de movilidad para restablecer una conexión de control de recurso de radio.

10 Antecedentes

Las optimizaciones de Internet de las cosas celular (CIoT) de plano de control CP) (también llamadas datos a través de estrato sin acceso (NAS) (DoNAS)) es una solución para transportar datos a través de NAS como se especifica en la especificación técnica TS del proyecto de asociación de tercera generación (3GPP) 23.401 V14.2.0, cláusula 5.3.4B (y otras especificaciones, por ejemplo, TS 24.301 V14.2.0). Las características de seguridad se especifican en TS 33.401 V14.1.0, cláusula 8.2. El impacto de seguridad de la solución básica es muy limitado. El propósito de la función DoNAS es enviar datos a través de la señalización NAS sin establecer portadores de radio de datos (DRB) y sin establecer la seguridad de estrato de acceso (AS). La intención es salvar la señalización. La figura 1, que corresponde a la figura 5.3.4B.2-1 de TS 23.401 V14.2.0, ilustra el principio DoNAS.

El elemento de trabajo en el documento 3GPP R3-161324 analiza las mejoras de movilidad para CIoT de CP. Los trasposos no son soportados para CIoT de CP, pero un equipo de usuario (UE) puede moverse de todos modos, provocando un fallo en el enlace de radio (RLF) cuando el UE está en modo conectado (es decir, tiene una conexión de control de recurso de radio (RRC) con un NodoB evolucionado (eNB)). Esto ha planteado la cuestión de qué hacer en tal caso. Dado que la seguridad AS no es soportada para la función de CIoT de CP, los mecanismos existentes para RLF no se pueden usar de forma segura tal como están. En otras palabras, no es aceptable desde el punto de vista de la seguridad usar el mecanismo de manejo de RLF existente en el CIoT de CP.

La capa de RRC se encuentra en los sistemas LTE (evolución a largo plazo) actuales, véase, por ejemplo, 3GPP TS 36.331 V14.1.0, especificado para incluir un elemento de información (IE) llamado ShortMAC-I que se usa para la identificación del UE, por ejemplo, durante los procedimientos de restablecimiento de conexión de RRC. El cálculo del ShortMAC-I incluye lo siguiente como entrada:

- Clave de integridad de RRC: CADENA DE BIT (TAMAÑO (128))

- Identidad de la célula de destino: CADENA DE BIT (TAMAÑO (28))

- Identidad de célula física de la célula de origen: ENTERO (0 ... 503)

- C-RNTI (identificador temporal de la red de radio de célula) del UE en la célula de origen: CADENA DE BIT (TAMAÑO (16))

La función usada se especifica en TS 33.401 V14.1.0.

La capa de RRC está en los sistemas LTE especificados para incluir un elemento de información (IE) llamado ShortResumeMAC-I que se usa para la identificación del UE, por ejemplo, durante los procedimientos de reanudación de la conexión de RRC. El cálculo del ShortResumeMAC-I incluye lo siguiente como entrada:

- Clave de integridad de RRC: CADENA DE BIT (TAMAÑO (128))

- Identidad de la célula de destino: CADENA DE BIT (TAMAÑO (28))

- Identidad de célula física de la célula de origen: ENTERO (0 ... 503)

- C-RNTI del UE en la célula de origen: CADENA DE BIT (TAMAÑO (16))

- Reanudar constante

Téngase en cuenta que el cálculo de ShortResumeMAC-I incluye adicionalmente una constante de reanudación, que permite diferenciar ShortMAC-I de ResumeShortMAC-I. La función usada = se especifica en TS 33.401 V14.1.0.

Ghizlande Orhanou et al: " Enfoque algorítmico de mecanismos de confidencialidad e integridad de EPS ", IJCSI International Journal of Computer Science Issues, vol. 7, no. 4, divulga la señalización de RRC y NAS. También se divulga una clave de integridad K_{NASint} para el tráfico NAS.

Sumario

Es un objeto de la invención permitir una señalización reducida durante el restablecimiento de una conexión de control de recurso de radio.

- 5 Otro objeto de la invención es permitir la autenticación de un eNB de destino por parte del UE durante el restablecimiento de conexión de RRC.

De acuerdo con un primer aspecto de la invención, se presenta un método para restablecer una conexión de control de recurso de radio (RRC) entre un equipo de usuario (UE) y un NodoB evolucionado de destino (eNB de destino).

- 10 El método lo realiza el UE y comprende:

recibir un mensaje de restablecimiento de conexión de RRC del eNB de destino, el mensaje de restablecimiento de conexión de RRC que incluye un token de autenticación de enlace descendente (DL) que ha sido generado por una entidad de gestión de movilidad (MME) y ha tenido una clave de integridad de estrato sin acceso (NAS) y un parámetro de actualización como entrada; y

- 15 autenticar el token de autenticación DL recibido.

De este modo, entre otras cosas, se consigue que el UE esté habilitado para autenticar un eNB durante el restablecimiento de conexión de RRC, tal como el restablecimiento de conexión de RRC para la optimización de EPS CP IoT, con la ayuda de una clave de integridad NAS. Por lo tanto, no es necesario crear claves de estrato de acceso (AS), lo cual es muy beneficioso, por ejemplo, porque las claves NAS deben generarse de todos modos, mientras que las claves AS tendrían que generarse únicamente para ser usadas en el restablecimiento de conexión de RRC.

- 25 El método también puede comprender un paso de calcular un token de autenticación de enlace ascendente (UL) con la clave de integridad NAS como entrada, y enviar una solicitud de restablecimiento de conexión de RRC que incluye el token de autenticación UL al eNB de destino. En ese caso, el token de autenticación UL puede calcularse con la identidad de una célula de destino como entrada.

- 30 Un segundo aspecto se refiere a un método para restablecer una conexión de RRC entre un UE y un eNB de destino y lo realiza el eNB de destino. El método comprende:

- 35 recibir, desde una MME, un mensaje que incluye un token de autenticación DL que ha sido generado por la MME, en el que el token de autenticación DL se ha generado con una clave de integridad NAS y un parámetro de actualización como entrada; y

enviar un mensaje de restablecimiento de conexión de RRC al UE, incluyendo el mensaje de restablecimiento de conexión de RRC el token de autenticación DL.

- 40 En una realización del segundo aspecto, el método comprende recibir del UE una solicitud de restablecimiento de conexión de RRC que incluye un token de autenticación UL, en el que el UE ha calculado el token de autenticación UL con la clave de integridad NAS como entrada. El token de autenticación UL puede haber sido calculado por el UE con la identidad de una célula de destino como entrada.

- 45 Un tercer aspecto se refiere a un método para restablecer una conexión de RRC entre un UE y un eNB de destino y lo realiza una MME. El método comprende:

- 50 generar un token de autenticación DL con una clave de integridad NAS y un parámetro de actualización como entrada; y

enviar un mensaje que incluye el token de autenticación DL generado al eNB de destino.

- 55 En una realización del tercer aspecto, la generación del token de autenticación DL se realiza con la identidad de una célula de destino como entrada (además de la clave de integridad NAS).

El método de acuerdo con el tercer aspecto puede comprender:

- 60 recibir un token de autenticación UL del eNB de destino, habiendo sido generado dicho token de autenticación UL por el UE con la clave de integridad NAS como entrada, y

verificar el token de autenticación UL.

- 65 El token de autenticación UL puede haber sido generado por el UE con la identidad de una célula de destino como entrada.

Un cuarto aspecto de la invención se refiere a un UE para restablecer una conexión de RRC entre el UE y un eNB de destino. El UE comprende:

un procesador; y un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el UE:

reciba un mensaje de restablecimiento de conexión de RRC del eNB de destino, incluyendo el mensaje de restablecimiento de conexión de RRC un token de autenticación DL que ha sido generado por una MME y ha tenido una clave de integridad NAS y un parámetro de actualización como entrada; y

autentique el token de autenticación DL recibido.

En una realización del UE, el token de autenticación DL ha sido calculado por la MME con la identidad de una célula de destino como entrada.

Un quinto aspecto se refiere a un eNB de destino para restablecer una conexión de RRC entre un UE y el eNB de destino. El eNB de destino comprende:

un procesador; y

un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de destino:

reciba, de una MME, un mensaje que incluye un token de autenticación DL que ha sido generado por la MME, en el que el token de autenticación DL se ha generado con una clave de integridad NAS y un parámetro de actualización como entrada; y

envíe un mensaje de restablecimiento de conexión de RRC al UE, incluyendo el mensaje de restablecimiento de conexión de RRC el token de autenticación DL.

Un sexto aspecto se refiere a una MME para restablecer una conexión de RRC entre un UE y un eNB de destino. La MME comprende:

un procesador; y

un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la MME:

genere un token de autenticación DL con una clave de integridad NAS y un parámetro de actualización como entrada; y

envíe un mensaje que incluya el token de autenticación DL generado al eNB de destino.

Generalmente, todos los términos usados en la lista detallada de realizaciones deben interpretarse de acuerdo con su significado ordinario en el campo técnico, a menos que se defina explícitamente lo contrario en el presente documento. Todas las referencias a "un/el elemento, aparato, componente, medio, paso, etc." deben interpretarse abiertamente como una referencia a al menos una instancia del elemento, aparato, componente, medio, paso, etc., a menos que se indique explícitamente lo contrario. Los pasos de cualquier método divulgado en el presente documento no tienen que realizarse en el orden exacto divulgado, a menos que se indique explícitamente.

Breve descripción de los dibujos

La invención se describe ahora, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

la figura 1 muestra esquemáticamente la señalización del principio DoNAS;

la figura 2 ilustra esquemáticamente un entorno en el que se pueden aplicar las realizaciones presentadas en el presente documento;

la figura 3a muestra esquemáticamente la señalización de acuerdo con una parte de una realización presentada en el presente documento;

la figura 3b muestra esquemáticamente la señalización de acuerdo con una parte de una realización presentada en el presente documento y comenzada en la figura 3a;

la figura 4a muestra esquemáticamente la señalización de acuerdo con una parte de una realización presentada en el presente documento;

la figura 4b muestra esquemáticamente la señalización de acuerdo con una parte de una realización presentada en el presente documento y comenzada en la figura 4a;

la figura 5 muestra esquemáticamente la señalización de acuerdo con una realización presentada en el presente documento;

la figura 6 muestra esquemáticamente la señalización de acuerdo con una realización presentada en el presente documento;

las figuras 7A a 7D son diagramas de flujo que ilustran métodos de acuerdo con las realizaciones presentadas en el presente documento;

las figuras 8 a 11 son diagramas esquemáticos que ilustran algunos componentes de entidades presentadas en el presente documento; y

las figuras 12 a 15 son diagramas esquemáticos que muestran módulos funcionales de realizaciones presentadas en el presente documento.

Descripción detallada

La invención se describirá ahora con más detalle a continuación con referencia a los dibujos adjuntos, en los que se muestran determinadas realizaciones de la invención. Sin embargo, esta invención puede realizarse de muchas formas diferentes y no debe interpretarse como limitada a las realizaciones expuestas en el presente documento; más bien, estas realizaciones se proporcionan a modo de ejemplo, de modo que esta divulgación sea minuciosa y completa, y transmita completamente el alcance de la invención a los expertos en la técnica. Los números similares se refieren a elementos similares en toda la descripción.

Los procedimientos de restablecimiento de conexión de control de recurso de radio (RRC) y suspensión/reanudación de conexión de RRC son soluciones existentes, que podrían ser candidatas para manejar un fallo de enlace de radio en caso de un caso de optimización de Internet de las cosas celular (CIoT) del plano de control (CP). Ambas soluciones existentes usan el token de autenticación de un equipo de usuario (UE) como se describe en los antecedentes para mostrar a un NodoB evolucionado (eNB) que un UE 1 genuino desea restablecer o reanudar una conexión de RRC. Además, los mensajes de RRC protegidos por integridad en la dirección del enlace descendente (DL) se usan para mostrar al UE 1 que está conectado a un eNB genuino. Sin embargo, esas soluciones se basan en la existencia de seguridad de estrato de acceso (AS) (especialmente seguridad de RRC), pero la seguridad AS y la seguridad de RRC no existen o no se usan para optimizaciones de CIoT de CP. Por lo tanto, el restablecimiento de conexión de RRC y los procedimientos de suspensión/reanudación de la conexión de RRC tal como están, no son aceptables desde el punto de vista de la seguridad para ser usados para manejar la movilidad en el CIoT de CP.

Una solución descrita en la contribución 3GPP S3-161717 propone que un token de autenticación se basaría en una nueva clave de integridad de RRC (llamada KeNB-RRC) que puede derivarse tanto del UE 1 como de la entidad 4 de gestión de movilidad (MME), sin configurar la seguridad AS (incluida la seguridad de RRC) entre el UE 1 y el eNB 2 de origen a través del procedimiento de comando de modo de seguridad AS (SMC), y el token se usaría entre el UE 1 y el eNB 3 de destino. Sin embargo, la solución descrita en la contribución 3GPP S3-161717 está tratando de resolver el problema de cómo mostrarle al eNB que un UE 1 genuino quiere restablecer una conexión de RRC. No se contempla el problema de cómo mostrarle al UE 1 que está conectado a un eNB genuino.

En ausencia de seguridad AS y, en consecuencia, la ausencia de protección de integridad de los mensajes de RRC DL desde el eNB al UE, en el contexto de la movilidad de CIoT de CP, actualmente no hay forma de mostrarle al UE que está conectado a un eNB. Para mitigar ese problema, se presenta el uso de un token de autenticación en dirección DL desde la red al UE. El token de autenticación puede ser generado y enviado por la MME, el eNB de origen o el eNB de destino. El token de autenticación DL se puede calcular usando las claves NAS o AS (aunque esta última no está dentro del alcance de las afirmaciones de esta solicitud) dependiendo de la entidad que lo envíe. Se identifican los siguientes casos:

Siempre se envía un token de autenticación DL al UE a través del eNB de destino.

Las siguientes cuatro soluciones variantes muestran cómo se puede lograr esto.

1a. El token de autenticación DL se envía desde el eNB de origen a través del eNB de destino al UE y el UE lo verifica con una clave AS. Alternativamente, el eNB de destino calcula el token con las claves Krrc_int recibidas del eNB de origen. Esta variante no está dentro del alcance de las reivindicaciones de esta solicitud.

1b. El token de autenticación DL se envía desde la MME a través del eNB de origen y el eNB de destino al UE y el UE lo verifica con una clave NAS.

2a. El token de autenticación DL se envía desde la MME en un mensaje de acuse de recibo de cambio de ruta a través del eNB de destino al UE y el UE verifica el token de autenticación DL con una clave NAS.

2b. El token de autenticación DL se envía desde la MME en un nuevo mensaje a través del eNB de destino al UE y el UE verifica el token con una clave NAS.

Cuando una verificación realizada por el UE de que está conectado a un eNB genuino se basa en un token de autenticación DL, no es necesario establecer claves de AS en absoluto. Por lo tanto, se puede evitar la generación de claves AS, lo cual es beneficioso, ya que, de lo contrario, las claves AS solo tendrían que generarse con el fin de restablecer la conexión de RRC y no se usarían para nada más. Sin embargo, las claves NAS podrían usarse para otros problemas de seguridad además de para autenticar el eNB. Más precisamente, las claves NAS se han creado de todos modos, ya que existe un contexto de seguridad NAS para un UE que envía datos a través del NAS.

Cuando el UE experimenta un fallo de enlace de radio (RLF) durante la conexión de CloT de CP (DoNAS), el UE intenta restablecer la conexión de RRC a otro eNB, véase la figura 2.

El token de autenticación de la red para usar en CloT de CP (denominado MAC CloT DL) es un token que se usará para la autenticación de la red, es decir, para mostrarle al UE 1 que está conectado a un eNB 3 de destino genuino.

El MAC CloT DL puede, de acuerdo con los aspectos de la invención reivindicada, calcularse con lo siguiente como entrada:

- clave de integridad NAS (NAS-int, por ejemplo, KNASint). En otras variantes, aunque no se reivindica en esta solicitud, también puede ser una clave de integridad AS o una clave derivada de NAS-int o clave de integridad AS (Krrc_int) o una clave derivada de cualquiera de esas claves. NAS-int se indica en muchos casos en el texto siguiente como MAC CloT DL de clave. El uso de la clave NAS o AS depende de si el MAC CloT DL es calculado por la MME 4 o un eNB. Otras claves alternativas fuera del alcance de las reivindicaciones de esta solicitud son claves raíz para NAS-int, por ejemplo, KASME en LTE y KAUSF, KSEAF y KAMF en sistemas de nueva radio.

- identidad de la célula de destino (ID de célula).

- identidad física célula de la célula de origen.

- C-RNTI de UE en la célula de origen.

- constante (la constante permite diferenciar MAC CloT de ShortResumeMAC-I y ShortMAC-I o un MAC definido de otras formas.

- una posible entrada para el cálculo de MAC CloT DL es un token de autenticación de enlace ascendente, UL, aquí llamado MAC CloT UL (enlace ascendente).

- un parámetro de actualización.

La entrada usada para el cálculo del MAC CloT DL se denominará MAC CloT DL de entrada. Por lo tanto, la identidad de la célula de destino puede ser parte de MAC CloT DL de entrada, pero la clave de integridad NAS puede estar separada de MAC CloT DL de entrada recibida por el UE, ya que típicamente ya tiene la clave de integridad NAS y la usó para cálculo del MAC CloT UL.

La función usada para el cálculo del MAC CloT DL (denominado Fun-MAC CloT DL) puede ser la misma que se usa en el anexo B.2 de TS 33.401 para el restablecimiento de RRC y la reanudación de RRC, es decir, un algoritmo de integridad en forma de algoritmo de integridad NAS de 128 bits, que puede ser 128-EIA1, 128-EIA2 y 128-EIA3.

La variante 1a se ilustra en las figuras 3a y 3b, en la que MAC CloT DL se envía desde el eNB de origen y es verificado por el UE con una clave AS (no dentro del alcance de las reivindicaciones de la solicitud) o una clave NAS.

Esta variante se basa en una negociación del algoritmo AS a través del protocolo NAS y la posterior verificación del token de enlace ascendente denominado MAC CloT UL en el eNB de origen. La variante comprende un mecanismo donde el eNB de origen, después de haber verificado MAC CloT UL, genera un token de enlace descendente denominado MAC CloT DL. El eNB de origen envía el MAC CloT DL al eNB de destino en un mensaje de respuesta de contexto de UE X2. El eNB de destino envía el MAC CloT DL además al UE en un mensaje de RRC para verificación de autenticación. Si la verificación del MAC CloT DL tiene éxito, el UE sabe que está conectado a un eNB auténtico y no a un eNB falso.

Los pasos del 1 al 15 se definen en las especificaciones 3GPP actuales. El UE establece una conexión de RRC y envía datos a través del NAS, que se reenvía desde MME a pasarela de servicio (S-GW)/pasarela de red de datos en paquetes (P-GW). Un RLF ocurre en el paso 15. El RLF también puede ocurrir antes de que el UE haya recibido datos DL.

Paso 16. El UE inicia una conexión de RRC enviando un mensaje de acceso aleatorio a un eNB de destino.

Paso 17. El eNB de destino responde con una respuesta de acceso aleatorio al UE.

Paso 18. El UE genera un token de autenticación, MAC Clot UL. El token puede calcularse de la siguiente manera: $\text{token} = f(\text{PCI de origen}, \text{C-RNTI de origen}, \text{ID de célula de destino}, \text{clave NAS}, \text{entrada de reproducción})$, donde la clave NAS es la clave de integridad NAS actual, por ejemplo, KNAS_{int} , o es un derivado del mismo. f = función. Sin embargo, con respecto a esta variante particular 1a, el token podría derivarse de una clave AS en lugar de la clave NAS. La clave AS puede ser una clave de integridad AS, como $\text{K}_{\text{RRChint}}$.

Paso 19. El UE envía un mensaje de restablecimiento de conexión de RRC al eNB de destino, por ejemplo, para la optimización de CP IoT EPS (sistema de paquete evolucionado). El mensaje incluye el MAC Clot UL.

Paso 20. El eNB de destino envía un mensaje de solicitud de contexto de UE X2 al eNB de origen. El mensaje incluye el MAC Clot UL.

Paso 21. El eNB de origen verifica si el MAC Clot UL es auténtico.

Paso 22. Si la autenticación tiene éxito, el eNB de origen genera MAC Clot DL como se describe anteriormente usando MAC Clot DL de entrada y MAC Clot DL de clave y el procesamiento continúa en el paso 23. Si la autenticación falla, el eNB de origen envía una respuesta de contexto de UE X2 que indica fallo. El fallo activará el eNB de destino para liberar la conexión de RRC (no ilustrada).

Paso 23. El eNB de origen envía una respuesta de contexto de UE X2 al eNB de destino. El mensaje incluye el MAC Clot DL. El mensaje puede incluir además MAC Clot DL de entrada.

Paso 24. El eNB de destino envía un mensaje de restablecimiento de conexión de RRC al UE. El mensaje incluye el MAC Clot DL. El mensaje puede incluir además MAC Clot DL de entrada.

Paso 25. Al recibir el mensaje de restablecimiento de conexión de RRC, el UE autentica el MAC Clot DL usando MAC Clot DL de entrada y MAC Clot DL de clave como se describió anteriormente.

Paso 26A. Si la autenticación de MAC Clot DL tiene éxito.

26A.1 El UE envía un mensaje de restablecimiento de conexión de RRC completo, que contiene opcionalmente la PDU de datos NAS, al eNB de destino.

26A.2.-26A.5. Estos pasos son procedimientos normales de cambio de ruta y modificación de portador.

26A.6. El eNB de destino ahora le dice al eNB de origen que libere el contexto de UE enviando un mensaje X2 llamado liberación de contexto de UE.

Si la autenticación del MAC Clot DL en el paso 25 falla, el UE puede realizar acciones tales como no enviar más mensajes o pasar al modo RRC_CONECTADO para autenticar la red, etc.

La variante 1b se ilustra en las figuras 4a a 4b, en el que MAC Clot DL se envía desde la MME al eNB de origen y desde el eNB de origen al eNB de destino y desde el eNB de destino al UE y luego el UE lo verifica con una clave NAS.

Este es un ejemplo aplicable a una situación en la que ocurre un RLF, por ejemplo, durante el envío de datos NAS para optimizaciones de Clot de CP.

Los pasos 1 a 18 son los definidos en las especificaciones 3GPP actuales.

Paso 19. El UE envía un mensaje de RRC al eNB de destino que incluye el MAC Clot UL. El mensaje de RRC puede ser una solicitud de restablecimiento de conexión de RRC, una solicitud de reanudación de RRC o algún otro mensaje de RRC.

Paso 20. El eNB de destino envía un mensaje X2 al eNB de origen, incluido el MAC Clot UL. El mensaje X2 puede ser un mensaje de búsqueda de contexto X2.

Paso 21. El eNB de origen envía un mensaje S1 a la MME que incluye MAC Clot UL y MAC Clot UL de entrada.

Paso 22. Al recibir el MAC Clot UL y el MAC Clot UL de entrada, la MME verifica el MAC Clot UL realizando el mismo cálculo que realizó el UE y comparándolo con el MAC Clot UL recibido. Si la verificación tiene éxito, la MME genera MAC Clot DL como se describe arriba usando MAC Clot DL de entrada y MAC Clot DL de clave y el procesamiento continúa en el paso 23, donde la MME envía un mensaje S1 indicando éxito al eNB de origen e incluye MAC Clot DL. Si la verificación no tiene éxito, la MME envía un mensaje S1 que indica error al eNB de origen. El eNB de origen envía entonces una respuesta de contexto de UE X2 que indica fallo. El fallo activará el eNB de destino para liberar la conexión de RRC (no ilustrada).

Paso 23. La MME envía un mensaje de respuesta de verificación S1 al eNB de origen indicando éxito. El mensaje incluye el MAC Clot DL. El mensaje puede incluir además MAC Clot DL de entrada.

Paso 24. El eNB de origen envía una respuesta de contexto de UE al eNB de destino. El mensaje incluye el MAC Clot DL. El mensaje puede incluir además MAC Clot DL de entrada.

Paso 25. El eNB de destino envía un mensaje de restablecimiento de conexión de RRC al UE. El mensaje incluye el MAC Clot DL. El mensaje puede incluir además MAC Clot DL de entrada.

Paso 26. Al recibir el mensaje de restablecimiento de conexión de RRC, el UE autentica el MAC Clot DL usando MAC Clot DL de entrada y MAC Clot DL de clave como se describe anteriormente.

Paso 27A. Si la autenticación de MAC Clot DL tiene éxito

27A.1. El UE envía un mensaje de restablecimiento de conexión de RRC completo, que contiene opcionalmente la PDU de datos NAS al eNB de destino.

27A.2.-27A.5. Estos pasos son procedimientos normales de cambio de ruta y modificación de portador.

27A.6. El eNB de destino ahora le dice al eNB de origen que libere el contexto de UE enviando un mensaje X2 llamado liberación de contexto de UE.

Si la autenticación del MAC Clot DL en el paso 25 falla, entonces el UE puede realizar acciones como no enviar más mensajes o hacer la transición al modo RRC_CONECTADO para autenticar la red, etc.

La variante 2a se ilustra en la figura 5, en la que el MAC Clot DL se envía desde la MME al eNB de destino en un mensaje de acuse de recibo de solicitud de cambio de ruta de SIAP. El MAC Clot DL se envía desde el eNB de destino al UE.

Esta variante se basa en un mensaje SIAP existente denominado acuse de recibo de solicitud de cambio de ruta que se envía desde la MME al eNB de destino. El acuse de recibo de solicitud de cambio de ruta se modifica para poder transportar el MAC Clot DL y el MAC Clot DL de entrada. Debe ser obvio para el experto en la materia que el orden de los pasos, mensajes y campos podría modificarse; mensajes combinados; campos colocados en diferentes mensajes, etc.; para lograr el mismo efecto.

Los pasos 1 a 17 son los mismos que los descritos anteriormente en relación con la figura 3a.

Los pasos 18 a 19 son también los mismos que los descritos anteriormente en relación con la figura 3a, pero también se muestran en la figura 5 para completar el procedimiento de restablecimiento de conexión de RRC.

Paso 20. El eNB de destino solicita al eNB de origen que envíe el contexto del UE. Un mensaje X2 existente llamado solicitud de recuperación de contexto de UE puede adaptarse según sea necesario (por ejemplo, usando Restablecer identidad de UE en lugar de Reanudar identidad).

Paso 21. El eNB de origen envía el contexto del UE al eNB de destino. Un mensaje X2 existente llamado respuesta de recuperación de contexto de UE puede adaptarse según sea necesario.

Paso 22. El eNB de destino envía un mensaje de restablecimiento de conexión de RRC al UE.

Paso 23. El UE envía un mensaje de restablecimiento de conexión de RRC completo, que contiene opcionalmente la PDU (unidad de datos de protocolo) de datos NAS al eNB de destino.

Paso 24. El eNB de destino envía una solicitud de cambio de ruta a la MME. En la solicitud de cambio de ruta, el eNB de destino incluye MAC Clot UL y MAC Clot UL de entrada. Como se indicó anteriormente, MAC Clot UL de entrada puede incluir la identidad de la célula de destino. El eNB de destino recibió el MAC Clot UL en el paso 19.

El MAC CloT UL de entrada puede incluir información que el eNB de destino recibió en el paso 19 y/o el paso 21, y/o la propia información del eNB de destino. La solicitud de cambio de ruta puede contener la información del UE que permite a la MME identificar el contexto del UE en la MME. La información de ese UE se denomina hoy "ID de SIAP de UE de MME de origen" que el eNB de destino puede proporcionar a partir de la información que recibió en el paso 23.

Paso 25. La MME autentica el MAC CloT UL, por ejemplo, usando MAC CloT UL de entrada y MAC CloT UL de clave como entrada para Fun-MAC CloT UL. El MAC CloT UL de clave es en una realización lo mismo que el MAC CloT DL de clave, es decir, la clave de integridad NAS que puede ser derivada por separado por la MME y el UE respectivamente basándose en KASME, como es conocido por el experto en la técnica.

A continuación, por simplicidad, solo se describen con más detalle los pasos relevantes para la presente solución, que son, si la autenticación en el paso 25 tiene éxito:

Paso 26. La MME genera MAC CloT DL como se describe anteriormente usando MAC CloT DL de entrada y MAC CloT DL de clave. Algunos elementos de MAC CloT DL de entrada, como la identidad de la célula de destino (ID de célula), pueden obtenerse de MAC CloT UL de entrada.

Paso 27. La MME envía un mensaje S1, mensaje de acuse de recibo de solicitud de cambio de ruta, que indica éxito al eNB de destino y el mensaje de acuse de recibo de solicitud de cambio de ruta se adapta para incluir MAC CloT DL y MAC CloT DL de entrada.

Paso 28. El eNB de destino ahora sabe que el MAC CloT UL enviado por el UE y mencionado en pasos anteriores es auténtico. El eNB de destino envía el MAC CloT DL y el MAC CloT DL de entrada al UE en un mensaje de RRC, por ejemplo poniéndolos en el campo DedicatedInfoNAS del mensaje de transferencia de información DL del procedimiento de transferencia de información de RRC DL. También se puede introducir un nuevo tipo de procedimiento de RRC para este propósito particular de transportar el MAC CloT DL al UE, por ejemplo, confirmación de restablecimiento de RRC.

Paso 29. El UE autentica el MAC CloT DL usando el MAC CloT DL de entrada y el MAC CloT DL de clave como entrada al Fun-MAC CloT DL.

Si la autenticación del MAC CloT DL en el paso 27 falla, entonces el UE puede realizar acciones tales como no enviar más mensajes o pasar al modo RRC_CONECTADO para autenticar la red, etc.

La variante 2b se ilustra en la figura 6, en la que el MAC CloT DL se envía desde la MME al eNB de destino en un nuevo mensaje SIAP y desde el eNB de destino al UE.

Esta variante se basa en un nuevo mensaje SIAP (denominado solicitud de verificación de MAC) que se envía desde el eNB de destino a la MME. El mensaje de solicitud de verificación de MAC puede transportar MAC CloT UL y MAC CloT UL de entrada. De manera similar, los nuevos mensajes SIAP, denominados acuse de recibo de verificación de MAC y fallo de verificación de MAC, que se envían desde la MME al eNB de destino, se usan para indicar respectivamente que el MAC CloT UL era auténtico o no auténtico. El nuevo mensaje acuse de recibo de verificación de MAC de SIAP lleva el MAC CloT DL y el MAC CloT DL de entrada desde la MME al eNB de destino. El eNB de destino incluye el MAC CloT DL y el MAC CloT DL de entrada al UE en un mensaje de restablecimiento de conexión de RRC. Debe ser obvio para una persona experta en la técnica notar que el orden de los pasos, mensajes, campos podría modificarse; mensajes combinados; campos colocan diferentes mensajes, etc. para lograr el mismo efecto.

Los pasos 1 a 17 son los mismos que se explicaron anteriormente en relación con la figura 3.

Los pasos 18 a 19 también son los mismos que se explicaron anteriormente, pero se ilustran para completar el procedimiento de restablecimiento de conexión de RRC.

Paso 20. El eNB de destino solicita al eNB de origen que envíe el contexto del UE. Un mensaje X2 existente llamado Solicitud de recuperación de contexto de UE puede adaptarse según sea necesario, por ejemplo, usando Restablecer identidad de UE en lugar de Reanudar identidad.

Paso 21. El eNB de origen envía el contexto del UE al eNB de destino. Un mensaje X2 existente llamado recuperar respuesta de contexto de UE puede adaptarse según sea necesario. El contexto del UE le dice al eNB de destino la MME correspondiente en la que está registrado el UE.

Paso 22. El eNB de destino envía un mensaje en forma de una solicitud de verificación de MAC a la MME identificada en el paso 21. En la solicitud de verificación de MAC, el eNB de destino incluye MAC CloT UL y MAC CloT UL de entrada. El eNB de destino recibió el MAC CloT UL en el paso 19. El MAC CloT UL de entrada puede incluir información que el eNB de destino recibió en el paso 19 y/o el paso 21, y/o la propia información del eNB de

destino Tal información incluida en MAC CloT UL de entrada puede ser la identidad de la célula de destino, que por lo tanto se ha usado como entrada junto con al menos la clave de integridad NAS para generar el token de autenticación UL MAC CloT UL. La solicitud de verificación de MAC también puede contener información del UE que permite a la MME identificar el contexto del UE en la MME. Esa información del UE puede ser, por ejemplo, el ID de SIAP de UE de MME que el eNB de destino recibió del eNB de origen en el paso 21.

Paso 23. La MME autentica el MAC CloT UL usando MAC CloT UL de entrada y MAC CloT UL de clave (por ejemplo, la misma clave de integridad NAS usada como MAC CloT DL de clave) como entrada para Fun-MAC CloT UL. En otras palabras, el resultado de Fun-MAC CloT UL se compara con el MAC CloT UL recibido para una verificación del MAC CloT UL recibido.

A continuación, para simplificar, solo se describen con más detalle los pasos relevantes para esta variante, que son, si la autenticación en el paso 23 tiene éxito:

Paso 24. La MME genera MAC CloT DL como se describió anteriormente usando MAC CloT DL de entrada y MAC CloT DL de clave. Algunos elementos de MAC CloT DL de entrada, como la identidad de la célula de destino, pueden obtenerse de MAC CloT UL de entrada. La MME envía un mensaje S1 (mensaje de acuse de recibo de verificación de MAC) que indica el éxito al eNB de destino e incluye MAC CloT DL y MAC CloT DL de entrada.

Paso 25. La MME envía un mensaje de acuse de recibo de solicitud de verificación de MAC al eNB de destino. El mensaje incluye MAC CloT DL y, opcionalmente, también MAC CloT DL de entrada. El eNB de destino ahora sabe que el MAC CloT UL mencionado en pasos anteriores es auténtico.

Paso 26. El eNB de destino envía un mensaje de restablecimiento de conexión de RRC al UE. Este mensaje incluye MAC CloT DL y puede incluir MAC CloT DL de entrada.

Paso 27. El UE autentica el MAC CloT DL usando el MAC CloT DL de entrada y el MAC CloT DL de clave como entrada al Fun-MAC CloT DL.

Paso 28. Si la autenticación de MAC CloT DL en el paso 27 tiene éxito, entonces el UE envía un mensaje de restablecimiento de conexión de RRC completo, que contiene opcionalmente la PDU de datos NAS al eNB de destino.

Si la autenticación del MAC CloT DL en el paso 27 falla, entonces el UE puede realizar algunas acciones tales como no enviar más mensajes o pasar al modo RRC_CONECTADO para autenticar la red, etc.

Un método, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE y un eNB de destino se presenta con referencia a la figura 7A. El método lo realiza el UE 1 y comprende recibir S100 un mensaje de restablecimiento de conexión de RRC desde un eNB 3 de destino, por ejemplo, para la optimización de CP IoT, incluyendo el mensaje de restablecimiento de conexión de RRC un token de autenticación DL que ha sido generado por la MME 4 y que ha tenido una clave de integridad NAS como entrada, y autenticar S110 el token de autenticación DL recibido.

El mensaje de restablecimiento de conexión de RRC que incluye el token de autenticación DL puede incluir opcionalmente también un MAC CloT DL de entrada, y el token de autenticación DL recibido puede autenticarse usando el MAC CloT DL de entrada recibido y la clave de integridad NAS.

El mensaje de RRC puede ser un mensaje de transferencia de información DL de RRC que incluye MAC CloT DL y, opcionalmente, MAC CloT DL de entrada, y el MAC CloT DL recibido puede autenticarse usando MAC CloT DL de entrada y MAC CloT DL de clave.

En un paso opcional S80 antes de S100, el UE calcula un token de autenticación UL (denominado UL AT en la figura 7A) con la clave de integridad NAS como entrada, y en un paso opcional S90 envía una solicitud de restablecimiento de conexión de RRC que incluye el token de autenticación UL al eNB 3 de destino. El token de autenticación UL puede calcularse con la identidad de la célula de destino como entrada y la identidad de la célula de destino puede incluirse en la solicitud de restablecimiento de conexión de RRC, por ejemplo, como parte de MAC UL de entrada.

Un método, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE y un eNB de destino, por ejemplo, para la optimización de CP IoT, se presenta con referencia a la figura 7B. El método lo realiza el eNB 3 de destino y comprende recibir S300, desde la MME 4, un mensaje que incluye un token de autenticación DL que ha sido generado por la MME, en el que el token de autenticación DL se ha generado con una clave de integridad de estrato sin acceso como entrada, y enviar S310 un mensaje de restablecimiento de conexión de RRC al UE 1, incluyendo el mensaje de restablecimiento de conexión de RRC el token de autenticación DL.

En un paso opcional S280 antes de S300, el eNB de destino recibe del UE 1 una solicitud de restablecimiento de conexión de RRC que incluye un token de autenticación UL, en el que el token de autenticación UL ha sido

calculado por el UE 1 con la clave de integridad NAS como entrada. El token de autenticación UL, en una realización junto con el MAC CIoT UL de entrada que incluye la identidad de la célula de destino. En un paso opcional S290 antes de S300, el eNB de destino envía/reenvía el token de autenticación UL a la MME 4, opcionalmente con el MAC CIoT UL de entrada que incluye la identidad de la célula de destino.

5 El mensaje enviado de restablecimiento de conexión de RRC puede incluir un MAC CIoT DL de entrada.

El mensaje recibido puede ser un mensaje de acuse de recibo de solicitud de cambio de ruta que incluye MAC CIoT DL de entrada.

10 El mensaje recibido puede ser un mensaje de acuse de recibo de verificación de MAC que incluye un MAC CIoT DL de entrada.

15 Un método, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE y un eNB de destino, por ejemplo, para la optimización de CP IoT, se presenta con referencia a la figura 7C. El método se realiza en un eNB 2 de origen y comprende obtener S200 un token de autenticación DL que se ha generado con una clave de integridad NAS como entrada, y enviar S210 un mensaje de respuesta a un eNB 3 de destino, incluyendo el mensaje de respuesta el token de autenticación DL obtenido.

20 La obtención S200 puede comprender generar el token de autenticación DL, o recibir un mensaje de respuesta de verificación S1 desde una MME 4, la respuesta de verificación S1 recibida incluye el token de autenticación DL y opcionalmente también MAC CIoT DL de entrada.

25 El mensaje de respuesta puede ser un mensaje de respuesta de contexto de UE X2.

Un método, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE y un eNB de destino, por ejemplo, para la optimización de CP IoT, se presenta con referencia a la figura 7D. El método lo realiza la MME 4 y comprende generar S400 un token de autenticación DL con una clave de integridad NAS como entrada, y enviar S410 un mensaje que incluye el token de autenticación DL generado al eNB 3 de destino. El token de autenticación DL puede generarse también con la identidad de la célula de destino como entrada.

35 En un paso opcional S380 antes de S400, la MME recibe un token de autenticación UL del eNB 3 de destino, dicho token de autenticación UL ha sido generado por el UE 1 con la clave de integridad NAS como entrada, y en un paso opcional S390 verifica el token de autenticación UL, por ejemplo calculando un segundo token de autenticación UL de la misma manera que lo hizo el UE (por ejemplo, con la clave de integridad NAS y la identidad de la célula de destino como entrada) y luego comparando el segundo token de autenticación UL con el recibido del eNB de destino.

40 El mensaje puede ser un mensaje de acuse de recibo de solicitud de cambio de ruta e incluye MAC CIoT DL de entrada.

El mensaje puede ser un mensaje de acuse de recibo de verificación de MAC que incluye MAC CIoT DL de entrada.

45 Un UE 1, de acuerdo con una realización, para restablecer una conexión de RRC entre el UE 1 y el eNB 3 de destino, se presenta con referencia a la figura 8. El UE 1 comprende un procesador 10 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el UE reciba un mensaje de restablecimiento de conexión de RRC de un eNB 3 de destino, incluyendo el mensaje de restablecimiento de conexión de RRC un token de autenticación DL que ha sido generado por la MME 4 y tiene una clave de integridad NAS como entrada y autentica el token de autenticación DL recibido.

50 El mensaje de restablecimiento de conexión de RRC puede incluir opcionalmente MAC CIoT DL de entrada, y el token de autenticación DL recibido puede autenticarse usando MAC CIoT DL de entrada y la clave de integridad NAS.

55 Un eNB de origen, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE 1 y un eNB 3 de destino, se presenta con referencia a la figura 9. El eNB 2 de origen comprende un procesador 20 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de origen obtenga un token de autenticación DL que se ha generado con una clave de integridad NAS como entrada, y envíe un mensaje de respuesta al eNB 3 de destino, incluyendo el mensaje de respuesta el token de autenticación DL obtenido.

El mensaje de respuesta puede ser un mensaje de respuesta de contexto de UE X2.

65 Un eNB de destino, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE 1 y un eNB 3 de destino, se presenta con referencia a la figura 10. El eNB 3 de destino comprende un procesador 30 y un

producto de programa informático. El programa informático produce almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de destino reciba de la MME 4 un mensaje que incluye un token de autenticación DL que ha sido generado por la MME 4, en el que el token de autenticación DL se ha generado con un clave de integridad NAS como entrada; y envíe un mensaje de restablecimiento de conexión de RRC a un UE 1, incluyendo el mensaje de restablecimiento de conexión de RRC el token de autenticación DL. El token de autenticación DL ha sido calculado en una realización por la MME 4 con la identidad de una célula de destino como entrada.

El mensaje de restablecimiento de conexión de RRC enviado incluye opcionalmente MAC CloT DL de entrada, que puede incluir la identidad de la célula de destino.

El mensaje recibido puede ser un mensaje de acuse de recibo de solicitud de cambio de ruta que incluye el MAC CloT DL de entrada.

El mensaje recibido puede ser un mensaje de acuse de recibo de verificación de MAC que incluye MAC CloT DL de entrada.

Una MME, de acuerdo con una realización, para restablecer una conexión de RRC entre un UE 1 y un eNB 3 de destino, se presenta con referencia a la figura 11. La MME 4 comprende un procesador 40 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la MME genere un token de autenticación DL con una clave de integridad NAS como entrada y envíe un mensaje que incluye el token de autenticación DL generado al eNB 3 de destino.

El mensaje puede ser un mensaje de acuse de recibo de solicitud de cambio de ruta, el mensaje incluye una MAC CloT DL de entrada.

El mensaje puede ser un mensaje de acuse de recibo de verificación de MAC, incluyendo el mensaje MAC CloT DL de entrada.

La figura 8 es un diagrama esquemático que muestra algunos componentes del UE 1. El procesador 10 puede proporcionarse usando cualquier combinación de una o más de una unidad central de procesamiento adecuada, CPU, multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado de aplicación específica, etc., capaz de ejecutar instrucciones de software de un programa informático 14 almacenado en una memoria. Por tanto, se puede considerar que la memoria es o forma parte del producto 12 de programa informático. El procesador 10 puede configurarse para ejecutar métodos descritos en el presente documento con referencia a la figura 7A.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM. La memoria también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

También puede proporcionarse un segundo producto 13 de programa informático en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 10. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM, y también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquier combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota. La memoria de datos puede, por ejemplo, albergar otras instrucciones de software 15, para mejorar la funcionalidad del UE 1.

El UE 1 puede comprender además una interfaz 11 de entrada/salida (I/O) que incluye, por ejemplo, una interfaz de usuario. El UE 1 puede comprender además un receptor configurado para recibir señalización de otros nodos y un transmisor configurado para transmitir señalización a otros nodos (no ilustrado). Se omiten otros componentes del UE 1 para no oscurecer los conceptos presentados en el presente documento.

La figura 12 es un diagrama esquemático que muestra bloques funcionales del UE 1. Los módulos pueden implementarse solo como instrucciones de software, como un programa informático que se ejecuta en el servidor de caché o solo como hardware, como circuitos integrados de aplicación específica, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc. o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden implementarse mediante software y otros mediante hardware. Los módulos corresponden a los pasos de los métodos ilustrados en la figura 7A, que comprende una unidad 60 de gestión de determinación y una unidad 61 de gestión de comunicación. En las realizaciones donde uno o más de los módulos son implementados por un programa informático, se entenderá que estos módulos no corresponden necesariamente a módulos de proceso, sino que pueden escribirse como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, ya que algunos lenguajes de programación típicamente no contienen módulos de proceso.

El gestor 60 de determinación permite restablecer una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso S110 de verificación de la figura 7A, es decir, la autenticación del token de autenticación DL recibido. Este módulo puede, por ejemplo, ser implementado por el procesador 10 de la figura 8, cuando se ejecuta el programa informático.

El gestor 61 de comunicación permite restablecer una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso S100 de recepción de la figura 7A. Este módulo puede, por ejemplo, ser implementado por el procesador 10 de la figura 12, cuando se ejecuta el programa informático.

La figura 9 es un diagrama esquemático que muestra algunos componentes del eNB 2 de origen. El procesador 20 se puede proporcionar usando cualquier combinación de una o más de una unidad central de procesamiento adecuada, CPU, multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado de aplicación específica, etc., capaz de ejecutar instrucciones de software de un programa informático 24 almacenado en una memoria. Por tanto, se puede considerar que la memoria es o forma parte del producto 22 de programa informático. El procesador 20 puede configurarse para ejecutar los métodos descritos en el presente documento con referencia a la figura 7B.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM. La memoria también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

También puede proporcionarse un segundo producto 23 de programa informático en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 20. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM, y también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquier combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota. La memoria de datos puede, por ejemplo, albergar otras instrucciones de software 25, para mejorar la funcionalidad del eNB 2 de origen.

El eNB 2 de origen puede comprender además una interfaz 21 de entrada/salida (I/O) que incluye, por ejemplo, una interfaz de usuario. El eNB 2 de origen puede comprender además un receptor configurado para recibir señalización de otros nodos y un transmisor configurado para transmitir señalización a otros nodos (no ilustrado). Otros componentes del eNB 2 de origen se omiten para no oscurecer los conceptos presentados en el presente documento.

La figura 13 es un diagrama esquemático que muestra bloques funcionales del eNB 2 de origen. Los módulos pueden implementarse solo como instrucciones de software, como un programa informático que se ejecuta en el servidor de caché o solo como hardware, como circuitos integrados de aplicación específica, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc. o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden implementarse mediante software y otros mediante hardware. Los módulos corresponden a los pasos de los métodos ilustrados en la figura 7C, que comprende una unidad 70 de gestión de determinación y una unidad 71 de gestión de comunicación. En las realizaciones donde uno o más de los módulos son implementados por un programa informático, se entenderá que estos módulos no corresponden necesariamente a módulos de proceso, sino que pueden escribirse como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, ya que algunos lenguajes de programación típicamente no contienen módulos de proceso.

El gestor 70 de determinación permite restablecer una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso S200 de obtención de la figura 7C. Este módulo puede, por ejemplo, ser implementado por el procesador 20 de la figura 9, cuando se ejecuta el programa informático.

El gestor 71 de comunicación permite restablecer una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso S210 de envío de la figura 7C. Este módulo puede, por ejemplo, ser implementado por el procesador 20 de la figura 13, cuando se ejecuta el programa informático.

La figura 10 es un diagrama esquemático que muestra algunos componentes del eNB 3 de destino. El procesador 30 se puede proporcionar usando cualquier combinación de una o más de una unidad central de procesamiento adecuada, CPU, multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado de aplicación específica, etc., capaz de ejecutar instrucciones de software de un programa informático 34 almacenado en una memoria. Por tanto, se puede considerar que la memoria es o forma parte del producto 32 de programa informático. El procesador 30 puede configurarse para ejecutar los métodos descritos en el presente documento con referencia a la figura 7C.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM. La memoria también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

5 También se puede proporcionar un segundo producto 33 de programa informático en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 30. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM, y también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquier
10 combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota. La memoria de datos puede, por ejemplo, albergar otras instrucciones 35 de software, para mejorar la funcionalidad del eNB 3 de destino.

15 El eNB 3 de destino puede comprender además una interfaz 31 de entrada/salida (I/O) que incluye, por ejemplo, una interfaz de usuario. El eNB 3 de destino puede comprender además un receptor configurado para recibir señalización de otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no ilustrado). Otros componentes del eNB 3 de destino se omiten para no oscurecer los conceptos presentados en el presente documento.

20 La figura 14 es un diagrama esquemático que muestra bloques funcionales del eNB 3 de destino. Los módulos pueden implementarse solo como instrucciones de software, como un programa informático que se ejecuta en el servidor de caché o solo como hardware, como circuitos integrados de aplicación específica, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc. o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden implementarse mediante
25 software y otros mediante hardware. Los módulos corresponden a los pasos de los métodos ilustrados en la figura 7B, que comprende una unidad 80 de gestión de determinación y una unidad 81 de gestión de comunicación. En las realizaciones donde uno o más de los módulos son implementados por un programa informático, se entenderá que estos módulos no corresponden necesariamente a módulos de proceso, sino que pueden escribirse como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, ya que algunos lenguajes
30 de programación típicamente no contienen módulos de proceso.

El gestor 81 de comunicación es para permitir restablecer una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso S300 de recepción y al paso 310 de envío de la figura 7B. Este módulo puede, por ejemplo, ser implementado por el procesador 30 de la figura 10, cuando se ejecuta el programa informático.

35 La figura 11 es un diagrama esquemático que muestra algunos componentes de la MME 4. El procesador 40 se puede proporcionar usando cualquier combinación de una o más de una unidad central de procesamiento adecuada, CPU, multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado de aplicación específica, etc., capaz de ejecutar instrucciones de software de un programa informático 44 almacenado en una memoria. Por tanto, se puede considerar que la memoria es o forma parte del producto 42 de programa informático. El procesador 40 puede configurarse para ejecutar métodos descritos en el presente documento con referencia a la
40 figura 7D.

45 La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM. La memoria también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

50 También se puede proporcionar un segundo producto 43 de programa informático en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 40. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM, y también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquier combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota. La memoria de datos puede, por ejemplo, albergar otras instrucciones de software 45, para mejorar la
55 funcionalidad de la MME 4.

La MME 4 puede comprender además una interfaz 41 de entrada/salida (I/O) que incluye, por ejemplo, una interfaz de usuario. La MME 4 puede comprender además un receptor configurado para recibir señalización de otros nodos y un transmisor configurado para transmitir señalización a otros nodos (no ilustrado). Se omiten otros componentes de
60 la MME 4 para no oscurecer los conceptos presentados en el presente documento.

La figura 15 es un diagrama esquemático que muestra bloques funcionales de la MME 4. Los módulos pueden implementarse solo como instrucciones de software, como un programa informático que se ejecuta en el servidor de caché o solo como hardware, como circuitos integrados de aplicación específica, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc. o como una combinación de los mismos. En una
65 realización alternativa, algunos de los bloques funcionales pueden implementarse mediante software y otros

mediante hardware. Los módulos corresponden a los pasos de los métodos ilustrados en la figura 7D, que comprende una unidad 90 de gestión de determinación y una unidad 91 de gestión de comunicación. En las realizaciones donde uno o más de los módulos son implementados por un programa informático, se entenderá que estos módulos no corresponden necesariamente a módulos de proceso, sino que pueden escribirse como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, ya que algunos lenguajes de programación típicamente no contienen módulos de proceso.

El gestor 90 de determinación es para permitir restablecer una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso 400 de generación de la figura 7D. Este módulo puede, por ejemplo, ser implementado por el procesador 40 de la figura. 11, cuando se ejecuta el programa informático.

El gestor 91 de comunicación es para permitir el restablecimiento de una conexión de RRC entre un UE y un eNB de destino. Este módulo corresponde al paso S410 de envío de la figura 7D. Este módulo puede, por ejemplo, ser implementado por el procesador 40 de la figura 11, cuando se ejecuta el programa informático.

La invención se ha descrito principalmente anteriormente con referencia a algunas realizaciones. Sin embargo, como apreciará fácilmente un experto en la técnica, otras realizaciones distintas de las divulgadas anteriormente son igualmente posibles dentro del alcance de la invención, tal como se define mediante las reivindicaciones.

REIVINDICACIONES

- 1.- Un método para restablecer una conexión de control de recurso de radio, RRC, entre un equipo (1) de usuario, UE, y un NodoB (3) de destino evolucionado, eNB de destino, siendo el método realizado por el UE (1) y que comprende:
- 5 recibir (S100) un mensaje de restablecimiento de conexión de RRC desde el eNB (3) de destino, incluyendo el mensaje de restablecimiento de conexión de RRC un token de autenticación de enlace descendente, DL, que ha sido generado por una entidad (4) de gestión de movilidad y ha tenido una clave de integridad de estrato sin acceso y un parámetro de actualización como entrada; y
- 10 autenticar (S110) el token de autenticación DL recibido.
- 2.- El método de acuerdo con la reivindicación 1, que comprende calcular un token de autenticación de enlace ascendente, UL, con la clave de integridad de estrato sin acceso como entrada, y enviar una solicitud de restablecimiento de conexión de RRC que incluye el token de autenticación UL al eNB (3) de destino.
- 15 3.- El método de acuerdo con la reivindicación 2, en el que el token de autenticación UL se calcula con la identidad de una célula de destino como entrada.
- 20 4.- Un método para restablecer una conexión de control de recurso de radio, RRC, entre un equipo (1) de usuario, UE, y un NodoB (3) de destino evolucionado, eNB de destino, siendo realizado el método por el eNB (3) de destino y que comprende:
- 25 recibir (S300), de una entidad (4) de gestión de movilidad, MME, un mensaje que incluye un token de autenticación de enlace descendente, DL, que ha sido generado por la MME (4), en el que el token de autenticación DL se ha generado con una clave de integridad de estrato sin acceso y parámetro de actualización como entrada; y
- 30 enviar (S310) un mensaje de restablecimiento de conexión de RRC al UE (1), incluyendo el mensaje de restablecimiento de conexión de RRC el token de autenticación DL.
- 5.- El método de acuerdo con la reivindicación 4, que comprende recibir del UE (1) una solicitud de restablecimiento de conexión de RRC que incluye un token de autenticación de enlace ascendente, UL, en el que el token de autenticación UL ha sido calculado por el UE (1) con la clave de integridad de estrato sin acceso como entrada.
- 35 6.- El método de acuerdo con la reivindicación 5, en el que el UE (1) ha calculado el token de autenticación UL con la identidad de una célula de destino como entrada.
- 7.- Un método para restablecer una conexión de control de recurso de radio, RRC, entre un equipo (1) de usuario, UE y un NodoB (3) de destino evolucionado, eNB de destino, el método siendo realizado por una entidad (4) de gestión de movilidad, MME, y que comprende:
- 40 generar (S400) un token de autenticación de enlace descendente, DL, con una clave de integridad de estrato sin acceso y un parámetro de actualización como entrada; y
- 45 enviar (S410) un mensaje que incluye el token de autenticación DL generado al eNB (3) de destino.
- 8.- El método de acuerdo con la reivindicación 7, que comprende generar el token de autenticación DL con la identidad de una célula de destino como entrada.
- 50 9.- El método de acuerdo con la reivindicación 7, que comprende
- recibir un token de autenticación de enlace ascendente, UL, desde el eNB de destino, habiendo sido generado dicho token de autenticación UL por el UE (1) con la clave de integridad de estrato sin acceso como entrada, y
- 55 verificar el token de autenticación UL.
- 10.- El método de acuerdo con la reivindicación 9, en el que el token de autenticación UL ha sido generado por el UE (1) con la identidad de una célula de destino como entrada.
- 60 11.- Un equipo (1) de usuario, UE, para restablecer una conexión de control de recurso de radio, RRC, entre el UE (1) y un NodoB (3) de destino evolucionado, eNB de destino, el UE (1) comprendiendo:
- 65 un procesador (10); y

un producto (12, 13) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el UE:

5 reciba un mensaje de restablecimiento de conexión de RRC desde el eNB (3) de destino, incluyendo el mensaje de restablecimiento de conexión de RRC un token de autenticación de enlace descendente, DL, que ha sido generado por una entidad (4) de gestión de movilidad y ha tenido una clave de integridad de estrato sin acceso y un parámetro de actualización como entrada; y

autentique el token de autenticación DL recibido.

10 12.- El UE de acuerdo con la reivindicación 11, en el que el token de autenticación DL ha sido calculado por la entidad (4) de gestión de movilidad con la identidad de una célula de destino como entrada.

15 12.- Un nodo B (3) de destino evolucionado, eNB de destino, para restablecer una conexión de control de recurso de radio, RRC, entre un equipo (1) de usuario, UE y el eNB de destino, comprendiendo el eNB (3) de destino:

un procesador (30); y

20 un producto (32, 33) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de destino:

reciba, de una entidad (4) de gestión de movilidad, MME, un mensaje que incluye un token de autenticación de enlace descendente, DL, que ha sido generado por la MME (4), en el que el token de autenticación DL se ha generado con una clave de integridad de estrato sin acceso y un parámetro de actualización como entrada; y

25 envíe un mensaje de restablecimiento de conexión de RRC al UE (1), incluyendo el mensaje de restablecimiento de conexión de RRC el token de autenticación DL.

30 14.- Una entidad (4) de gestión de movilidad, MME, para restablecer una conexión de control de recurso de radio, RRC, entre un equipo (1) de usuario, UE, y un NodoB (3) de destino evolucionado, eNB de destino, la MME (4) comprendiendo:

un procesador (40); y

35 un producto (42, 43) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la MME:

genere un token de autenticación de enlace descendente, DL, con una clave de integridad de estrato sin acceso y un parámetro de actualización como entrada; y

40 envíe un mensaje que incluya el token de autenticación DL generado al eNB (3) de destino.

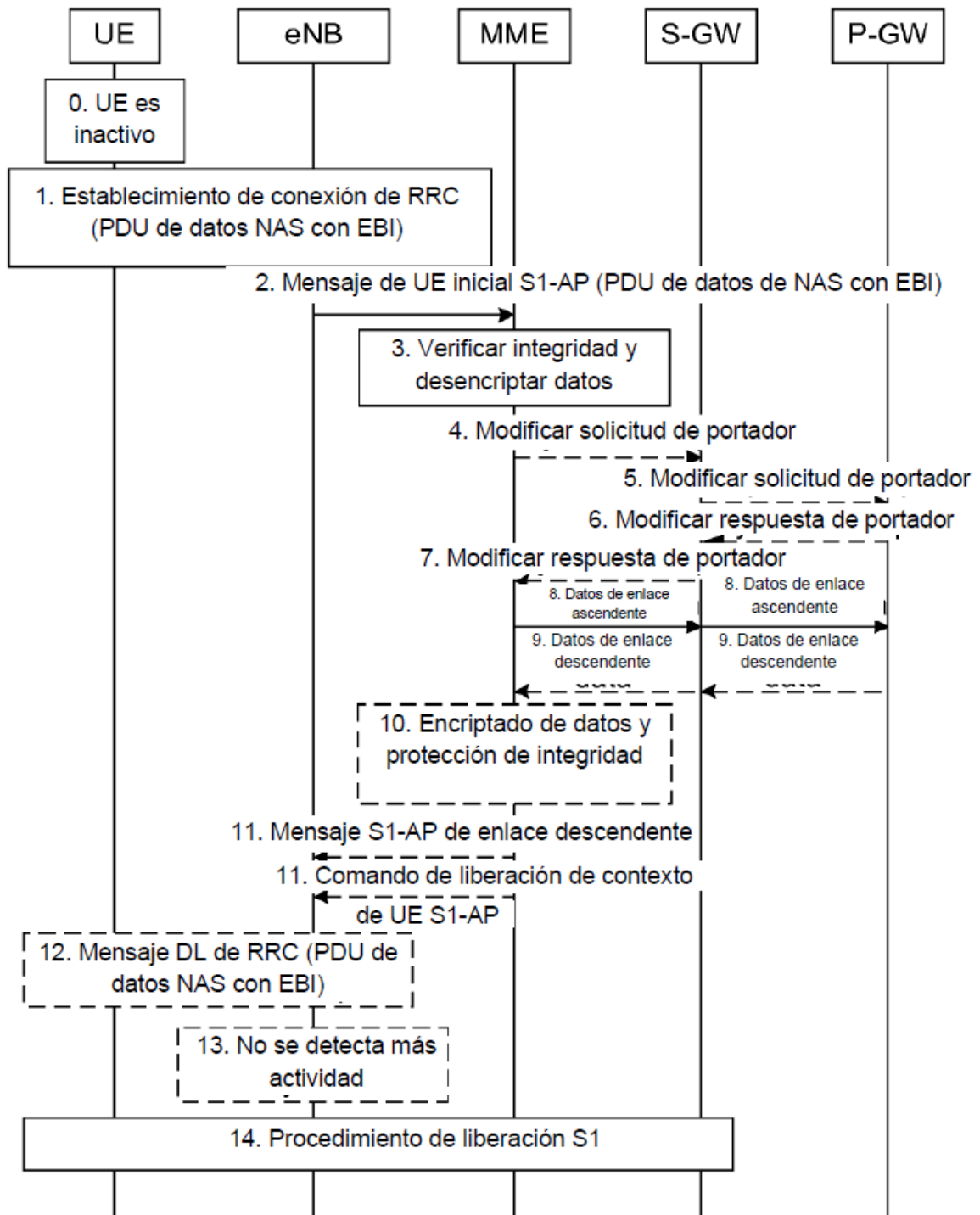


Fig. 1

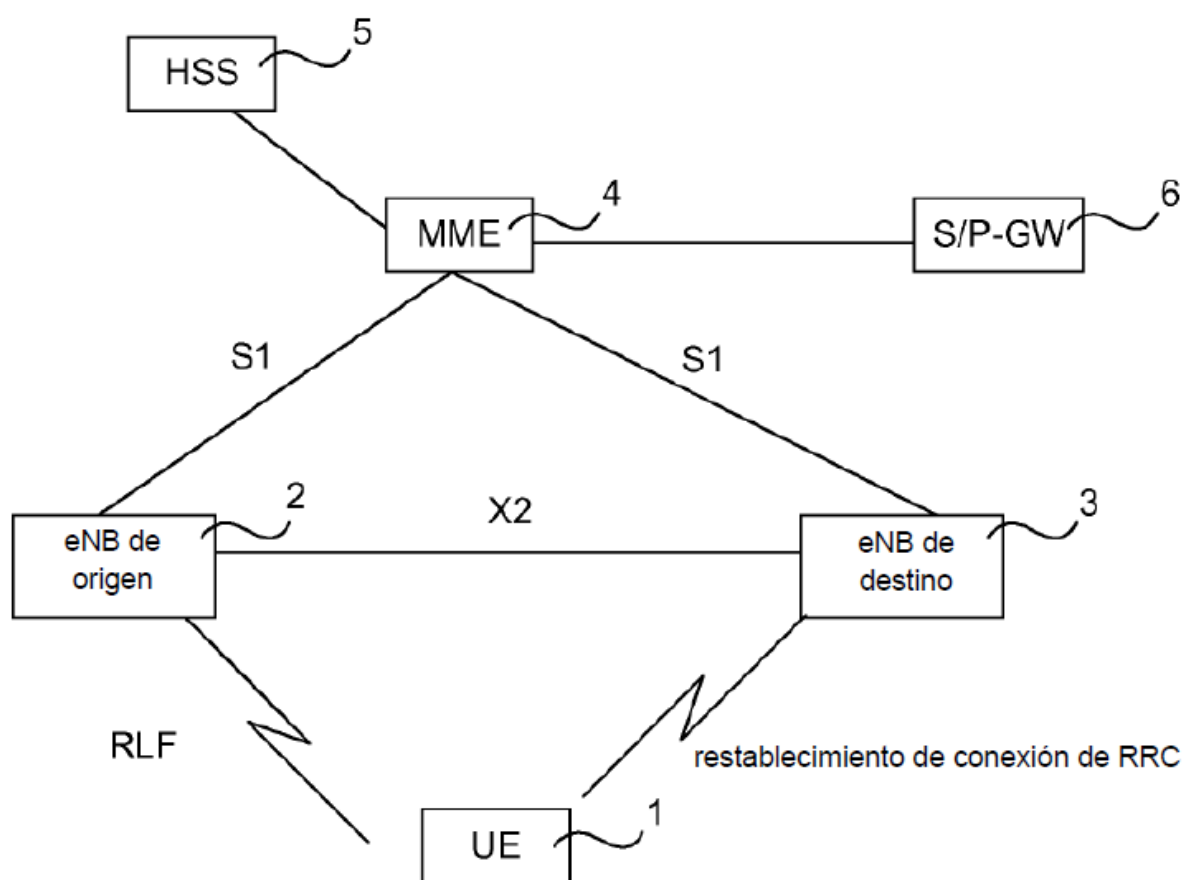


Fig. 2

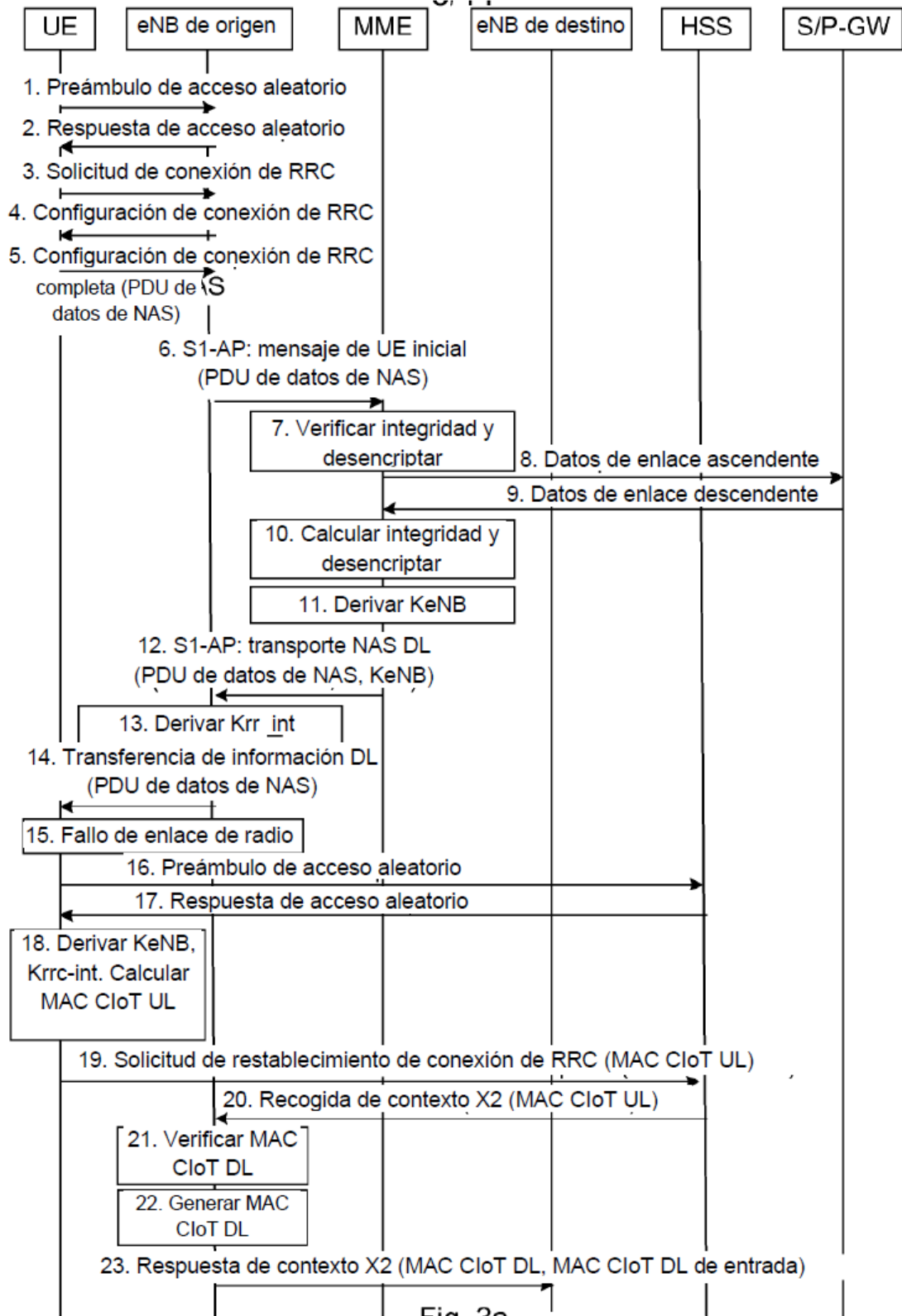


Fig. 3a

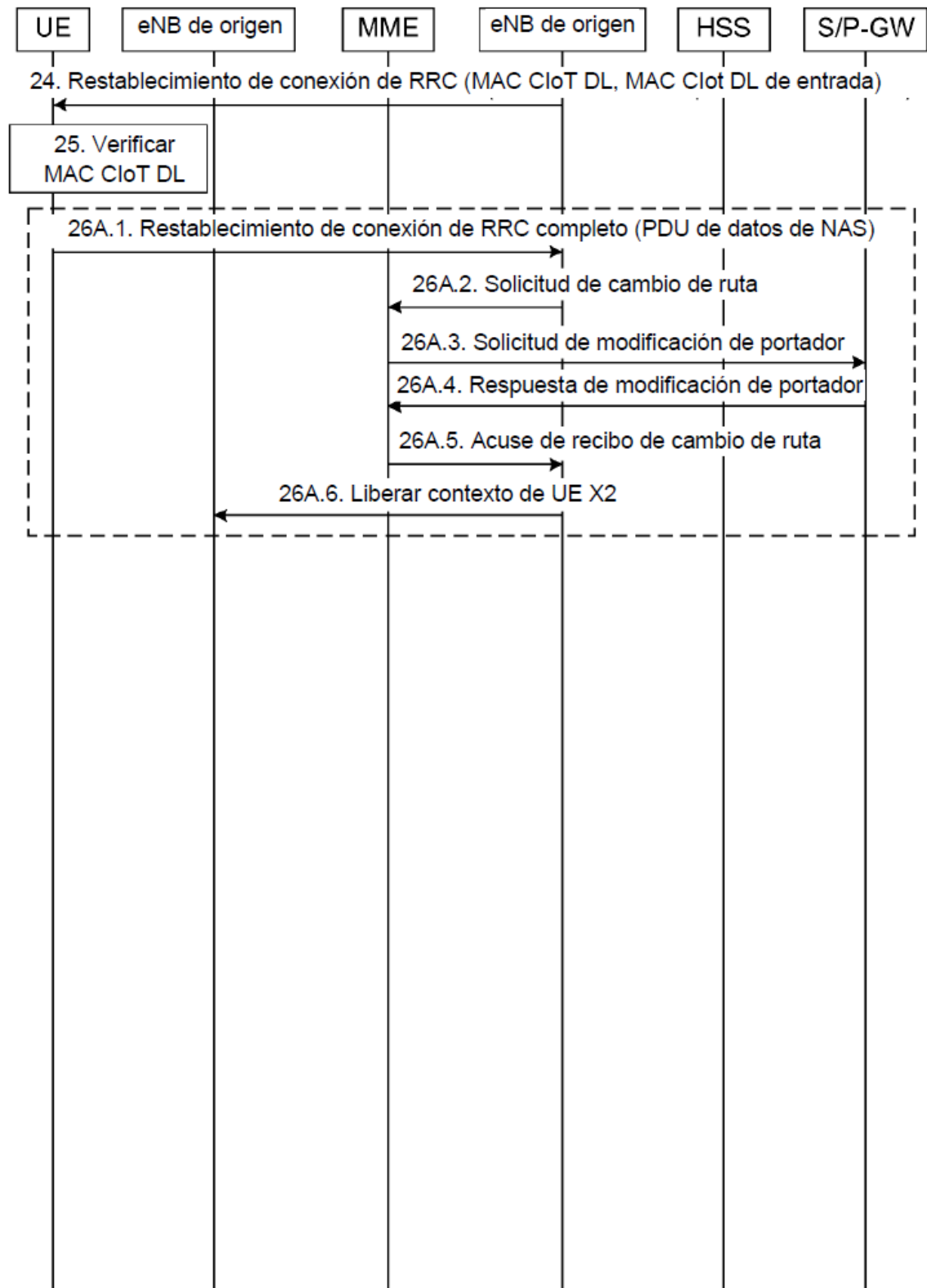
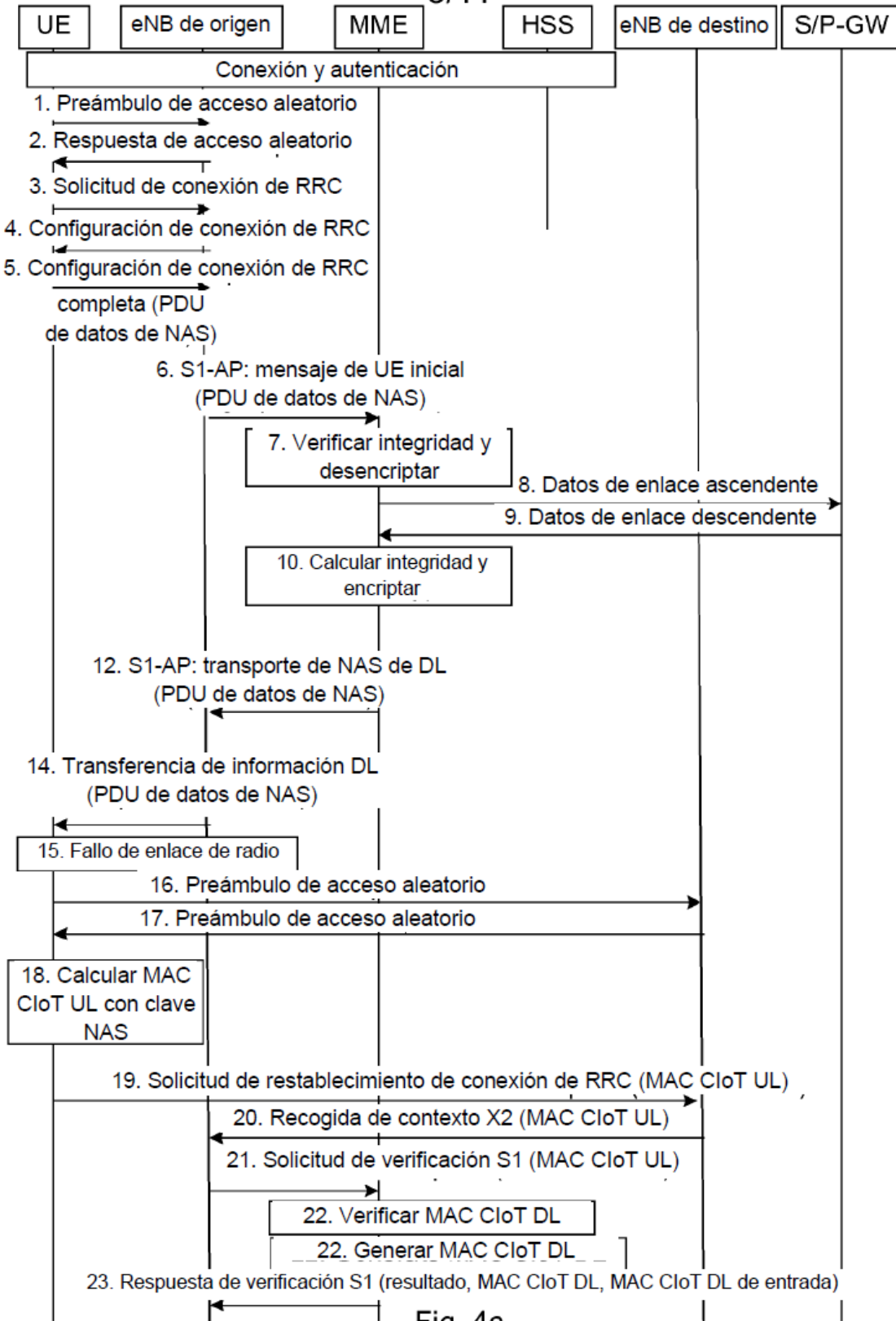


Fig. 3b



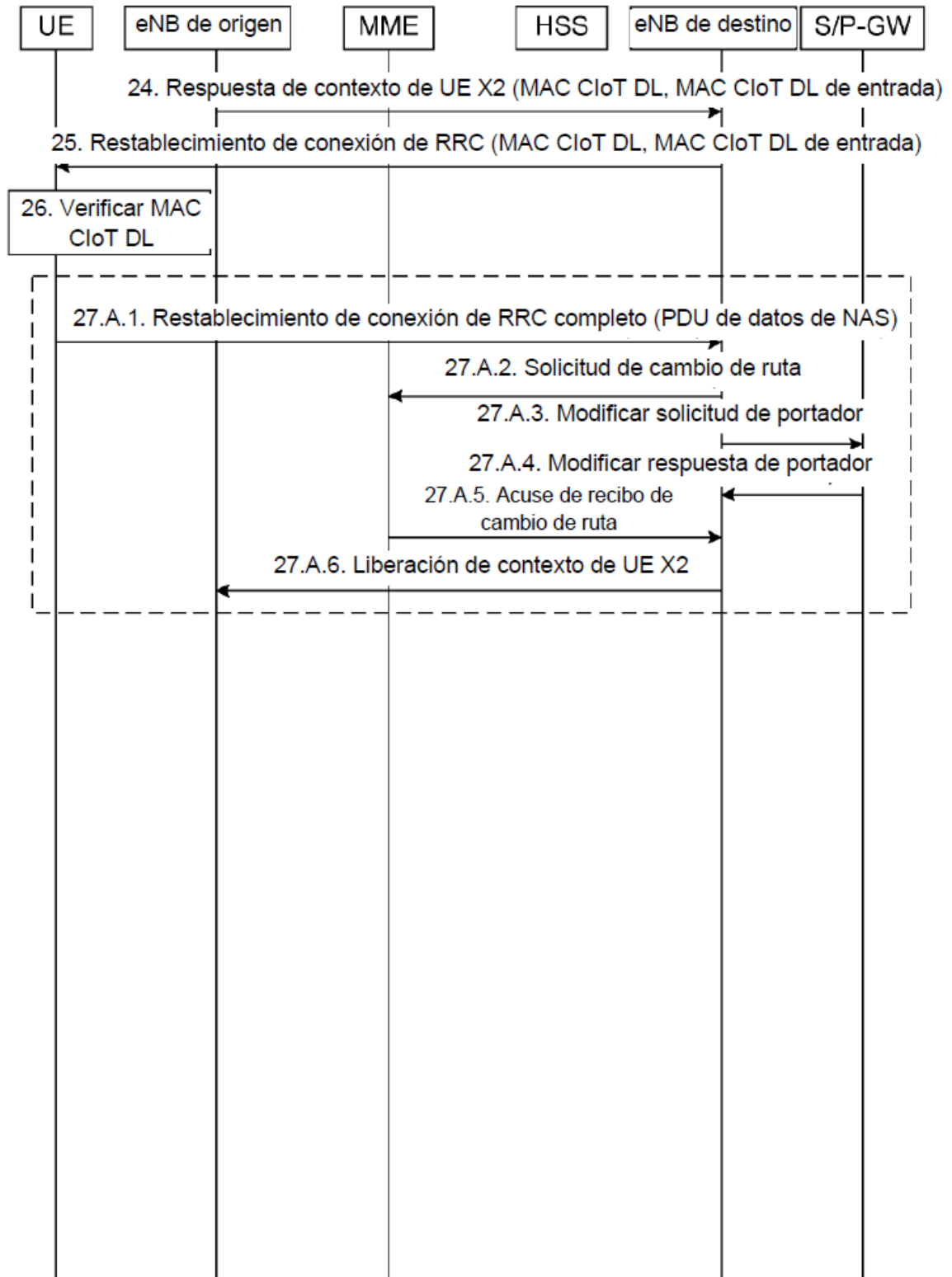


Fig. 4b

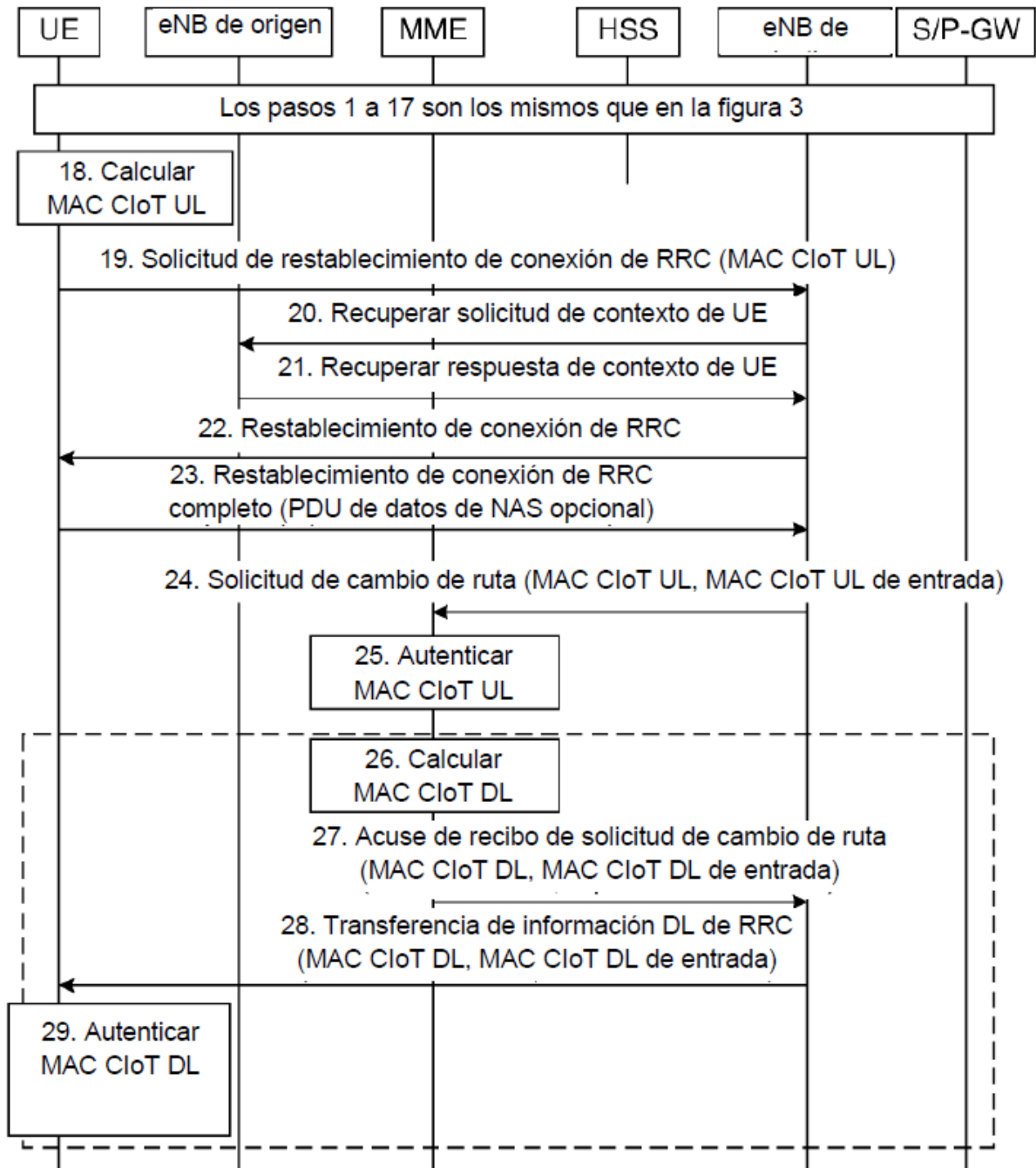


Fig. 5

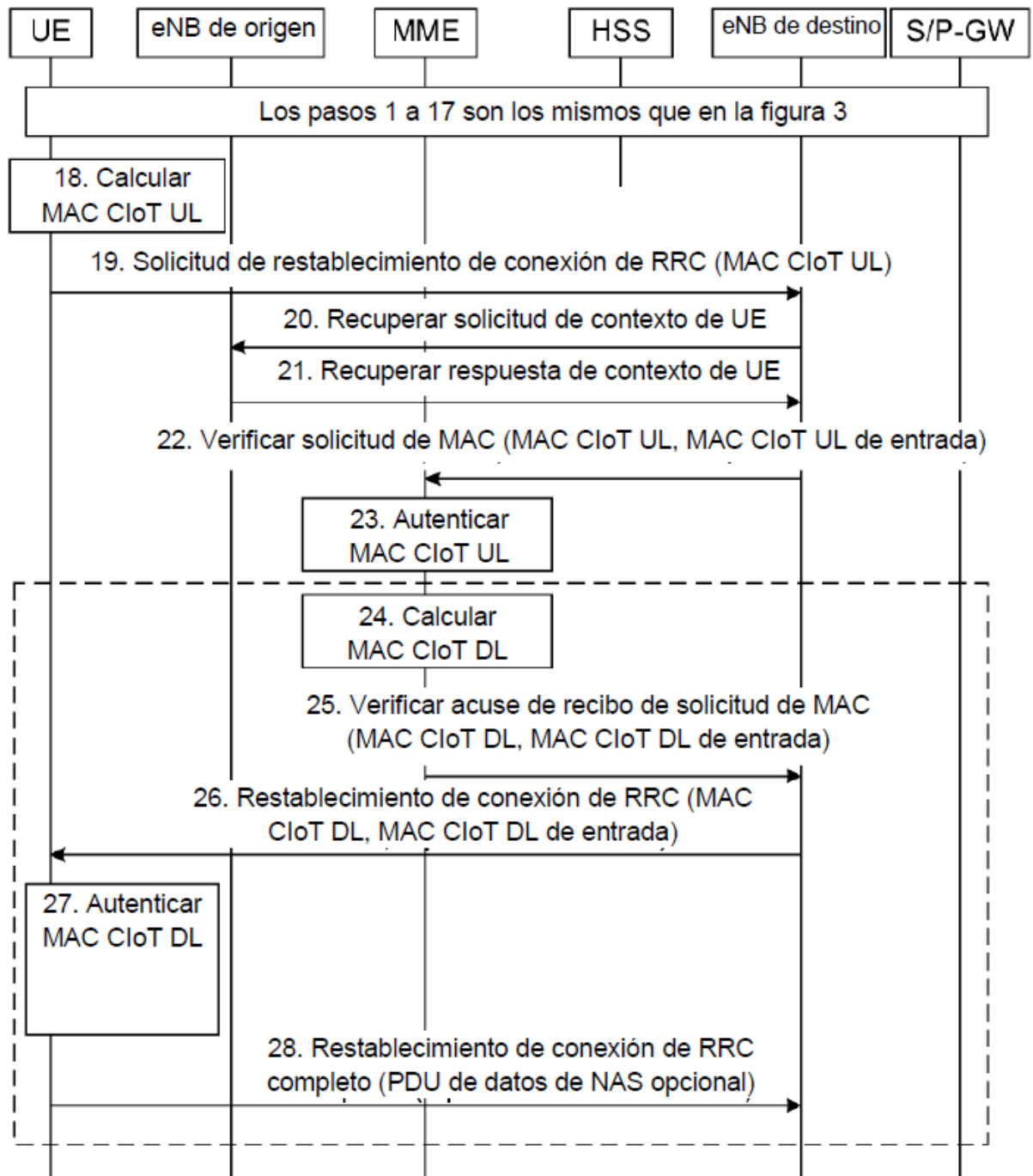


Fig. 6

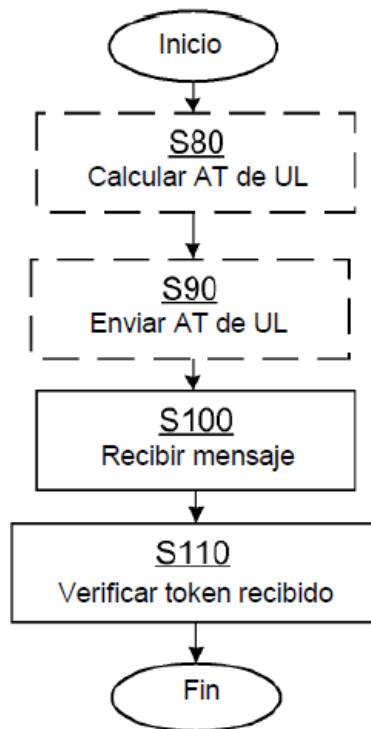


Fig. 7A

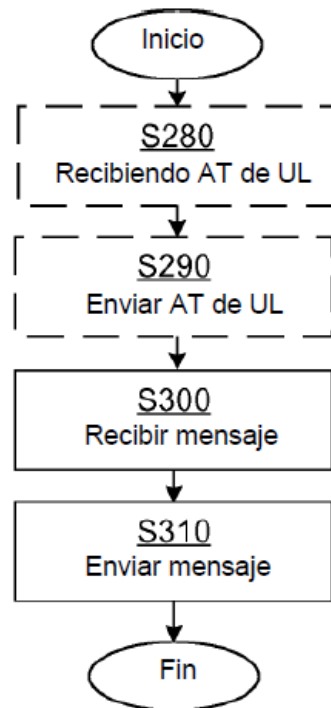


Fig. 7B

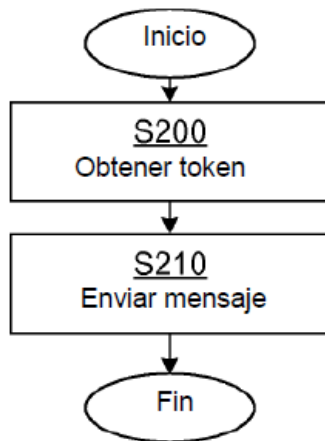


Fig. 7C

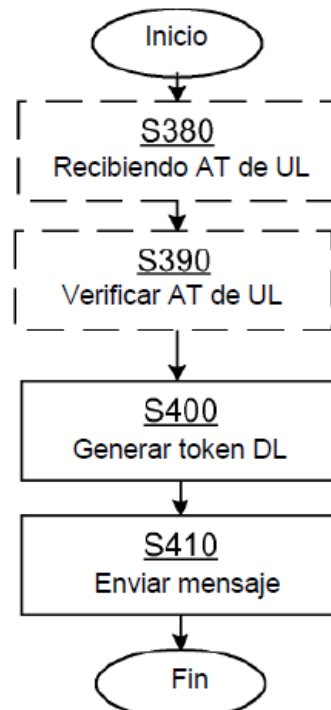


Fig. 7D

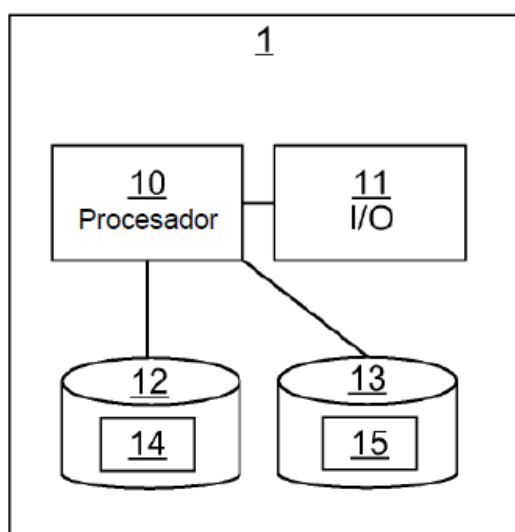


Fig. 8

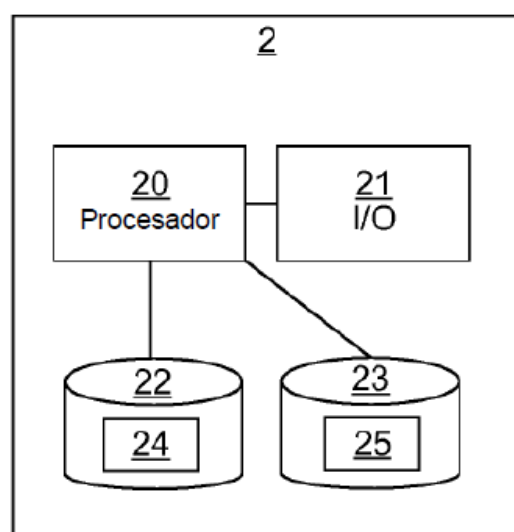


Fig. 9

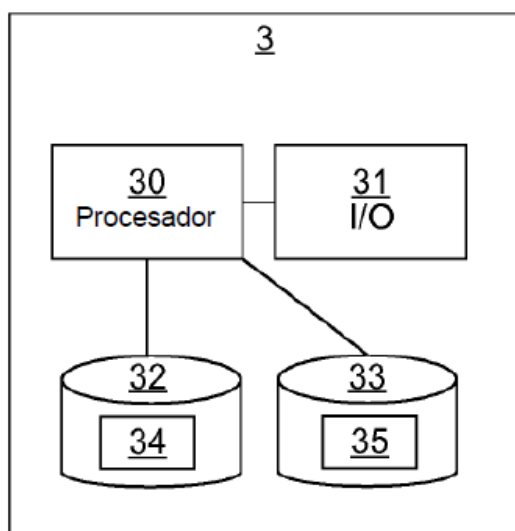


Fig. 10

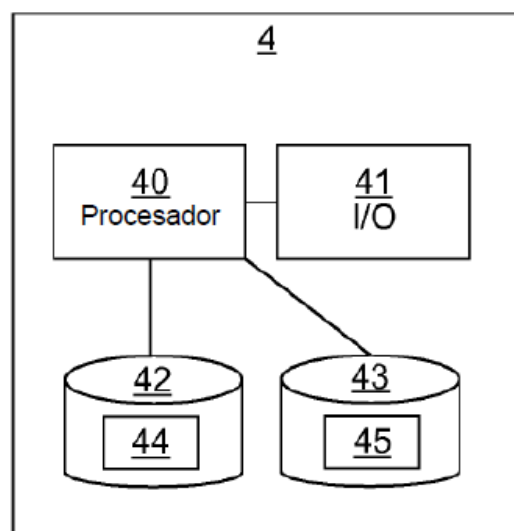


Fig. 11

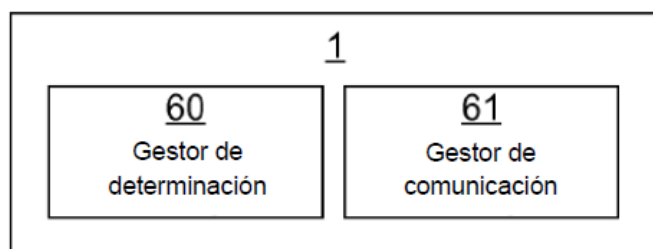


Fig. 12

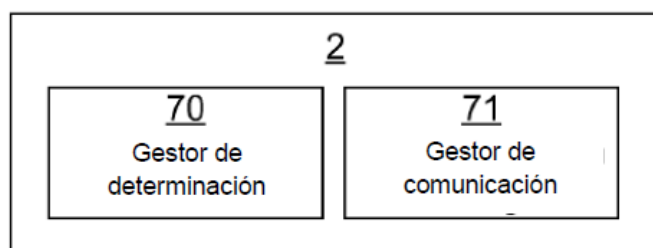


Fig. 13

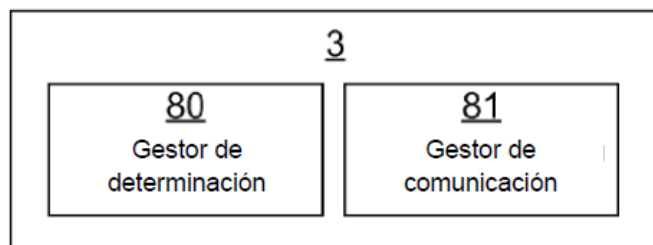


Fig. 14

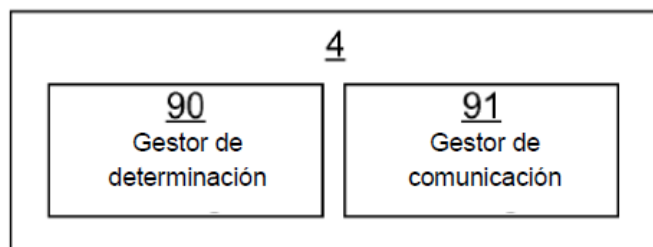


Fig. 15