(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 950 488**

(51) Int. CI.:

H04W 12/04 (2011.01)
H04W 36/14 (2009.01)
H04W 60/02 (2009.01)
H04W 12/041 (2011.01)
H04W 36/00 (2009.01)
H04W 48/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.01.2018 E 21188067 (9)**

(97) Fecha y número de publicación de la concesión europea: **28.06.2023 EP 3923616**

(54) Título: **Manejo del contexto de seguridad en 5G durante el modo inactivo**

(30) Prioridad:

30.01.2017 US 201762452267 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.10.2023

(73) Titular/es:

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

(72) Inventor/es:

BEN HENDA, NOAMEN;
JOST, CHRISTINE;
WIFVESSON, MONICA y
NORRMAN, KARL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Manejo del contexto de seguridad en 5G durante el modo inactivo

Campo técnico

La presente descripción se refiere en general a la seguridad en redes de comunicación inalámbrica y, más particularmente, a métodos y aparatos para el manejo del contexto de seguridad cuando se cambia entre dominios de gestión de movilidad.

Antecedentes

El Proyecto de Asociación de Tercera Generación (3GPP) está desarrollando actualmente los estándares para los sistemas de Quinta Generación (5G). Se espera que las redes 5G admitan muchos escenarios y casos de uso nuevos y sean un habilitador para el Internet de las cosas (IoT). También se espera que los sistemas 5G proporcionen conectividad para una amplia gama de nuevos dispositivos, como sensores, dispositivos portátiles inteligentes, vehículos, máquinas, etc. La flexibilidad será una propiedad clave en los sistemas 5G. Esta nueva flexibilidad se refleja en los requisitos de seguridad para el acceso a la red que exigen el soporte de métodos de autenticación alternativos y diferentes tipos de credenciales además de las habituales Credenciales de Autenticación y Acuerdo de Clave (AKA) proporcionadas previamente por el operador y almacenadas de forma segura en la Tarjeta de Circuito Integrado Universal (UICC). Las funciones de seguridad más flexibles permitirían a los propietarios de fábricas o empresas aprovechar sus propios sistemas de gestión de credenciales e identidades para la autenticación y la seguridad de la red de acceso.

Entre las nuevas características de seguridad en los sistemas 5G se encuentra la introducción de una Función de Anclaje de Seguridad (SEAF). El propósito de SEAF es atender la flexibilidad y el dinamismo en el despliegue de las funciones de red de núcleo 5G, proporcionando un anclaje en una ubicación segura para el almacenamiento de claves. De hecho, se espera que SEAF aproveche la virtualización para lograr la flexibilidad deseada. Como consecuencia, la Función de Gestión de Acceso y Movilidad (AMF), la función 5G responsable de la gestión de acceso y movilidad, se puede implementar en un dominio que es potencialmente menos seguro que la red de núcleo del operador, mientras que la clave maestra permanece en la SEAF en una ubicación segura.

La SEAF está destinada a establecer y compartir una clave denominada KSEAF con el equipo de usuario (UE), que se usa para derivar otras claves, como las claves para la protección del plano de control (por ejemplo, la clave K_{CN}) y la protección de la interfaz de radio. Estas claves generalmente corresponden a las claves de estrato sin acceso (NAS) y la clave de estrato de acceso (KENB) en los sistemas de Evolución a Largo Plazo (LTE). Se supone que la SEAF reside en una ubicación segura y la clave KSEAF nunca abandonaría la SEAF. La SEAF se comunica con las AMF y proporciona el material de clave necesario (derivado de la clave KSEAF) para la protección del tráfico del plano de control (CP) y del plano de usuario (UP) con el equipo de usuario (UE). Una ventaja de este enfoque es que evita la reautenticación cada vez que un UE se mueve de un área atendida por una AMF a un área atendida por otra AMF. De hecho, la autenticación es un procedimiento costoso, particularmente cuando el UE está en itinerancia.

Recientemente, se ha presentado una propuesta para coubicar la SEAF y la AMF, lo que anula el propósito de la SEAF en primer lugar. Vale la pena señalar que el diseño de seguridad en los sistemas LTE se basó conceptualmente en el supuesto de que la entidad de gestión de la movilidad (MME), es decir, el nodo responsable de la gestión de la movilidad en los sistemas LTE, siempre está ubicado en una ubicación segura dentro de la red de núcleo del operador. Esta suposición no se aplica a la AMF en los sistemas 5G. En áreas densas, una AMF podría implementarse más cerca del borde de la red y, por lo tanto, potencialmente en ubicaciones expuestas (por ejemplo, en un centro comercial). Por lo tanto, durante un cambio de AMF, es posible que una de las AMF no esté ubicada en un dominio igualmente seguro que la otra y, por lo tanto, la AMF de destino o de origen podría necesitar protegerse de la otra.

El Sistema de Paquetes Evolucionados (EPS) se basó en la suposición de que la MME siempre está ubicada en una ubicación segura. Por lo tanto, durante un cambio de MME, la nueva MME simplemente obtuvo el contexto de seguridad del UE de la MME anterior. Además, una MME puede desencadenar opcionalmente una nueva autenticación para la seguridad de reenvío.

Con los mecanismos heredados, la seguridad hacia adelante (es decir, la antigua MME no conoce el contexto de seguridad usado por la nueva MME) podría lograrse mediante la reautenticación, pero no había ningún mecanismo para la seguridad hacia atrás (es decir, la nuevo MME no conoce el contexto de seguridad usado por la antigua MME). La nueva AMF puede desencadenar una nueva autenticación, eliminando así cualquier posibilidad de que la antigua AMF determine las nuevas claves. La necesidad de reautenticación podría, por ejemplo, estar basada en una política del operador que tenga en cuenta la ubicación de las diferentes AMF.

Confiar únicamente en el procedimiento de autenticación no es muy eficiente ya que, en términos de rendimiento, es uno de los procedimientos más costosos. Por lo tanto, sigue existiendo la necesidad de proporcionar seguridad al cambiar de AMF sin necesidad de volver a autenticarse.

El Documento 3GPP R2-1700320 "Report of email discusión: [96#34][NR] Inter-Rat mobility" describe un flujo de

mensajes para un traspaso (HO) de modo S1/NG inter-RAT de Nueva Radio (NR) a LTE.

El documento 3GPP TS23.401 V9.16.0 describe mejoras del Servicio General de Radio por Paquetes (GPRS) para el acceso a la Red de Acceso por Radio Terrestre Universal Evolucionada (E-UTRAN). La cláusula 5.3.3.1 describe el procedimiento de actualización del área de seguimiento con cambio de Puerta de Enlace de Servicio y la cláusula 5.3.10.4.2 describe el procedimiento de Comando de Modo de Seguridad (SMC) de NAS en el contexto de GPRS para E-UTRAN.

El documento 3GPP S2-170048 analiza el uso de la Actualización de Área de Seguimiento (TAU) para la movilidad en modo inactivo entre Núcleo NG y Núcleo de Paquetes Evolucionado (EPC).

La especificación 3GPP TS33.401 V 14.1.0 se relaciona con la arquitectura de seguridad en Evolución de Arquitectura de Sistema 3GPP (SAE). La cláusula 14 de ese documento describe la Continuidad de Llamada de Voz de Radio Única (SRVCC) entre la Red de Acceso por Radio Terrestre Universal Evolucionada (E-UTRAN) y la Red de Acceso por Radio EDGE UTRAN/GSM de Circuito Conmutado (GERAN). La cláusula 14.3 describe SRVCC de UTRAN/GERAN con conmutación de circuitos a E-UTRAN para una llamada de emergencia.

El documento 3GPP R2-1700126 describe una propuesta de la empresa Ericsson en la que la empresa admite un cambio clave en NR en el traspaso cuando el contexto de seguridad RAN se mueve o necesita ser actualizado. El cambio de clave se realizará cuando lo ordene la red.

Compendio

La presente descripción se refiere a métodos y aparatos para la gestión flexible del contexto de seguridad durante los cambios de AMF. La presente invención está definida por la materia de las reivindicaciones independientes. Las realizaciones preferidas están definidas por las reivindicaciones dependientes.

Un aspecto de la descripción comprende un método para transferir un contexto de seguridad para un equipo de usuario en un modo inactivo, el método implementado por uno o más nodos de red de núcleo en una red de núcleo de una red de comunicación inalámbrica, en donde uno o más nodos de red de núcleo proporciona una Función de Gestión de Acceso y Movilidad (AMF) de origen. El método comprende:

recibir, desde una AMF de destino, una solicitud de un contexto de seguridad para el equipo de usuario;

generar una nueva clave de estrato sin acceso (NAS) en respuesta a la determinación de que se cumple una política de seguridad específica del operador, en donde la nueva clave NAS se genera usando una clave NAS y un parámetro de actualización; y

enviar, en respuesta a la solicitud, la nueva clave NAS y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave a la AMF de destino en donde la bandera indicadora de cambio de clave se establece en un valor que indica que la clave NAS ha sido cambiada.

Otro aspecto se relaciona con un nodo de red de núcleo en una red de núcleo de una red de comunicación inalámbrica, proporcionando el nodo de red de núcleo una AMF de origen. El nodo de la red de núcleo está configurado para:

recibir, desde una AMF de destino, una solicitud de un contexto de seguridad para un equipo de usuario en un modo inactivo;

generar una nueva clave NAS, usando una clave NAS y un parámetro de actualización, en respuesta a la determinación de que se cumple una política de seguridad específica del operador; y

enviar, en respuesta a la solicitud, la nueva clave NAS y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave a la AMF de destino, en donde la bandera indicadora de cambio de clave se establece en un valor que indica que se ha cambiado una clave de estrato sin acceso.

Otro aspecto se refiere a un programa informático que comprende instrucciones ejecutables que, cuando son ejecutadas por un circuito de procesamiento en un nodo de red de núcleo de una red de comunicación inalámbrica, hacen que el nodo de red de núcleo realice el método anterior.

Otro aspecto se relaciona con un método para transferir un contexto de seguridad de un equipo de usuario durante un modo inactivo, el método implementado por uno o más nodos de red de núcleo en una red de núcleo de una red de comunicación inalámbrica, en donde uno o más nodos de red de núcleo proporcionan una AMF de destino. El método comprende:

recibir, desde el equipo de usuario, un mensaje de registro que indica un cambio de AMF;

solicitar un contexto de seguridad para el equipo de usuario desde una AMF de origen;

recibir desde la AMF de origen, en respuesta a la solicitud y a que la AMF de origen determina que se cumple

una política de seguridad específica del operador, una nueva clave NAS generada por la AMF de origen y una indicación de cambio de clave que comprende un indicador de cambio de clave establecido en un valor indicando que se ha cambiado una clave NAS; y

enviar la indicación de cambio de clave y un parámetro de actualización al equipo de usuario.

Otro aspecto se refiere a un nodo de red de núcleo en una red de núcleo de una red de comunicación inalámbrica. El nodo de red de núcleo proporciona una AMF de destino y comprende un circuito de interfaz para comunicarse con un equipo de usuario y una AMF de origen. El nodo de la red de núcleo también comprende un circuito de procesamiento configurado para:

recibir, desde el equipo de usuario, un mensaje de registro indicando un cambio de AMF;

solicitar un contexto de seguridad de la AMF de origen;

recibir desde la AMF de origen, en respuesta a la solicitud y a que la AMF de origen determina que se cumple una política de seguridad específica del operador, una nueva clave NAS generada por la AMF de origen y una indicación de cambio de clave que comprende un indicador de cambio de clave establecido en un valor indicando que se ha cambiado una clave de estrato sin acceso; y

enviar la indicación de cambio de clave y un parámetro de actualización al equipo de usuario.

Otro aspecto se refiere a un método implementado por un equipo de usuario durante un modo inactivo, comprendiendo el método:

enviar un mensaje de registro a una AMF de destino en una red de comunicación inalámbrica;

recibir desde la AMF de destino, en respuesta al mensaje de registro enviado, un parámetro de actualización y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave que tiene un valor que indica que una AMF de origen ha cambiado una clave de estrato sin acceso con base en una política de seguridad específica de operador; y

generar, en respuesta a la indicación de cambio de clave, una nueva clave NAS usando una clave NAS y el parámetro de actualización.

Otro aspecto se relaciona con un programa informático que comprende instrucciones ejecutables que, cuando son ejecutadas por un circuito de procesamiento en un equipo de usuario en una red de comunicación inalámbrica, hacen que el equipo de usuario realice el método en el párrafo anterior.

Otro aspecto se relaciona con un equipo de usuario en una red de comunicación inalámbrica. El equipo de usuario está configurado para, durante el modo inactivo:

enviar un mensaje de registro a una AMF de destino;

recibir desde la AMF de destino, en respuesta al mensaje de registro enviado, un parámetro de actualización y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave establecida en un valor que indica que una AMF de origen ha cambiado una clave de estrato sin acceso con base una política de seguridad específica de operador; y

generar, en respuesta a la indicación de cambio de clave, una nueva clave NAS usando una clave NAS y el parámetro de actualización.

Breve descripción de los dibujos

La Figura 1 ilustra una red de comunicación inalámbrica ejemplar.

La Figura 2 ilustra un procedimiento para el manejo del contexto de seguridad durante un traspaso.

La Figura 3 ilustra un primer procedimiento para el manejo del contexto de seguridad cuando un UE cambia las AMF en un modo inactivo.

La Figura 4 ilustra un primer procedimiento ejemplar de generación de claves.

La Figura 5 ilustra un segundo procedimiento ejemplar de generación de claves.

La Figura 6 ilustra un segundo procedimiento para el manejo del contexto de seguridad durante un traspaso.

La Figura 7 ilustra un tercer procedimiento para el manejo del contexto de seguridad durante un traspaso.

La Figura 8 ilustra un segundo procedimiento para el manejo del contexto de seguridad cuando un UE cambia

las AMF en un modo inactivo.

La Figura 9 ilustra un método implementado por una estación base de origen durante un traspaso.

La Figura 10 ilustra una estación base ejemplar configurada para realizar el método de la Figura 9.

La Figura 11 ilustra un método implementado por una AMF de origen durante un traspaso.

La Figura 12 ilustra una AMF de origen ejemplar configurada para realizar el método de la Figura 9.

La Figura 13 ilustra un método implementado por una AMF de destino durante un traspaso.

La Figura 14 ilustra un AMF de destino ejemplar configurada para realizar el método de la Figura 13.

La Figura 15 ilustra un método implementado por un UE durante un traspaso.

La Figura 16 ilustra un ejemplo de UE configurado para realizar el método de la Figura 15.

La Figura 17 ilustra un método implementado por una AMF de origen cuando un UE cambia las AMF en modo inactivo.

La Figura 18 ilustra una AMF de origen ejemplar configurada para realizar el método de la Figura 9.

La Figura 19 ilustra un método implementado por un AMF de destino cuando un UE cambia las AMF en modo inactivo.

La Figura 20 ilustra un AMF de destino ejemplar configurada para realizar el método de la Figura 19.

La Figura 21 ilustra un método de actualización de ubicación implementado por un UE cuando un UE se mueve entre AMF en modo inactivo.

La Figura 22 ilustra un ejemplo de UE configurado para realizar el método de la Figura 21.

La Figura 23 ilustra una estación base ejemplar configurada para implementar los procedimientos de manejo del contexto de seguridad como se describe en el presente documento.

La Figura 24 ilustra un nodo de red de núcleo ejemplar configurado para implementar los procedimientos de manejo del contexto de seguridad como se describe en este documento.

La Figura 25 ilustra un ejemplo de UE configurado para implementar los procedimientos de manejo del contexto de seguridad como se describe en el presente documento.

Descripción detallada

Con referencia ahora a los dibujos, se describirá una realización ejemplar de la descripción en el contexto de una red de comunicación inalámbrica 5G. Los expertos en la materia apreciarán que los métodos y aparatos aquí descritos no se limitan al uso en redes 5G, sino que también se pueden usar en redes de comunicación inalámbrica que operan según otros estándares.

La Figura 1 ilustra una red 10 de comunicación inalámbrica según una realización ejemplar. La red 10 de comunicación inalámbrica comprende una red 20 de acceso por radio (RAN) y una red 30 de núcleo. La RAN 20 comprende una o más estaciones 25 base que brindan acceso por radio a los UE 70 que operan dentro de la red 10 de comunicación inalámbrica. Las estaciones 25 base también son conocidas como gNodoB (gNB). La red 30 de núcleo proporciona una conexión entre la RAN 20 y otras redes 80 de paquetes de datos.

En una realización ejemplar, la red 30 de núcleo comprende una función 35 de servidor de autenticación (AUSF), una función 40 de gestión de acceso y movilidad (AMF), una función 45 de gestión de sesión (SMF), una función 50 de control de políticas (PCF), una función 55 de gestión unificada de datos (UDM) y función 60 de plano de usuario (UPF). Estos componentes de la red 10 de comunicación inalámbrica comprenden entidades lógicas que residen en uno o más nodos de red de núcleo. Las funciones de las entidades lógicas pueden implementarse mediante uno o más procesadores, hardware, firmware o una combinación de los mismos. Las funciones pueden residir en un solo nodo de red de núcleo o pueden distribuirse entre dos o más nodos de red de núcleo.

La AMF 40, entre otras cosas, realiza funciones de gestión de movilidad similares a la MME en LTE. La AMF y la MME se denominan aquí genéricamente funciones de gestión de la movilidad. En la realización ejemplar que se muestra en la Figura 1, la AMF 40 es el punto de terminación para la seguridad del estrato sin acceso (NAS). La AMF 40 comparte una clave, denominada clave de red de núcleo (K_{CN}), con el UE 70 que se usa para derivar las claves de protocolo de nivel inferior de NAS para la protección de la integridad y la confidencialidad. La K_{CN} es generalmente equivalente a la clave base denominada K_{ASME} en el Sistema de Paquetes Evolucionados (EPS). La K_{CN} la clave es generalmente equivalente a la clave K_{AMF} usada en las especificaciones 5G. Siempre sucede que después de la autenticación, una

nueva K_{CN} se pone en uso. Como la K_{CN} la clave se establece después de la autenticación no es un aspecto material de la presente divulgación. Los métodos y aparatos descritos en este documento no dependen del método particular usado para calcular la K_{CN} después de la autenticación. Es decir, los métodos de manejo del contexto de seguridad funcionan independientemente de si la K_{CN} se deriva de una clave de nivel superior o se establece directamente mediante el procedimiento de autenticación similar al establecimiento de la K_{ASME} en EPS.

Una vez que se autentica un UE 70, el UE 70 puede moverse entre celdas dentro de la red. Cuando un UE 70 se mueve entre celdas mientras está en un modo conectado, se ejecuta un traspaso. Cuando un UE 70 en modo inactivo se mueve entre celdas, se puede ejecutar un procedimiento de actualización de ubicación. La AMF 40 realiza un seguimiento de la ubicación del UE 70 en su dominio. Normalmente, la red 30 de núcleo tendrá múltiples AMF 40, cada una de las cuales proporcionará servicios de gestión de movilidad en un dominio respectivo. Cuando un UE 70 se mueve entre celdas supervisadas por diferentes AMF 40, el contexto de seguridad debe transferirse desde la AMF 40 de origen a la AMF 40 de destino.

En los sistemas LTE, el contexto de seguridad se transfiere sin cambios desde una entidad de gestión de movilidad (MME) de origen a la MME de destino durante un traspaso o actualización de ubicación entre MME. Después de un cambio de AMF, se puede realizar un procedimiento de comando de modo de seguridad (SMC) de NAS, que usa nuevas claves de NAS y de estrato de acceso (AS). La generación de claves NAS y AS puede ser necesaria, por ejemplo, cuando se necesita un cambio de algoritmo a nivel de NAS. Generalmente, cambiar el algoritmo usado en la capa del protocolo NAS no tiene ningún efecto en las claves AS. Sin embargo, cambiar la clave de contexto NAS principal hace que las claves AS actuales queden obsoletas.

Un aspecto de la descripción es un mecanismo para lograr seguridad hacia atrás durante los cambios de AMF. En lugar de pasar la clave NAS actual a la AMF 40 de destino, la AMF 40 de origen obtiene una nueva clave NAS, proporciona la nueva clave NAS a la AMF 40 de destino y envía un KCI al UE 70. El UE 70 puede luego derivar la nueva clave NAS a partir de la antigua clave NAS. En algunas realizaciones, la AMF 40 de origen puede proporcionar un parámetro de generación de clave al UE 70 para usarlo en la obtención de la nueva clave NAS. En otras realizaciones, la AMF 40 de destino puede cambiar uno o más algoritmos de seguridad.

La Figura 2 ilustra un procedimiento ejemplar para transferir un contexto de seguridad durante un traspaso en el que cambia la AMF. En el paso 1, la estación 25 base de origen (por ejemplo, el gNB de origen) decide iniciar un traspaso basado en N2 debido, por ejemplo, a que no hay conectividad Xn con la estación 25 base de destino (por ejemplo, el gNB de destino). La interfaz Xn es el equivalente 5G de la interfaz X2 en EPS. En el paso 2, la estación 25 base de origen envía un mensaje de traspaso requerido (o el equivalente 5G del mensaje de traspaso requerido) a la AMF 40 de origen. Esta es la AMF 40 que actualmente da servicio al UE 70, con el que comparte un contexto de seguridad NAS completo basado en una clave de estrato sin acceso denominada como clave K_{CN} . La clave K_{CN} se estableció posiblemente después de una autenticación previa o un procedimiento de cambio de AMF 40. En el paso 3, la AMF 40 de origen selecciona la AMF 40 de destino y decide derivar una nueva clave K_{CN} para protegerse a sí misma y a todas las sesiones anteriores de la AMF 40 de destino. La decisión de derivar una nueva clave puede basarse en una política de seguridad específica de operador.

Como ejemplo, podría usarse una nueva clave K_{CN} cuando cambia un conjunto AMF. En general, se supone que no se necesita una derivación de clave horizontal cuando un conjunto AMF no cambia. El razonamiento actual detrás de estas dos suposiciones es que el contexto de seguridad 5G se almacena en la función de red de Almacenamiento de Datos No Estructurados (UDSF) dentro de un conjunto AMF. Entonces, cuando a un UE se le asigna una AMF diferente dentro del mismo conjunto AMF, entonces la derivación horizontal de K_{CN} no es necesaria. Pero cuando a un UE se le asigna una AMF diferente en un conjunto de AMF diferente, entonces la UDSF es diferente y es necesaria una derivación horizontal de K_{CN} . Sin embargo, es posible que estas suposiciones no sean válidas para todas las implementaciones de red posibles. Primero, la UDSF es una función de red opcional. Además, no hay razón para restringir la arquitectura de red a implementaciones donde hay un almacenamiento compartido solo dentro de un conjunto AMF. Algunas implementaciones de red podrían tener almacenamiento seguro en varios conjuntos de AMF. En este caso, no es necesario exigir la derivación horizontal de K_{CN} cuando cambia el conjunto AMF. De manera similar, algunas implementaciones de red podrían usar almacenamiento seguro múltiple dentro de un solo conjunto AMF. En este caso, la derivación de clave horizontal puede ser deseable incluso cuando el UE 70 no cambia los conjuntos AMF. Por lo tanto, la decisión de realizar la derivación horizontal de K_{CN} al cambiar entre AMF se debe hacer según la política de la red, en lugar de exigir/restringir según el conjunto AMF. Por ejemplo, el operador de la red puede tener una política de que se requiera una nueva K_{CN} cuando el UE 70 cambia de una AMF 40 de origen a una AMF 40 de destino que no comparten el mismo almacenamiento seguro.

Volviendo a la Figura 2, la AMF 40 de origen, en el paso 4, envía un mensaje de solicitud de reubicación hacia adelante (o equivalente 5G) que incluye a la nueva K_{CN} junto con cualquier parámetro de seguridad relevante, como las capacidades del UE. La AMF 40 de destino usa esta clave K_{CN} para configurar un nuevo contexto de seguridad y derivar una nueva clave AS. En el paso 5, la AMF 40 de destino envía una solicitud de traspaso (o equivalente 5G) a la estación 25 base de destino. La solicitud de traspaso incluye la nueva clave AS y todos los parámetros de seguridad relevantes, como las capacidades del UE. Esto establece el contexto de seguridad del UE 70 en la estación 25 base de destino. En el paso 6, la estación 25 base de destino reconoce la solicitud de traspaso. En respuesta al reconocimiento, la AMF 40 de destino envía, en el paso 7, un mensaje de respuesta de reubicación hacia adelante (o

equivalente 5G) que incluye un contenedor transparente a la AMF 40 de origen. Este contenedor se reenvía hasta el UE 70 en los pasos 8 y 9

En los pasos 8 y 9, la AMF 40 de origen envía un mensaje de comando de traspaso al UE 70 a través de la estación 25 base de origen, que envía el comando de traspaso al UE 70. El comando de traspaso incluye la información relevante del mensaje de respuesta de reubicación hacia adelante y un KCI que indica que una nueva K_{CN} ha sido derivada. El KCI puede comprender un indicador de cambio de clave explícito establecido en un valor que indica que la clave K_{CN} ha sido cambiada. En respuesta al KCI, el UE 70 establece un nuevo contexto de seguridad y deriva una nueva K_{CN}. El UE 70 usa la nueva clave K_{CN} para derivar una nueva clave AS para comunicarse con la estación 25 base de destino.

La Figura 3 ilustra un procedimiento ejemplar para transferir un contexto de seguridad cuando un UE 70 en modo inactivo cambia las AMF 40. En EPS, la actualización de ubicación durante el modo inactivo es indicada por el UE 70 en una solicitud de Actualización de Área de Seguimiento (TAU). En 5G, se espera que el UE 70 use una solicitud de registro de tipo "registro de movilidad" como se especifica en la TS 23.502, § 4.1.1.2.

En el paso 1, el UE 70 envía una solicitud de registro (Tipo de registro = registro de movilidad, otros parámetros) a la nueva AMF 40 (es decir, la AMF de destino). Los expertos en la materia apreciarán que se pueden enviar otros mensajes para iniciar una actualización de ubicación. El mensaje de solicitud de registro incluye toda la información necesaria para permitir que la nueva AMF 40 identifique la antigua AMF 40 (es decir, la AMF de origen), que actualmente contiene el contexto de seguridad del UE 70. En el paso 2, la nueva AMF 40 envía, en respuesta al mensaje de solicitud de registro, un mensaje de solicitud de contexto a la antigua AMF 40 para solicitar el contexto de seguridad para el UE 70. En el paso 3, la antigua AMF 40 decide derivar una nueva K_{CN} para protegerse a sí misma y a todas las sesiones anteriores de la AMF 40 de destino. La decisión puede basarse en una política de seguridad específica de operador.

En el paso 4, la antigua AMF 40 envía un mensaje de respuesta de solicitud de contexto a la nueva AMF 40. El mensaje de respuesta de solicitud de contexto contiene la información de contexto de seguridad del UE 70 necesaria, incluida la nueva clave K_{CN} . El mensaje de respuesta a la solicitud de contexto incluye además un KCI que indica que la clave NAS, K_{CN}, ha sido cambiada. la antigua clave K_{CN} no se envía a la nueva AMF 40. La nueva AMF 40 usa la nueva clave K_{CN} para establecer un nuevo contexto de seguridad y activa el nuevo contexto de seguridad realizando un procedimiento SMC NAS o un procedimiento similar con el UE 70 como se especifica en la TS 33.401, § 7.2.4.4. En el paso 5, se informa al UE 70 de un cambio de clave a través de un KCI en el primer mensaje de enlace descendente del procedimiento SMC NAS, u otro mensaje enviado durante el procedimiento SMC NAS.

El contexto de seguridad del NAS basado en la clave K_{CN} se comparte entre el UE 70 y la AMF 40 que actualmente le da servicio. El contexto de seguridad incluye parámetros de seguridad similares a los de los sistemas LTE, como los contadores NAS, el identificador de conjunto de claves, etc. En una realización ejemplar, se usa un mecanismo de derivación de clave horizontal para generar una nueva clave K_{CN} durante el cambio de AMF 40. La derivación de la nueva K_{CN} podría basarse únicamente en la K_{CN} anterior. Desde una perspectiva de seguridad, no hay beneficio de una entrada adicional en el paso de derivación de clave.

La Figura 4 ilustra un primer procedimiento de obtención de claves. En esta realización, se supone que la función de derivación de claves (KDF) deriva la nueva clave K_{CN} con base en únicamente la antigua clave K_{CN}. Este encadenamiento de claves de la AMF 40 a la AMF 40 puede continuar hasta que se realice una nueva autenticación. Puede dejarse a la política del operador cómo configurar la AMF 40 con respecto a qué mecanismo de seguridad se selecciona durante un cambio de AMF 40. Por ejemplo, según los requisitos de seguridad de un operador, el operador puede decidir si realizar una nueva autenticación en la AMF 40 de destino o si se necesita un cambio de clave en la AMF 40 de origen.

La Figura 5 ilustra otro procedimiento de obtención de claves. Esta realización puede ser útil en escenarios en los que una AMF 40 necesita preparar claves por adelantado para más de una AMF 40 de destino potencial. En este caso, se necesita un parámetro de derivación de clave (KDP) adicional para la separación criptográfica, de modo que se preparan diferentes claves K_{CN} para diferentes AMF 40 de destino potenciales. Según el tipo de parámetro, es posible que sea necesario proporcionar el UE 70 con el KDP elegido además del KCI. En algunas realizaciones, el KDP también puede servir como un KCI implícito para que no se requiera un KCI separado. Por ejemplo, cuando el KDP comprende un nonce generado por la AMF 40 de origen, el nonce debe proporcionarse al UE 70. Otros KDP potenciales incluyen una marca de tiempo, un número de versión. Según la invención, se usa un parámetro de actualización como KDP.

Durante un traspaso en modo conectado, el KDP podría enviarse desde la AMF 40 de origen al UE 70 a través de la estación 25 base de origen en un comando de traspaso. De manera alternativa, el KDP puede enviarse al UE 70 a través de la AMF 40 de destino en un contenedor NAS transparente. Durante un procedimiento de registro o actualización de ubicación, el KDP podría enviarse desde la AMF 40 de destino en un SMC NAS. Sin embargo, en escenarios en los que el KDP está disponible para el UE 70, como un parámetro similar a un identificador público AMF, puede que no sea necesario proporcionar al UE 70 el parámetro KDP. Más generalmente, cualquier información estática, tal como un parámetro de configuración de red estática o un parámetro de configuración de UE estático,

conocida por el UE 70 y la AMF 40 de origen, puede usarse como un KDP.

La Figura 6 ilustra un procedimiento de traspaso en donde se usa un KDP para derivar la nueva clave K_{CN}. Este procedimiento es generalmente el mismo que el procedimiento que se muestra en la Figura 2. En aras de la brevedad, no se describen los pasos que no han cambiado. En el paso 3, la AMF 40 de origen selecciona la AMF 40 de destino y decide derivar un nuevo K_{CN} para protegerse a sí mismo y a todas las sesiones anteriores de la AMF 40 de destino. En esta realización, la AMF 40 de origen genera un KDP (por ejemplo, el número de versión) y usa el KDP para derivar la nueva clave K_{CN}. En el paso 4, la AMF 40 de origen envía un mensaje de solicitud de reubicación hacia adelante (o equivalente 5G) que incluye la nueva K_{CN} junto con cualquier parámetro de seguridad relevante, como las capacidades del UE. La AMF 40 de destino usa esta clave K_{CN} para configurar un nuevo contexto de seguridad y derivar una nueva clave AS. La AMF 40 de origen no proporciona el KDP a la nueva AMF 40. En cambio, en el paso 8, la AMF 40 de origen envía un comando de traspaso a la estación 25 base de origen, en donde el comando de traspaso incluye el KDP además de o en lugar del KCI. Como se señaló anteriormente, el KDP puede servir como un KCI implícito. En respuesta al KCI y/o KDP, el UE 70 establece un nuevo contexto de seguridad y deriva una nueva K_{CN} usando el KDP. El UE 70 puede usar la nueva clave K_{CN} para derivar una nueva clave AS para comunicarse con la estación 25 base de destino.

En los sistemas LTE, un cambio de algoritmo NAS en la AMF 40 de destino solo puede tener efecto a través de un procedimiento SMC NAS. Dado que las capacidades del UE 70 se envían con otra información de contexto del UE 70 a la AMF 40 de destino, es posible que la AMF 40 de destino indique qué nuevos algoritmos NAS se han seleccionado. La Figura 7 ilustra un procedimiento de traspaso ejemplar en donde la AMF 40 de destino selecciona uno o más algoritmos de seguridad NAS nuevos (por ejemplo, algoritmos criptográficos). Los pasos 1 - 4 son los mismos que se describen en la Figura 2. En el paso 5, la AMF 40 de destino selecciona uno o más algoritmos de seguridad NAS nuevos. Los pasos 6 y 7 son los mismos que los pasos 5 y 6 de la Figura 2. En el paso 8, la AMF 40 de destino incluye una indicación de los nuevos algoritmos de seguridad en el contenedor transparente al elemento de información de origen del mensaje de respuesta de reubicación hacia adelante enviado a la AMF 40 de origen. Este contenedor se reenvía hasta el UE 70 en los pasos 9 y 10. La indicación del algoritmo de seguridad puede incluirse con el KCI en el comando de transferencia, o en un mensaje separado. Como consecuencia, el UE 70 tiene todos los parámetros necesarios para activar el contexto de seguridad NAS con la AMF 40 de destino sin necesidad de un procedimiento SMC NAS. Este mecanismo funciona independientemente de cómo se deriva la clave K_{CN} .

La Figura 8 ilustra un procedimiento ejemplar para transferir un contexto de seguridad cuando un UE 70 en modo inactivo cambia las AMF 40. Este procedimiento es similar al procedimiento que se muestra en la Figura 3. En EPS, la actualización de ubicación durante el modo inactivo es indicada por el UE 70 en un Solicitud de Actualización del Área de Seguimiento (TAU). En 5G, se espera que el UE 70 use una solicitud de registro de tipo "registro de movilidad" como se especifica en la TS 23.502, § 4.1.1.2.

En el paso 1, el UE 70 envía una solicitud de registro (Tipo de registro = registro de movilidad, otros parámetros) a la nueva AMF 40 (es decir, la AMF de destino). Los expertos en la materia apreciarán que se pueden enviar otros mensajes para iniciar una actualización de ubicación. El mensaje de solicitud de registro incluye toda la información necesaria para permitir que la nueva AMF 40 identifique la antigua AMF 40 (es decir, la AMF de origen), que actualmente contiene el contexto de seguridad del UE 70. En el paso 2, la nueva AMF 40 envía, en respuesta al mensaje de solicitud de registro, un mensaje de solicitud de contexto a la antigua AMF 40 para solicitar el contexto de seguridad para el UE 70. En el paso 3, la antigua AMF 40 decide derivar un nuevo K_{CN} para protegerse a sí mismo ya todas las sesiones anteriores de la AMF 40 de destino. La decisión puede basarse en una política de seguridad específica de operador.

En una realización denominada Alternativa 1, la antigua AMF 40 envía, en el paso 4A, un mensaje de respuesta de solicitud de contexto a la nueva AMF 40. El mensaje de respuesta de solicitud de contexto contiene la información de contexto de seguridad del UE 70 necesaria, incluida la nueva clave K_{CN}. El mensaje de respuesta a la solicitud de contexto incluye además un KCI que indica que la clave NAS, K_{CN}, se ha cambiado y se ha usado un KDP para derivar la nueva calve K_{CN} . la antigua clave K_{CN} no se envía a la nueva AMF 40. La nueva AMF 40 usa la nueva clave K_{CN} para establecer un nuevo contexto de seguridad y activa el nuevo contexto de seguridad realizando un procedimiento SMC NAS o un procedimiento similar con el UE 70 como se especifica en la TS 33.401, § 7.2.4.4. En el paso 5A, el KCI y el KDP (por ejemplo, un parámetro de actualización o nonce) se envían al UE 70 en el primer mensaje de enlace descendente del procedimiento SMC NAS u otro mensaje de enlace descendente en el procedimiento SMC NAS. El KCI indica al UE 70 que la clave K_{CN} ha sido cambiada. El KDP es un parámetro de seguridad que usa el UE 70 para derivar la nueva clave K_{CN}. En esta realización, el KCI y el KDP son parámetros separados.

En otra realización denominada Alternativa 2, la antigua AMF 40 envía, en el paso 4B, un mensaje de respuesta de solicitud de contexto a la nueva AMF 40. El mensaje de respuesta de solicitud de contexto contiene la información de contexto de seguridad del UE 70 necesaria, incluida la nueva clave K_{CN}. El mensaje de respuesta a la solicitud de contexto incluye además un KDP que indica implícitamente que la clave NAS, K_{CN}, ha sido cambiada. La antigua clave K_{CN} no se envía a la nueva AMF 40. La nueva AMF 40 usa la nueva clave K_{CN} para establecer un nuevo contexto de seguridad y activa el nuevo contexto de seguridad realizando un SMC NAS o un procedimiento similar con el UE 70 como se especifica en la TS 33.401, § 7.2.4.4. En el paso 5B, la nueva AMF 40 envía el KDP (por ejemplo, un parámetro de actualización o nonce) al UE 70 en el primer mensaje de enlace descendente del procedimiento SMC NAS, o algún otro mensaje de enlace descendente en el procedimiento SMC NAS. El KDP funciona como una

indicación de cambio de clave para indicar al UE 70 que se ha cambiado la clave NAS. El UE 70 usa el KDP y su antigua clave K_{CN} para derivar la nueva clave K_{CN}.

La Figura 9 ilustra un método 100 ejemplar implementado durante un traspaso por una estación 25 base de origen en una red de acceso de una red 10 de comunicación inalámbrica. La estación 25 base de origen envía un primer mensaje de traspaso a una AMF 40 de origen en una red 30 de núcleo de la red 10 de comunicación inalámbrica para iniciar un traspaso de un UE 70 (bloque 105). Posteriormente, la estación 25 base de origen recibe, en respuesta al primer mensaje de traspaso, un segundo mensaje de traspaso de la AMF 40 de origen (bloque 110). El segundo mensaje de traspaso incluye un KCI que indica que una clave de estrato sin acceso (por ejemplo, K_{CN}) ha sido cambiada. La estación 25 base de origen reenvía el segundo mensaje de traspaso con el KCI al UE 70 (bloque 115).

En algunas realizaciones del método 100, el KCI comprende una bandera indicadora de cambio de clave establecida en un valor que indica que la clave del estrato sin acceso ha sido cambiada. En otras realizaciones, el KCI comprende un parámetro de seguridad que indica implícitamente que se ha cambiado la clave del estrato sin acceso. El parámetro de seguridad comprende uno de un nonce, marca de tiempo, parámetro de actualización y número de versión.

Algunas realizaciones del método 100 comprenden además recibir, desde la AMF 40 de origen, un KDP que necesita el UE 70 para generar una nueva clave de estrato sin acceso, y reenviar el KDP al UE 70. En algunos ejemplos, el KDP se recibe con el KCI en el segundo mensaje de traspaso. El KDP comprende, por ejemplo, uno de un nonce, marca de tiempo, parámetro de actualización y número de versión. En algunas realizaciones, la derivación de claves sirve como un KCI implícito.

Algunas realizaciones del método 100 comprenden además recibir, desde la AMF 40 de origen, un parámetro de algoritmo de seguridad que indica al menos un algoritmo de seguridad que usará el UE 70, y reenviar el parámetro de algoritmo de seguridad al UE 70. En un ejemplo, el parámetro del algoritmo de seguridad se recibe con el KCI en el segundo mensaje de traspaso.

En una realización del método 100, el primer mensaje de traspaso comprende un mensaje de traspaso requerido que indica la necesidad de un traspaso del UE 70.

En una realización del método 100, el segundo mensaje de traspaso comprende un comando de traspaso que incluye un KCI.

En una realización del método 100, la clave de estrato sin acceso comprende una clave de red de núcleo (K_{CN}).

La Figura 10 es una estación 120 base de ejemplo configurada para realizar el método 100 que se muestra en la Figura 9. La estación 120 base comprende una unidad 125 de envío, una unidad 130 de recepción y una unidad 135 de reenvío. La unidad 125 de envío está configurada para enviar un primer traspaso mensaje a una AMF 40 de origen en una red 30 de núcleo de la red 10 de comunicación inalámbrica para iniciar un traspaso de un UE 70. La unidad 130 de recepción está configurada para recibir, en respuesta al primer mensaje de traspaso, un segundo mensaje de traspaso desde la AMF 40 de origen. La unidad 135 de reenvío está configurada para reenviar el segundo mensaje de traspaso con el KCI al UE 70. El KCI indica un cambio de la clave de estrato sin acceso (por ejemplo, K_{CN}). La unidad 125 de envío, la unidad 130 de recepción y la unidad 135 de reenvío pueden comprender circuitos de hardware, microprocesadores y/o software configurados para realizar el método que se muestra en la Figura 9. En algunas realizaciones, la unidad 125 de envío, la unidad 130 de recepción y la unidad 135 de reenvío son implementadas por un solo microprocesador. En otras realizaciones, la unidad 125 de envío, la unidad 130 de recepción y la unidad 135 de reenvío pueden implementarse mediante dos o más microprocesadores.

La Figura 11 ilustra un método 150 ejemplar implementado durante un traspaso por una AMF 40 de origen en una red 30 de núcleo de una red 10 de comunicación inalámbrica. La AMF 40 de origen recibe, desde la estación 25 base de origen, un primer mensaje de traspaso que indica que se necesita un traspaso del UE 70 (bloque 155). La AMF de origen genera una nueva clave de estrato sin acceso (por ejemplo, K_{CN}) (bloque 160), y envía la nueva clave de estrato sin acceso a una AMF 40 de destino en la red 30 de núcleo de la red 10 de comunicación inalámbrica (bloque 165). La AMF 40 de origen también envía un KCI al UE 70 en un segundo mensaje de traspaso (bloque 170). El KCI indica un cambio de la clave de estrato sin acceso.

En algunas realizaciones del método 150, generar la nueva clave de estrato sin acceso comprende generar la nueva clave de estrato sin acceso a partir de una clave de estrato sin acceso anterior. En otras realizaciones, generar la nueva clave de estrato sin acceso comprende generar la nueva clave de estrato sin acceso a partir de una clave de estrato sin acceso anterior y el KDP. En algunas realizaciones, la AMF de origen envía el KDP al UE 70 junto con el KCI en el segundo mensaje de traspaso.

Algunas realizaciones del método 150 comprenden además seleccionar la AMF 40 de destino y generar la nueva clave de estrato sin acceso dependiendo de la selección de la AMF 40 de destino.

Algunas realizaciones del método 150 comprenden además generar dos o más claves de estrato sin acceso, cada una para diferentes AMF 40 de destino. En un ejemplo, las dos o más claves de estrato sin acceso se generan usando diferentes KDP.

Algunas realizaciones del método 150 comprenden además enviar uno o más parámetros de seguridad a la AMF 40 de destino. En un ejemplo, el uno o más parámetros de seguridad se transmiten a la AMF 40 de destino en el segundo mensaje de traspaso. En un ejemplo, uno o más parámetros de seguridad incluyen información de capacidad de UE.

Algunas realizaciones del método 150 comprenden además recibir, desde la AMF 40 de destino, un parámetro de algoritmo de seguridad que indica al menos un algoritmo de seguridad, y enviar el parámetro de algoritmo de seguridad al UE 70. En otro ejemplo, el parámetro de algoritmo de seguridad se recibe desde la AMF 40 de destino en un mensaje de respuesta de reubicación hacia adelante.

En una realización del método 150, el primer mensaje de traspaso comprende un mensaje de traspaso requerido que indica la necesidad de un traspaso del UE 70.

En una realización del método 150, el segundo mensaje de traspaso comprende un comando de traspaso que incluye el KCI.

En una realización del método 150, la nueva clave de estrato sin acceso se envía a la AMF (40) de destino en un mensaje de solicitud de reubicación hacia adelante.

En una realización del método 150, la clave de estrato sin acceso comprende una clave de red de núcleo (K_{CN}).

La Figura 12 es una AMF 175 de origen ejemplar configurada para realizar el método 150 que se muestra en la Figura 11. La AMF 175 de origen comprende una unidad 180 de recepción, una unidad 185 de generación de claves, una primera unidad 190 de envío y una segunda unidad 195 de envío. La unidad 180 de recepción está configurada para recibir, desde una estación 25 base de origen, un primer mensaje de traspaso que indica que se necesita un traspaso del UE 70. La unidad 185 de generación de claves está configurada para generar una nueva clave de estrato sin acceso (por ejemplo, K_{CN}) como se describe en el presente documento. La primera unidad 190 de envío está configurada para enviar la nueva clave de estrato sin acceso a una AMF 40 de destino en la red 30 de núcleo de la red 10 de comunicación inalámbrica. La segunda unidad 195 de envío está configurada para enviar un KCI al UE 70 en un segundo mensaje de traspaso. El KCI indica un cambio de la clave de estrato sin acceso. La unidad 180 de recepción, una unidad 185 de generación de claves, la primera unidad 190 de envío y la segunda unidad 195 de envío pueden comprender circuitos de hardware, microprocesadores y/o software configurados para realizar el método que se muestra en la Figura 11. En algunas realizaciones, la unidad 180 de recepción, la unidad 185 de generación de claves, la primera unidad 190 de envío y la segunda unidad 195 de envío están implementadas por un solo microprocesador. En otras realizaciones, la unidad 180 de recepción, la unidad 185 de generación de claves, la primera unidad 190 de envío y la segunda unidad 195 de envío pueden implementarse mediante dos o más microprocesadores.

La Figura 13 ilustra un método 200 ejemplar implementado durante un traspaso por una AMF 40 de destino en una red 30 de núcleo de una red 10 de comunicación inalámbrica. La AMF 40 de destino recibe, de la AMF 40 de origen, una nueva clave de estrato sin acceso (por ejemplo, K_{CN}) (bloque 205). La AMF de destino establece un nuevo contexto de seguridad que incluye una nueva clave de estrato de acceso derivada de la nueva clave de estrato sin acceso (bloque 210), y envía la nueva clave de estrato de acceso a una estación 25 base de destino (bloque 215).

Algunas realizaciones del método 200 comprenden además recibir uno o más parámetros de seguridad desde la función de gestión de movilidad de origen. En un ejemplo, uno o más parámetros de seguridad incluyen la información de capacidad de UE. En una realización, los parámetros de seguridad se reciben con la nueva clave de estrato sin acceso.

En algunas realizaciones del método 200, establecer el nuevo contexto de seguridad comprende seleccionar uno o más algoritmos de seguridad. En un ejemplo, al menos uno de los algoritmos de seguridad se selecciona con base en la información de capacidad del UE.

Algunas realizaciones del método 200 comprenden además el envío a la función de gestión de movilidad de origen, un parámetro de algoritmo de seguridad que indica al menos un algoritmo de seguridad para el nuevo contexto de seguridad.

En algunas realizaciones del método 200, la nueva clave de estrato sin acceso se recibe desde la función de gestión de movilidad de origen en un mensaje de solicitud de reubicación hacia adelante.

En algunas realizaciones del método 200, la nueva clave de estrato de acceso se envía a la estación base de destino en una solicitud de traspaso.

En algunas realizaciones del método 200, el parámetro del algoritmo de seguridad se envía a la función de gestión de movilidad de origen en un mensaje de respuesta de reubicación hacia adelante.

En algunas realizaciones del método 200, la clave de estrato sin acceso comprende una clave de red de núcleo (KCN).

La Figura 14 es un ejemplo de AMF 220 de destino configurada para realizar el método 200 que se muestra en la Figura 13. La AMF 220 de destino comprende una unidad 225 de recepción, una unidad 230 de seguridad y una unidad 235 de envío. La unidad 225 de recepción está configurada para recibir, desde una AMF 40 de origen, una nueva clave de estrato sin acceso (por ejemplo, K_{CN}). La unidad 230 de seguridad está configurada para establecer un nuevo contexto de seguridad que incluye una nueva clave de estrato de acceso derivada de la nueva clave de estrato sin

acceso. La unidad 235 de envío está configurada para enviar la nueva clave de estrato de acceso a una estación 25 base de destino. La unidad 225 de recepción, la unidad 230 de seguridad y la unidad 235 de envío pueden comprender circuitos de hardware, microprocesadores y/o software configurados para realizar el método que se muestra en Figura 13. En algunas realizaciones, la unidad 225 de recepción, la unidad 230 de seguridad y la unidad 235 de envío están implementadas por un solo microprocesador. En otras realizaciones, la unidad 225 de recepción, la unidad 230 de seguridad y la unidad 235 de envío pueden implementarse mediante dos o más microprocesadores.

La Figura 15 ilustra un método 250 ejemplar implementado por un UE 70 en una red 10 de comunicación inalámbrica durante un traspaso. El UE 70 recibe un mensaje de traspaso que incluye un KCI desde una estación 25 base de origen en el dominio de una AMF 40 de origen de la red 10 de comunicación inalámbrica (bloque 255). El KCI indica al UE 70 que una clave de estrato sin acceso (por ejemplo, K_{CN}) ha sido cambiada. El UE 70 realiza un traspaso desde la estación 25 base de origen a una estación 25 base de destino en un dominio de una AMF 40 de destino (bloque 260). El UE 70 establece, en respuesta al KCI, un nuevo contexto de seguridad con la AMF 40 de destino (bloque 265). El nuevo contexto de seguridad incluye una nueva clave de estrato sin acceso. El UE 70 puede comunicarse opcionalmente con la AMF 40 de destino usando la nueva clave de estrato sin acceso (bloque 270).

En algunas realizaciones del método 250, el KCI comprende una bandera indicadora de cambio de clave establecida en un valor que indica que la clave del estrato sin acceso ha sido cambiada. En otras realizaciones, el KCI comprende un parámetro de seguridad que indica implícitamente que se ha cambiado la clave del estrato sin acceso. El parámetro de seguridad comprende un KDP utilizado para generar la nueva clave de estrato sin acceso.

Algunas realizaciones del método 250 comprenden además generar la nueva clave de estrato sin acceso usando el KDP. En un ejemplo, el KDP comprende uno de un nonce, marca de tiempo, parámetro de actualización, número de versión e información estática conocida por el UE 70 y la AMF de origen. En algunas realizaciones, el KDP se recibe con el KCI en el segundo mensaje de traspaso. En algunas realizaciones, el KDP sirve como un KCI implícito.

Algunas realizaciones del método 250 comprenden además generar una nueva clave de estrato de acceso a partir de la nueva clave de estrato sin acceso, y comunicarse con una estación 25 base de destino usando la nueva clave de estrato de acceso.

Algunas realizaciones del método 250 comprenden además recibir un parámetro de algoritmo de seguridad desde la estación 25 base de origen que identifica uno o más algoritmos de seguridad usados en el nuevo contexto de seguridad. En un ejemplo, el parámetro del algoritmo de seguridad se recibe en el mensaje de traspaso junto con el KCI.

En algunas realizaciones del método 250, el mensaje de traspaso comprende un comando de traspaso.

En algunas realizaciones del método 250, la clave de estrato sin acceso comprende una clave de red de núcleo (K_{CN}).

La Figura 16 es un ejemplo de UE 275 configurado para realizar el método 250 que se muestra en la Figura 15. El UE 275 comprende una unidad 280 de recepción, una unidad 285 de traspaso y una unidad 290 de seguridad. La unidad 280 de recepción está configurada para recibir un mensaje de traspaso que incluye un KCI de una estación 25 base de origen en el dominio de una AMF 40 de origen de la red 10 de comunicación inalámbrica. El KCI indica al UE 70 que una clave de estrato sin acceso (por ejemplo, K_{CN}) ha sido cambiada. La unidad 285 de traspaso está configurada para realizar un traspaso desde la estación 25 base de origen a una estación 25 base de destino en un dominio de una AMF 40 de destino. La unidad 290 de seguridad está configurada para establecer, en respuesta al KCI, un nuevo contexto de seguridad con la AMF 40 de destino . El UE 275 también puede incluir opcionalmente una unidad 295 de comunicación configurada para comunicarse con la AMF 40 de destino usando la nueva clave de estrato sin acceso. La unidad 280 de recepción, la unidad 285 de traspaso, la unidad 290 de seguridad y la unidad 295 de comunicación pueden comprender circuitos de hardware, microprocesadores y/o software configurados para realizar el método que se muestra en la Figura 15. En algunas realizaciones, la unidad 280 de recepción, la unidad 285 de traspaso, la unidad 290 de seguridad y la unidad 295 de comunicación están implementadas por un solo microprocesador. En otras realizaciones, la unidad 280 de recepción, la unidad 285 de traspaso, la unidad 290 de seguridad y la unidad 295 de comunicación pueden implementarse mediante dos o más microprocesadores.

La Figura 17 ilustra un método 300 inventivo implementado por una AMF 40 de origen en una red 30 de núcleo de la red 10 de comunicación cuando un UE 70 en modo inactivo cambia las AMF 40. La AMF 40 de origen recibe una solicitud de un contexto de seguridad para el UE 70 de una AMF 40 de destino (bloque 305). La AMF 40 de origen genera una nueva clave de estrato sin acceso (por ejemplo, K_{CN}) (bloque 310), y envía, en respuesta a la solicitud, la nueva clave de estrato sin acceso y un KCI a la AMF 40 de destino (bloque 315). El KCI indica un cambio de la clave del estrato sin acceso.

En algunas realizaciones no reivindicadas del método 300, generar una nueva clave de estrato sin acceso comprende generar la nueva clave de estrato sin acceso a partir de la clave de estrato sin acceso anterior. En otras realizaciones, según la invención, el método comprende generar un KDP y generar la nueva clave de estrato sin acceso a partir de una clave de estrato sin acceso antigua y el KDP.

Según la invención, en el método 300, la indicación de cambio de clave comprende una bandera indicadora de cambio de clave establecida en un valor que indica que la clave del estrato sin acceso ha sido cambiada. El parámetro de

seguridad comprende un KDP que es un parámetro de actualización, usado para generar la nueva clave de estrato sin acceso.

Algunas realizaciones del método 300 comprenden además el envío, en respuesta a la solicitud, de un KDP usado para generar la nueva clave de estrato sin acceso. El KDP comprende uno de un nonce, marca de tiempo, parámetro de actualización y número de versión.

Algunas realizaciones del método 300 comprenden además seleccionar la AMF 40 de destino y generar una nueva clave de estrato sin acceso dependiendo de la selección de la AMF 40 de destino.

En algunas realizaciones del método 300, generar una nueva clave de estrato sin acceso comprende generar dos o más claves de estrato sin acceso, cada una para una AMF 40 de destino diferente. En un ejemplo, las dos o más claves de estrato sin acceso se generan usando diferentes KDP.

Algunas realizaciones del método 300 comprenden además el envío de uno o más parámetros de seguridad con la nueva clave de estrato sin acceso a la AMF 40 de destino. En un ejemplo, el uno o más parámetros de seguridad incluyen información de capacidad de UE.

En algunas realizaciones del método 300, la solicitud de un contexto de seguridad se recibe desde la AMF 40 de destino en un mensaje de solicitud de contexto.

En algunas realizaciones del método 300, la nueva clave de estrato sin acceso se envía a la AMF 40 de destino en un mensaje de respuesta de solicitud de contexto.

En algunas realizaciones del método 300, la clave de estrato sin acceso comprende una clave de red de núcleo (KCN).

La Figura 18 es una AMF 320 de origen ejemplar configurada para realizar el método 300 que se muestra en la Figura 17. La AMF 320 de origen comprende una unidad 325 de recepción, una unidad 330 de generación de claves y una unidad 335 de envío. La unidad 325 de recepción está configurada para recibir una solicitud para un contexto de seguridad para el UE 70 desde una AMF 40 de destino. La unidad 330 de generación de claves está configurada para generar una nueva clave de estrato sin acceso (por ejemplo, K_{CN}). La unidad 235 de envío está configurada para enviar, en respuesta a la solicitud, la nueva clave de estrato sin acceso y un KCI a la AMF 40 de destino. La unidad 325 de recepción, una unidad 330 de generación de claves y una unidad 335 de envío pueden comprender circuitos de hardware, microprocesadores y/o software configurado para realizar el método mostrado en la Figura 17. En algunas realizaciones, la unidad 325 de recepción, la unidad 330 de generación de claves y la unidad 335 de envío se implementan mediante un solo microprocesador. En otras realizaciones, la unidad 325 de recepción, la unidad 330 de generación de claves y la unidad 335 de envío pueden implementarse mediante dos o más microprocesadores.

La Figura 19 ilustra un método 350 inventivo implementado por una AMF 40 de destino en una red 30 de núcleo de una red 10 de comunicación inalámbrica cuando un UE 70 en modo inactivo cambia los AMF 40. La AMF 40 de destino recibe, del UE 70, un mensaje de registro u otro mensaje de control que indica un cambio de AMF (bloque 355). La AMF 40 de destino solicita un contexto de seguridad de una AMF 40 de origen en la red de comunicación inalámbrica (bloque 360). En respuesta a la solicitud, la AMF 40 de destino recibe una nueva clave de estrato sin acceso (por ejemplo, K_{CN}) y un KCI que indica que se ha cambiado la clave del estrato sin acceso (bloque 365). La AMF 40 de destino envía el KCI al UE 70 (bloque 370) y opcionalmente establece un nuevo contexto de seguridad para el UE 70 que incluye la nueva clave de estrato sin acceso (bloque 375).

Algunas realizaciones del método 350 comprenden además el establecimiento de un nuevo contexto de seguridad que incluye la nueva clave de estrato sin acceso.

Según la invención el método 350 comprende además recibir uno o más parámetros de seguridad desde la AMF 40 de origen. En un ejemplo, el uno o más parámetros de seguridad incluyen información de capacidad del UE. En otro ejemplo, los parámetros de seguridad se reciben junto con el KCI.

Según la invención, en el método 350, la indicación de cambio de clave comprende una bandera indicadora de cambio de clave establecida en un valor que indica que la clave de estrato sin acceso ha sido cambiada. El parámetro de seguridad comprende un KDP que es un parámetro de actualización usado para generar la nueva clave de estrato sin acceso.

Algunas realizaciones del método 350 comprenden además recibir, en respuesta a la solicitud, un KDP utilizado para generar la nueva clave de estrato sin acceso. Según la invención KDP comprende un parámetro de actualización. En la realización no reivindicada, KDP comprende uno de un nonce, marca de tiempo y número de versión. En algunas realizaciones, la AMF 40 de destino envía el KDP al UE 70 junto con el KCI en un mensaje SMC NAS.

En algunas realizaciones del método 350, establecer un nuevo contexto de seguridad comprende, en parte, seleccionar uno o más algoritmos de seguridad. En un ejemplo, al menos uno de los algoritmos de seguridad se selecciona con base en la información de capacidad del UE.

Algunas realizaciones del método 350 comprenden además enviar al UE 70 un parámetro de algoritmo de seguridad

que indica al menos un algoritmo de seguridad para el nuevo contexto de seguridad.

En algunas realizaciones del método 350, el KCI se recibe desde una AMF 70 de origen en un mensaje de respuesta de solicitud de contexto.

En algunas realizaciones del método 350, el KCI se envía al UE 70 en un mensaje de establecimiento de seguridad.

En algunas realizaciones del método 350, la clave de estrato sin acceso comprende una clave de red de núcleo (KCN).

La Figura 20 es un ejemplo de AMF 380 de destino configurada para realizar el método 350 que se muestra en la Figura 19. La AMF 380 de destino comprende una primera unidad 382 de recepción, una unidad 384 de solicitud, una segunda unidad 386 de recepción y una unidad 388 de envío. La primera unidad 382 de recepción se configura para recibir, desde el UE 70, un mensaje de registro u otro mensaje de control que indique un cambio de AMF. La unidad 384 de solicitud está configurada para solicitar, en respuesta al mensaje de registro, un contexto de seguridad de una AMF 40 de origen en la red de comunicación inalámbrica. La segunda unidad 386 de recepción está configurada para recibir, desde la AMF 40 de origen en respuesta a la solicitud de contexto de seguridad, una nueva clave de estrato sin acceso y un KCI que indica que la clave de estrato sin acceso (por ejemplo, K_{CN}) ha sido cambiada. La unidad 388 de envío está configurada para enviar el KCI al UE 70. La AMF 380 de destino también puede incluir opcionalmente una unidad 390 de seguridad configurada para establecer un nuevo contexto de seguridad para el UE 70 que incluye la nueva clave de estrato sin acceso. La primera unidad 382 de recepción, la unidad 384 de solicitud, la segunda unidad 386 de recepción, la unidad 388 de envío y la unidad 390 de seguridad pueden comprender circuitos de hardware, microprocesadores y/o software configurados para realizar el método que se muestra en la Figura 19. En algunas realizaciones, la primera unidad 382 de recepción, la unidad 384 de solicitud, la segunda unidad 386 de recepción, la unidad 388 de envío y la unidad de 390 seguridad están implementadas por un solo microprocesador. En otras realizaciones, la primera unidad 382 de recepción, la unidad 384 de solicitud, la segunda unidad 386 de recepción, la unidad 388 de envío y la unidad 390 de seguridad pueden implementarse mediante dos o más microprocesadores.

La Figura 21 ilustra un método 400 ejemplar implementado por un UE 70 en modo inactivo en una red 10 de comunicación inalámbrica cuando el UE 70 cambia las AMF 40. El UE 70 envía un mensaje de registro u otro mensaje de control a una AMF 40 de destino en la red de comunicación inalámbrica (bloque 405). El UE 70 recibe, en respuesta al mensaje de registro u otro mensaje de control, un KCI que indica que una clave de estrato sin acceso (por ejemplo, K_{CN}) ha sido cambiada (bloque 410). En respuesta al KCI, el UE 70 genera una nueva clave de estrato sin acceso (bloque 415). Después de generar la nueva clave de estrato sin acceso, el UE 70 puede establecer opcionalmente un nuevo contexto de seguridad con la AMF 40 de destino (bloque 420), donde el nuevo contexto de seguridad incluye la nueva clave de estrato sin acceso y luego comunicarse con la AMF 40 de destino usando la nueva clave de estrato sin acceso (bloque 425).

Algunas realizaciones del método 350 comprenden además el establecimiento de un nuevo contexto de seguridad con el AMF 40 de destino, incluyendo el nuevo contexto de seguridad la nueva clave de estrato sin acceso y la comunicación con el AMF 40 de destino usando la nueva clave de estrato sin acceso.

Según la invención, en el método 400, el KCI comprende una bandera indicadora de cambio de clave establecida en un valor que indica que la clave del estrato sin acceso ha sido cambiada. El parámetro de seguridad comprende un parámetro de actualización. En la realización no reivindicada, el parámetro de seguridad comprende uno de un nonce, marca de tiempo y número de versión.

Algunas realizaciones del método 400 comprenden además recibir un KDP de la AMF 40 de destino y generar la nueva clave de estrato sin acceso usando el KDP. Según a invención el KDP comprende un parámetro de actualización. En la realización no reivindicada, el KDP comprende uno de un nonce, marca de tiempo y número de versión. En otro ejemplo, el KDP se recibe con el KCI.

En algunas realizaciones del método 400, generar la nueva clave de estrato sin acceso comprende generar la nueva clave de estrato sin acceso a partir de la clave de estrato sin acceso anterior. En otras realizaciones del método 400, generar la nueva clave de estrato sin acceso comprende generar la nueva clave de estrato sin acceso a partir de la clave de estrato sin acceso anterior y un KDP. Según la invención el KDP comprende un parámetro de actualización. En las realizaciones no reivindicadas, el KDP comprende al menos uno de un nonce, marca de tiempo y número de versión. En otras realizaciones, el KDP comprende información estática que es conocida por el UE 70 y la AMF 40 de origen.

Algunas realizaciones del método 400 comprenden además recibir un parámetro de algoritmo de seguridad desde la AMF 40 de destino que identifica uno o más algoritmos de seguridad usados en el nuevo contexto de seguridad. En un ejemplo, el parámetro del algoritmo de seguridad se recibe con el KCI.

En algunas realizaciones del método 400, la nueva clave de estrato sin acceso se recibe en un mensaje de establecimiento de seguridad.

En algunas realizaciones del método 400, la clave de estrato sin acceso comprende una clave de red de núcleo (KCN).

La Figura 22 es un ejemplo de UE 430 configurado para realizar el método 400 que se muestra en la Figura 21. El UE

430 comprende una unidad 435 de envío, una unidad 440 de recepción y una unidad 445 de generación de claves. La unidad 435 de envío está configurada para enviar un mensaje de registro u otro mensaje de control a una AMF 40 de destino en la red de comunicación inalámbrica. La unidad 440 de recepción está configurada para recibir, en respuesta al mensaje de registro u otro mensaje de control, un KCI que indica que se ha cambiado una clave de estrato sin acceso. La unidad 445 de generación de claves está configurada para generar, en respuesta al KCI, una nueva clave de estrato sin acceso. El UE 430 también puede incluir opcionalmente la unidad 450 de seguridad configurada para establecer un nuevo contexto de seguridad con la AMF 40 de destino y una unidad 350 de comunicación configurada para comunicarse con la AMF 40 de destino usando la nueva clave de estrato sin acceso. La unidad 435 de envío, la unidad 440 de recepción, la unidad 445 de generación de claves, la unidad 450 de seguridad y la unidad 455 de comunicación pueden comprender circuitos de hardware, microprocesadores y/o software configurados para realizar el método que se muestra en la Figura 9. En algunas realizaciones, la unidad 435 de envío, la unidad 440 de recepción, la unidad 445 de generación de claves, la unidad 450 de seguridad y la unidad 455 de comunicación están implementadas por un solo microprocesador. En otras realizaciones, la unidad 435 de envío, la unidad 440 de recepción, la unidad 445 de generación de claves, la unidad 450 de seguridad y la unidad 455 de comunicación pueden implementarse mediante dos o más microprocesadores.

La Figura 23 ilustra los principales componentes funcionales de la estación 500 base configurada para implementar los métodos de manejo del contexto de seguridad como se describe en el presente documento. La estación 500 base comprende un circuito 510 de procesamiento, una memoria 530 y un circuito 540 de interfaz.

El circuito 540 de interfaz incluye un circuito 545 de interfaz de radiofrecuencia (RF) acoplado a una o más antenas 550. El circuito 545 de interfaz de RF comprende los componentes de radiofrecuencia (RF) necesarios para comunicarse con los UE 70 a través de un canal de comunicación inalámbrico. Normalmente, los componentes de RF incluyen un transmisor y un receptor adaptados para comunicaciones según los estándares 5G u otra Tecnología de Acceso por Radio (RAT). El circuito 540 de interfaz incluye además un circuito 555 de interfaz de red para comunicarse con los nodos de la red de núcleo en la red 10 de comunicación inalámbrica.

El circuito 510 de procesamiento procesa las señales transmitidas o recibidas por la estación 500 base. Dicho procesamiento incluye la codificación y modulación de las señales transmitidas y la demodulación y decodificación de las señales recibidas. El circuito 510 de procesamiento puede comprender uno o más microprocesadores, hardware, firmware o una combinación de los mismos. El circuito 510 de procesamiento incluye una unidad 515 de movilidad para realizar funciones relacionadas con el traspaso. La unidad 515 de movilidad comprende el circuito de procesamiento dedicado a las funciones relacionadas con la movilidad. La unidad de 515 movilidad está configurada para realizar los métodos y procedimientos que se describen en el presente documento, incluidos los métodos que se muestran en las Figuras 2, 6, 7 y 9.

La memoria 530 comprende memoria tanto volátil como no volátil para almacenar el código del programa informático y los datos que necesita el circuito 510 de procesamiento para su funcionamiento. La memoria 530 puede comprender cualquier medio de almacenamiento tangible, no transitorio legible por ordenador para almacenar datos, incluido el almacenamiento de datos electrónicos, magnéticos, ópticos, electromagnéticos o de semiconductores. La memoria 530 almacena un programa 535 informático que comprende instrucciones ejecutables que configuran el circuito 510 de procesamiento para implementar los métodos y procedimientos descritos en este documento, incluido el método 100 según las Figuras 2, 6, 7 y 9. En general, las instrucciones del programa informático y la información de configuración se almacenan en una memoria no volátil, como una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable (EPROM) o una memoria flash. Los datos temporales generados durante la operación pueden almacenarse en una memoria volátil, como una memoria de acceso aleatorio (RAM). En algunas realizaciones, el programa 535 informático para configurar el circuito 510 de procesamiento como se describe en el presente documento puede almacenarse en una memoria extraíble, como un disco compacto portátil, un disco de vídeo digital portátil u otro medio extraíble. El programa 535 informático también puede incorporarse en un soporte tal como una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por ordenador.

La Figura 24 ilustra los componentes funcionales principales de un nodo 600 de red de núcleo en la red 10 de comunicación inalámbrica configurado para implementar el procedimiento de manejo de contexto de seguridad como se describe en este documento. El nodo 600 de red de núcleo puede usarse para implementar funciones de red de núcleo, tales como la AMF 40 de origen y la AMF 40 de destino como se describe en este documento. Los expertos en la materia apreciarán que una función de red de núcleo, como la AMF 40, puede implementarse mediante un solo nodo de red de núcleo, o puede distribuirse entre dos o más nodos de red de núcleo.

El nodo de red 600 de núcleo comprende un circuito 610 de procesamiento, una memoria 630 y un circuito 640 de interfaz. El circuito 640 de interfaz incluye un circuito 645 de interfaz de red para permitir la comunicación con otros nodos de red de núcleo y con estaciones 25 base en la RAN.

El circuito 610 de procesamiento controla el funcionamiento del nodo 600 de red de núcleo. El circuito 610 de procesamiento puede comprender uno o más microprocesadores, hardware, firmware o una combinación de los mismos. El circuito 610 de procesamiento puede incluir una unidad 615 de seguridad NAS para manejar funciones de seguridad relacionadas con NAS y una unidad 620 de gestión de movilidad para manejar funciones de gestión de movilidad. Generalmente, la unidad 615 de seguridad NAS es responsable de obtener claves de seguridad, establecer

un contexto de seguridad y otras funciones de seguridad relacionadas. La unidad 620 de gestión de movilidad es responsable de gestionar las funciones de gestión de movilidad y la señalización relacionada. Como se describió anteriormente, la unidad 615 de seguridad NAS puede proporcionar a la unidad 620 de gestión de movilidad información, como claves NAS, KDP y otros parámetros de seguridad para enviar al UE 70. En algunas realizaciones, la unidad 615 de seguridad NAS y la unidad 620 de gestión de la movilidad puede residir en el mismo nodo de red de núcleo. En otras realizaciones, pueden residir en diferentes nodos de la red de núcleo. En una realización ejemplar, la unidad 615 de seguridad NAS y la unidad 620 de gestión de movilidad están configuradas para realizar los métodos y procedimientos que se describen en el presente documento, incluidos los métodos que se muestran en las Figuras 2, 3, 6-8, 11, 13, 17 y 19.

La memoria 630 comprende memoria tanto volátil como no volátil para almacenar el código del programa informático y los datos que necesita el circuito 610 de procesamiento para su funcionamiento. La memoria 630 puede comprender cualquier medio de almacenamiento tangible, no transitorio legible por ordenador para almacenar datos, incluido el almacenamiento de datos electrónicos, magnéticos, ópticos, electromagnéticos o de semiconductores. La memoria 630 almacena un programa 635 informático que comprende instrucciones ejecutables que configuran el circuito 610 de procesamiento para implementar los métodos y procedimientos descritos en este documento, incluidos los métodos según las Figuras 2, 3, 6-8, 11, 13, 17 y 19. En general, las instrucciones de programa informático y la información de configuración se almacenan en una memoria no volátil, como una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable (EPROM) o una memoria flash. Los datos temporales generados durante la operación pueden almacenarse en una memoria volátil, como una memoria de acceso aleatorio (RAM). En algunas realizaciones, un programa informático 635 para configurar el circuito de procesamiento 610 como se describe en el presente documento puede almacenarse en una memoria extraíble, como un disco compacto portátil, un disco de vídeo digital portátil u otro medio extraíble. El programa 635 informático también puede incorporarse en un soporte tal como una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por ordenador.

La Figura 25 ilustra los principales componentes funcionales del UE 700 configurados para implementar los métodos de manejo del contexto de seguridad como se describe en el presente documento. El UE 700 comprende un circuito 710 de procesamiento, una memoria 730 y un circuito 740 de interfaz.

El circuito 740 de interfaz incluye un circuito 745 de interfaz de radiofrecuencia (RF) acoplado a una o más antenas 750. El circuito 745 de interfaz de RF comprende los componentes de radiofrecuencia (RF) necesarios para comunicarse con los UE 70 a través de un canal de comunicación inalámbrico. Normalmente, los componentes de RF incluyen un transmisor y un receptor adaptados para comunicaciones según los estándares 5G u otra Tecnología de Acceso por Radio (RAT).

El circuito 710 de procesamiento procesa las señales transmitidas o recibidas por el UE 700. Dicho procesamiento incluye la codificación y modulación de las señales transmitidas y la demodulación y decodificación de las señales recibidas. El circuito 710 de procesamiento puede comprender uno o más microprocesadores, hardware, firmware o una combinación de los mismos. El circuito 710 de procesamiento puede incluir una unidad 715 de seguridad NAS para manejar funciones de seguridad relacionadas con NAS y una unidad de gestión de movilidad 720 para manejar funciones de gestión de movilidad. Generalmente, la unidad 715 de seguridad NAS es responsable de derivar claves de seguridad, establecer un contexto de seguridad y otras funciones de seguridad como se describe en este documento. La unidad 720 de gestión de movilidad es responsable de gestionar las funciones de gestión de movilidad y la señalización relacionada. En una realización ejemplar, la unidad 715 de seguridad NAS y la unidad 720 de gestión de movilidad están configuradas para realizar los métodos y procedimientos que se describen en el presente documento, incluidos los métodos que se muestran en las Figuras 2, 3, 6-8, 15 y 21.

La memoria 730 comprende memoria tanto volátil como no volátil para almacenar el código del programa informático y los datos que necesita el circuito 710 de procesamiento para su funcionamiento. La memoria 730 puede comprender cualquier medio de almacenamiento tangible, no transitorio legible por ordenador para almacenar datos, incluido el almacenamiento de datos electrónicos, magnéticos, ópticos, electromagnéticos o de semiconductores. La memoria 730 almacena un programa 735 informático que comprende instrucciones ejecutables que configuran el circuito 710 de procesamiento para implementar los métodos y procedimientos descritos en este documento, incluido el método 100 según las Figuras 2, 3, 6-8, 15 y 21. En general, las instrucciones y la configuración del programa informático la información se almacena en una memoria no volátil, como una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable (EPROM) o una memoria flash. Los datos temporales generados durante la operación pueden almacenarse en una memoria volátil, como una memoria de acceso aleatorio (RAM). En algunas realizaciones, el programa 735 informático para configurar el circuito 710 de procesamiento como se describe en el presente documento puede almacenarse en una memoria extraíble, como un disco compacto portátil, un disco de vídeo digital portátil u otro medio extraíble. El programa 735 informático también puede incorporarse en un soporte tal como una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por ordenador.

REIVINDICACIONES

1. Un método (300) para transferir un contexto de seguridad para un equipo (70, 430, 700) de usuario en modo inactivo, implementado el método por uno o más nodos (320, 600) de red de núcleo en una red (30) de núcleo de una red (10) de comunicación inalámbrica, en donde uno o más nodos de red (320, 600) de núcleo proporcionan una Función (40) de Gestión de Movilidad y Acceso , AMF, de origen, comprendiendo el método:

recibir (305), desde una AMF (40) de destino, una solicitud de un contexto de seguridad para el equipo (70, 430, 700) de usuario;

generar (310) una nueva clave de estrato sin acceso en respuesta a la determinación de que se cumple una política de seguridad específica del operador, en donde la nueva clave de estrato sin acceso se genera utilizando una clave de estrato sin acceso y un parámetro de actualización; y

enviar (315), en respuesta a la solicitud, la nueva clave de estrato sin acceso y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave al AMF (40) de destino, en donde la bandera indicadora de cambio de clave se establece en un valor que indica que se ha cambiado la clave de estrato sin acceso.

2. El método (300) de la reivindicación 1, que comprende además enviar uno o más parámetros de seguridad con la nueva clave de estrato sin acceso a la AMF (40) de destino.

3. El método (300) de la reivindicación 2, en donde uno o más parámetros de seguridad incluyen información sobre la capacidad del equipo de usuario.

4. El método (300) de una cualquiera de las reivindicaciones 1-3, en donde la clave de estrato sin acceso es una clave de red de núcleo (K_{CN}).

5. Un nodo (320, 600) de red de núcleo en una red (30) de núcleo de una red (10) de comunicaciones inalámbricas, proporcionando el nodo (600) de red de núcleo una Función (40) de Gestión de Acceso y Movilidad, AMF, de origen, estando el nodo (600) de red de núcleo configurado para:

recibir, desde una AMF (40) de destino, una solicitud de un contexto de seguridad para un equipo (70, 430, 700) de usuario en un modo inactivo;

generar una nueva clave de estrato sin acceso, usando una clave de estrato sin acceso y un parámetro de actualización, en respuesta a la determinación de que se cumple una política de seguridad específica de operador; y

enviar, en respuesta a la solicitud, la nueva clave de estrato sin acceso y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave a la AMF (40) de destino, en donde la bandera indicadora de cambio de clave se establece en un valor que indica que se ha cambiado una clave de estrato sin acceso.

6. Un programa (635) informático que comprende instrucciones ejecutables que, cuando son ejecutadas por un circuito (610) de procesamiento en un nodo (320, 600) de red de núcleo de una red (10) de comunicación inalámbrica, hace que el nodo (600) de red de núcleo realice el método según cualquiera de las reivindicaciones 1 - 4.

7. Un método (350) para transferir un contexto de seguridad de un equipo (70, 430, 700) de usuario durante un modo inactivo, implementado el método por uno o más nodos (600) de red de núcleo en una red (30) de núcleo de una red (10) de comunicación inalámbrica, en donde el uno o más nodos (600) de red de núcleo proporcionan una Función (40) de Gestión de Acceso y Movilidad , AMF, de destino, comprendiendo el método:

recibir (355), desde el equipo (70, 430, 700) de usuario, un mensaje de registro que indica un cambio de AMF (40);

solicitar (360) un contexto de seguridad para el equipo (70, 430, 700) de usuario desde una AMF (40) de origen;

recibir (365) de la AMF (40) de origen, en respuesta a la solicitud y a la AMF (40) de origen que determina que se cumple una política de seguridad específica de operador, una nueva clave de estrato sin acceso generada por la AMF de origen, y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave establecida en un valor que indica que se ha cambiado una clave de estrato sin acceso; y

enviar (370) la indicación de cambio de clave y un parámetro de actualización al equipo (70, 430, 700) de usuario.

8. El método (350) de la reivindicación 7, que comprende además establecer un nuevo contexto de seguridad que incluye la nueva clave de estrato sin acceso.

9. Un nodo (380, 600) de red de núcleo en una red (30) de núcleo de una red (10) de comunicación inalámbrica, proporcionando dicho nodo (380, 600) de red de núcleo una Función (40) de Gestión de Acceso y Movilidad , AMF, de destino, comprendiendo dicho nodo (380, 600) de red de núcleo :

un circuito (640) de interfaz para comunicarse con un equipo (70, 430, 700) de usuario y una AMF (40) de origen;

un circuito (610) de procesamiento configurado para:

recibir, desde el equipo (70, 430, 700) de usuario en un modo inactivo, un mensaje de registro que indica un cambio de AMF (40);

solicitar un contexto de seguridad de la AMF (40) de origen;

recibir desde la AMF (40) de origen, en respuesta a la solicitud y a la AMF de origen que determina que se cumple una política de seguridad específica de operador, una nueva clave de estrato sin acceso generada por la AMF de origen, y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave establecida en un valor que indica que se ha cambiado una clave de estrato sin acceso; y

enviar la indicación de cambio de clave y un parámetro de actualización al equipo (70, 430, 700) de usuario.

10. Un método (400) implementado por un equipo (70, 430, 700) de usuario durante un modo inactivo, comprendiendo el método:

enviar (405) un mensaje de registro a una Función (40) de Gestión de Acceso y Movilidad , AMF, de destino, en una red (10) de comunicación inalámbrica;

recibir (410) desde la AMF (40) de destino, en respuesta al mensaje de registro enviado, un parámetro de actualización y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave que tiene un valor que indica que una clave de estrato sin acceso ha sido cambiada por una AMF de origen con base en una política de seguridad específica de operador; y

generar (420), en respuesta a la indicación de cambio de clave, una nueva clave de estrato sin acceso usando una clave de estrato sin acceso y el parámetro de actualización.

11. El método (400) de la reivindicación 10, que comprende además:

establecer (420) un nuevo contexto de seguridad con la AMF (40) de destino, incluyendo el nuevo contexto de seguridad la nueva clave de estrato sin acceso; y

comunicarse (425) con la AMF (40) de destino usando la nueva clave de estrato sin acceso.

12. Un equipo (70, 430, 700) de usuario en una red (10) de comunicación inalámbrica, estando configurado el equipo (70, 430, 700) de usuario para, durante el modo inactivo:

enviar un mensaje de registro a una Función (40) de Gestión de Acceso y Movilidad , AMF, de destino;

recibir desde la AMF (40) de destino, en respuesta al mensaje de registro enviado, un parámetro de actualización y una indicación de cambio de clave que comprende una bandera indicadora de cambio de clave establecida en un valor que indica que una clave de estrato sin acceso ha sido cambiada por una AMF de origen con base en una política de seguridad específica de operador; y

generar, en respuesta a la indicación de cambio de clave, una nueva clave de estrato sin acceso usando una clave de estrato sin acceso y el parámetro de actualización.

13. Un programa informático que comprende instrucciones ejecutables que, cuando es ejecutado por un circuito de procesamiento en un equipo (70, 430, 700) de usuario en una red (10) de comunicación inalámbrica, hace que el equipo (70, 430, 700) de usuario realice el método de la reivindicación 10.

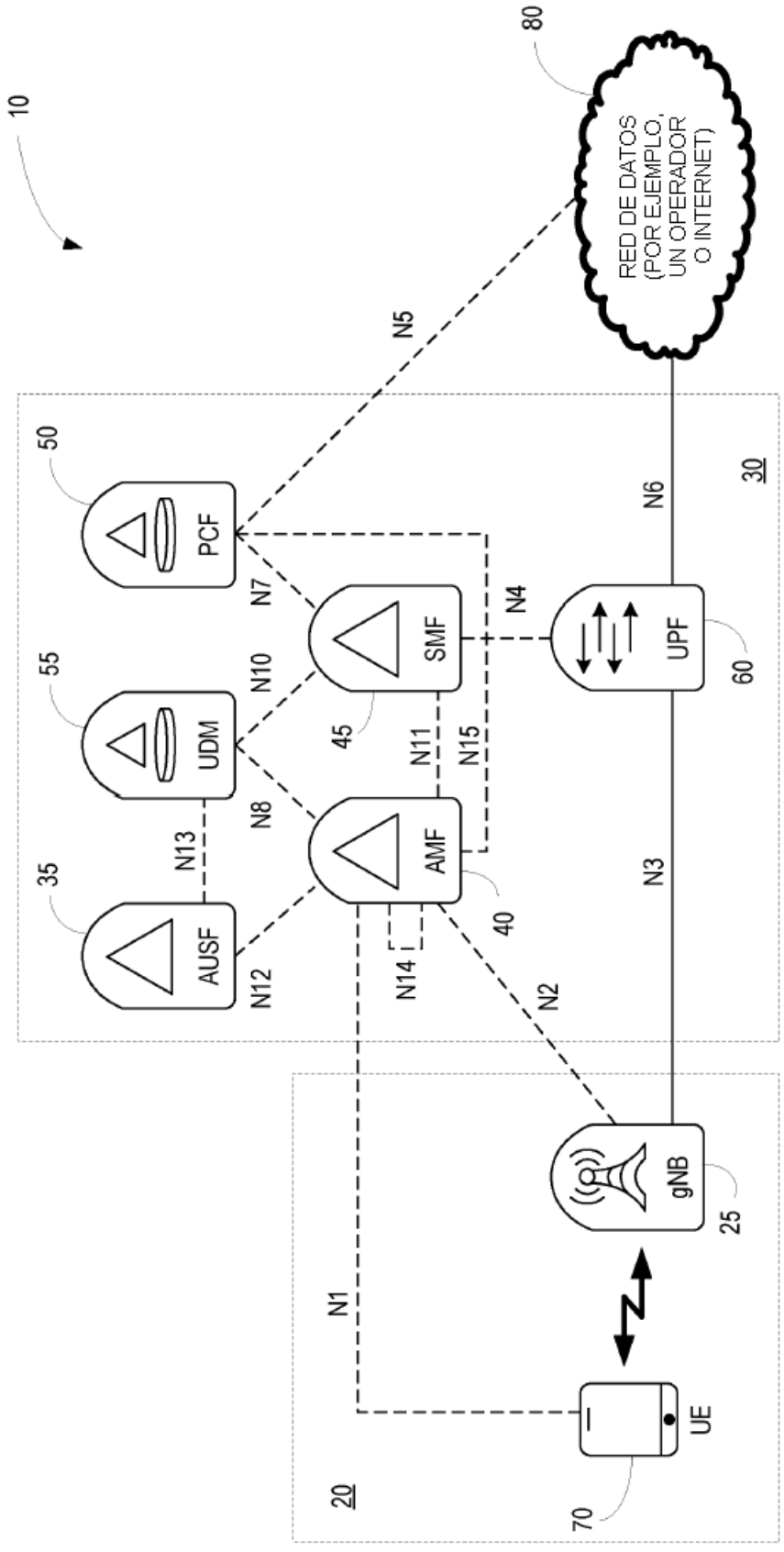
10
80
RED DE DATOS (POR EJEMPLO, UN OPERADOR O INTERNET)
N5
50
PCF
N7
SMF
N4
UPF
N6
30
55
UDM
N10
45
N11
N15
60
N8
AMF
N13
35
AUSF
N12
N14
40
N2
N3
gNB
25
N1
UE
20
70

Figura 1

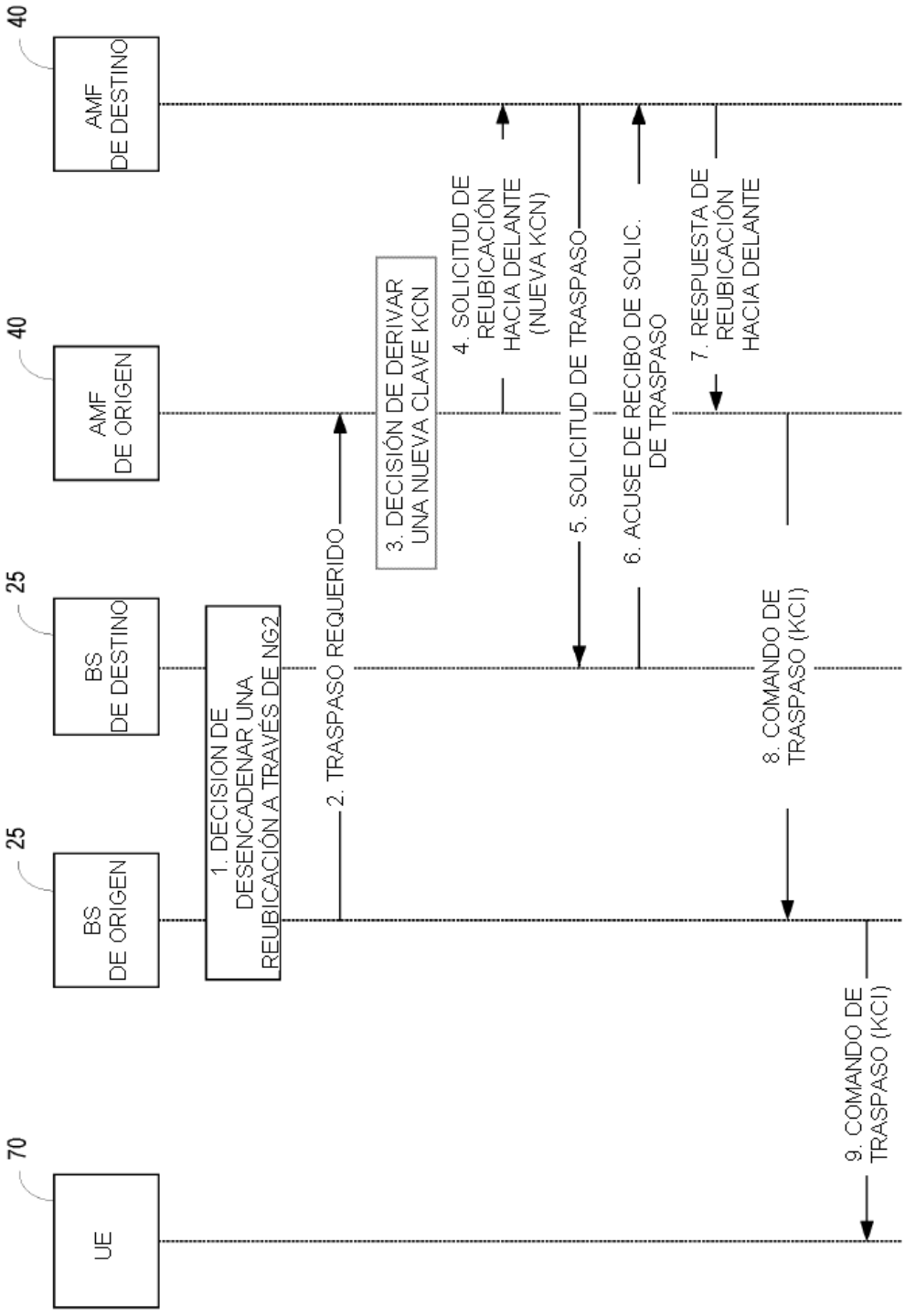
70
UE
25
BS
DE ORIGEN
25
BS
DE DESTINO
40
AMF
DE ORIGEN
40
AMF
DE DESTINO
1. DECISION DE
DESENCADENAR UNA
REUBICACIÓN A TRAVÉS DE NG2
2. TRASPASO REQUERIDO
3. DECISIÓN DE DERIVAR
UNA NUEVA CLAVE KCN
4. SOLICITUD DE
REUBICACIÓN
HACIA DELANTE
(NUEVA KCN)
5. SOLICITUD DE TRASPASO
6. ACUSE DE RECIBO DE SOLIC.
DE TRASPASO
7. RESPUESTA DE
REUBICACIÓN
HACIA DELANTE
8. COMANDO DE
TRASPASO (KCI)
9. COMANDO DE
TRASPASO (KCI)

Figura 2

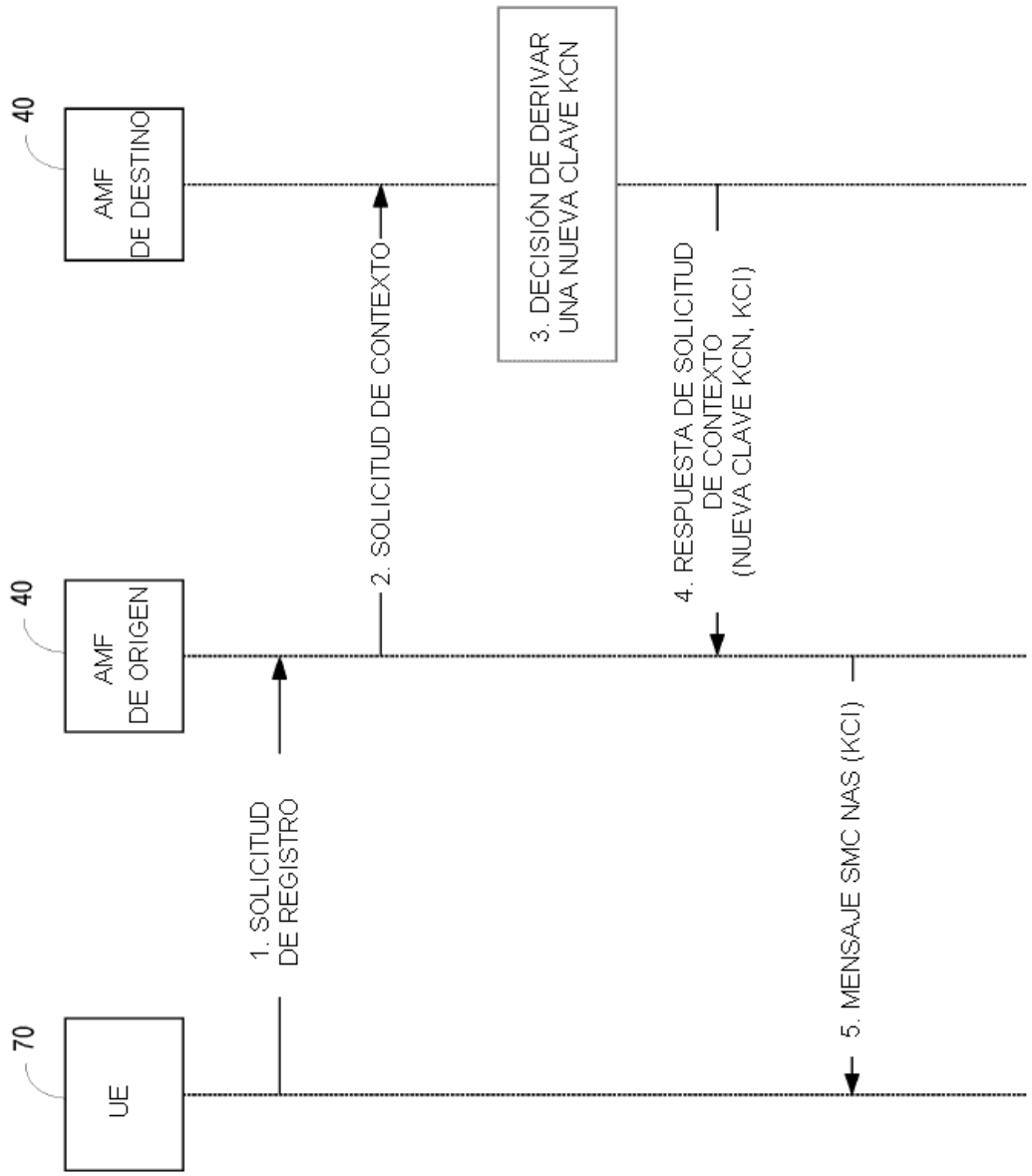
70
UE
40
AMF
DE ORIGEN
40
AMF
DE DESTINO
1. SOLICITUD
DE REGISTRO
2. SOLICITUD DE CONTEXTO
3. DECISIÓN DE DERIVAR
UNA NUEVA CLAVE KCN
4. RESPUESTA DE SOLICITUD
DE CONTEXTO
(NUEVA CLAVE KCN, KCI)
5. MENSAJE SMC NAS (KCI)

Figura 3

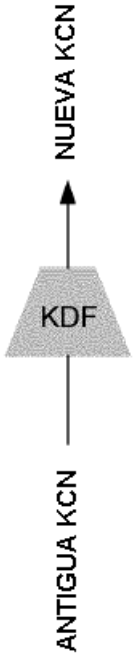

Figura 4

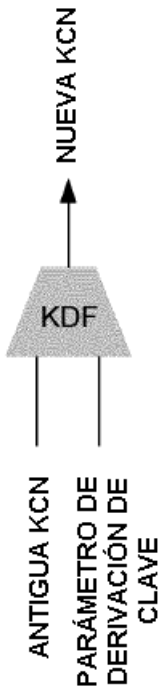

Figura 5

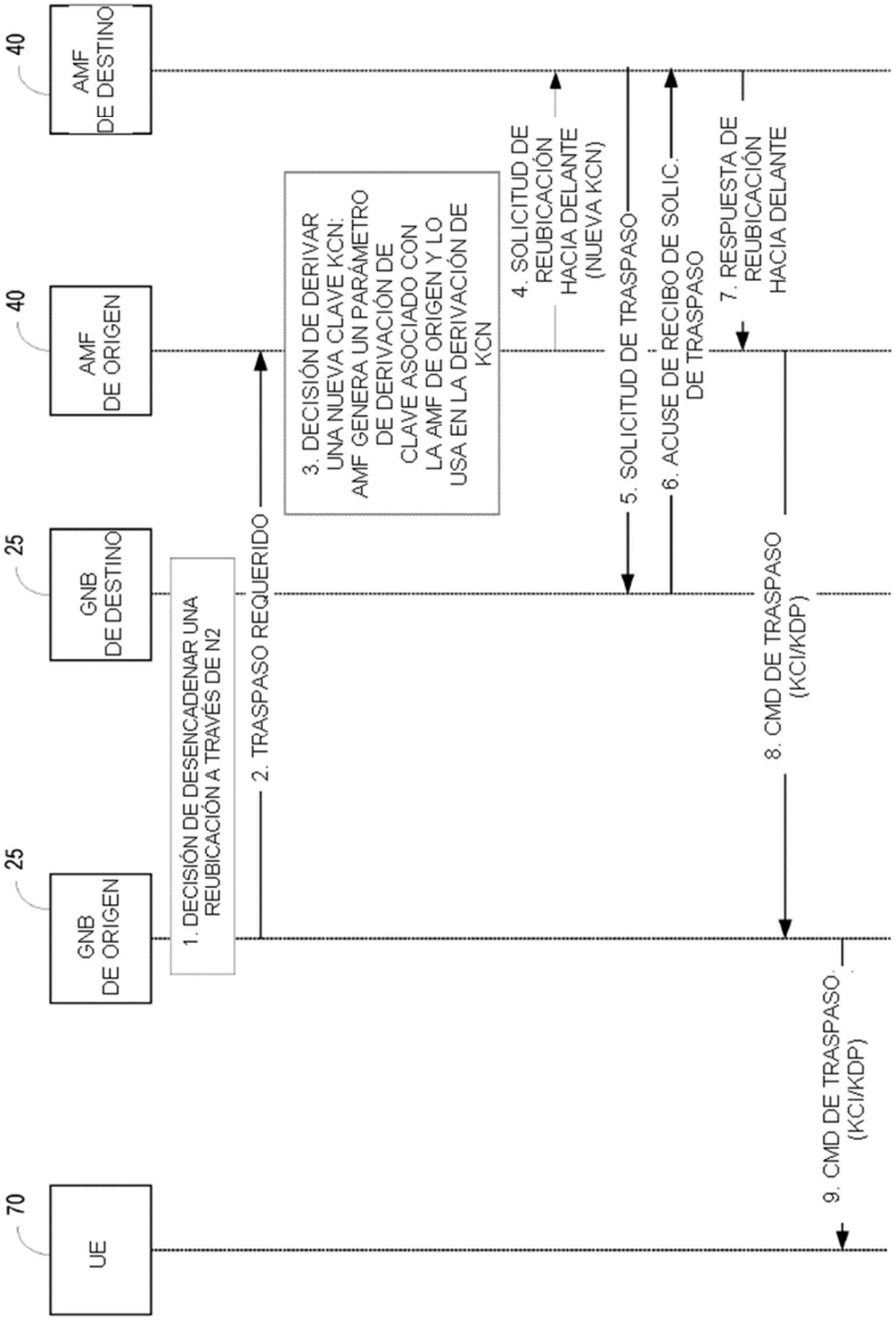
70
UE
25
GNB
DE ORIGEN
25
GNB
DE DESTINO
40
AMF
DE ORIGEN
40
AMF
DE DESTINO
1. DECISIÓN DE DESENCADENAR UNA REUBICACIÓN A TRAVÉS DE N2
2. TRASPASO REQUERIDO
3. DECISIÓN DE DERIVAR UNA NUEVA CLAVE KCN: AMF GENERA UN PARÁMETRO DE DERIVACIÓN DE CLAVE ASOCIADO CON LA AMF DE ORIGEN Y LO USA EN LA DERIVACIÓN DE KCN
4. SOLICITUD DE REUBICACIÓN HACIA DELANTE (NUEVA KCN)
5. SOLICITUD DE TRASPASO
6. ACUSE DE RECIBO DE SOLIC. DE TRASPASO
7. RESPUESTA DE REUBICACIÓN HACIA DELANTE
8. CMD DE TRASPASO (KCI/KDP)
9. CMD DE TRASPASO (KCI/KDP)

Figura 6

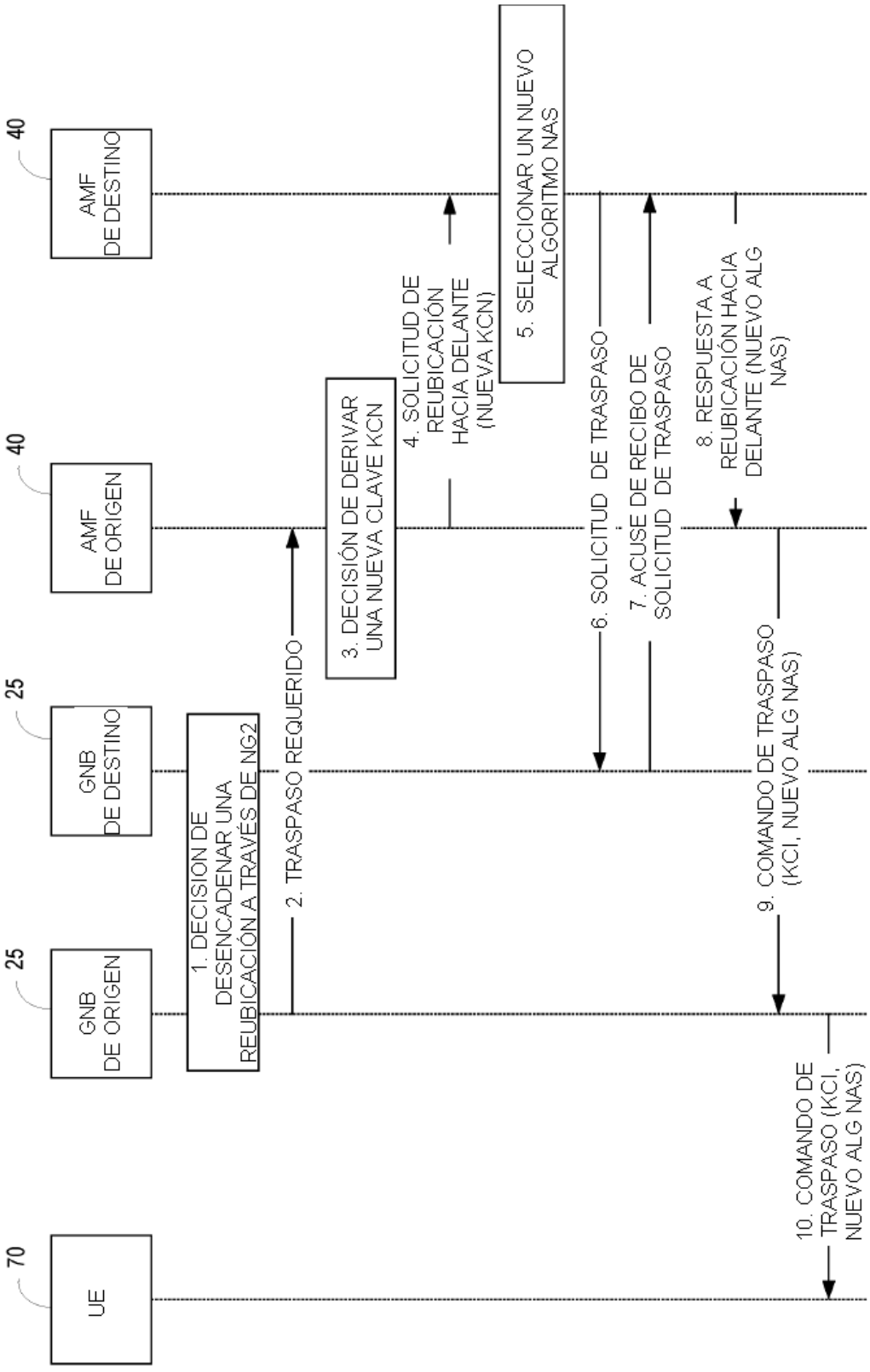
70
UE
25
GNB
DE ORIGEN
25
GNB
DE DESTINO
40
AMF
DE ORIGEN
40
AMF
DE DESTINO
1. DECISION DE DESENCADENAR UNA REUBICACIÓN A TRAVÉS DE NG2
2. TRASPASO REQUERIDO
3. DECISIÓN DE DERIVAR UNA NUEVA CLAVE KCN
4. SOLICITUD DE REUBICACIÓN HACIA DELANTE (NUEVA KCN)
5. SELECCIONAR UN NUEVO ALGORITMO NAS
6. SOLICITUD DE TRASPASO
7. ACUSE DE RECIBO DE SOLICITUD DE TRASPASO
8. RESPUESTA A REUBICACIÓN HACIA DELANTE (NUEVO ALG NAS)
9. COMANDO DE TRASPASO (KCI, NUEVO ALG NAS)
10. COMANDO DE TRASPASO (KCI, NUEVO ALG NAS)

Figura 7

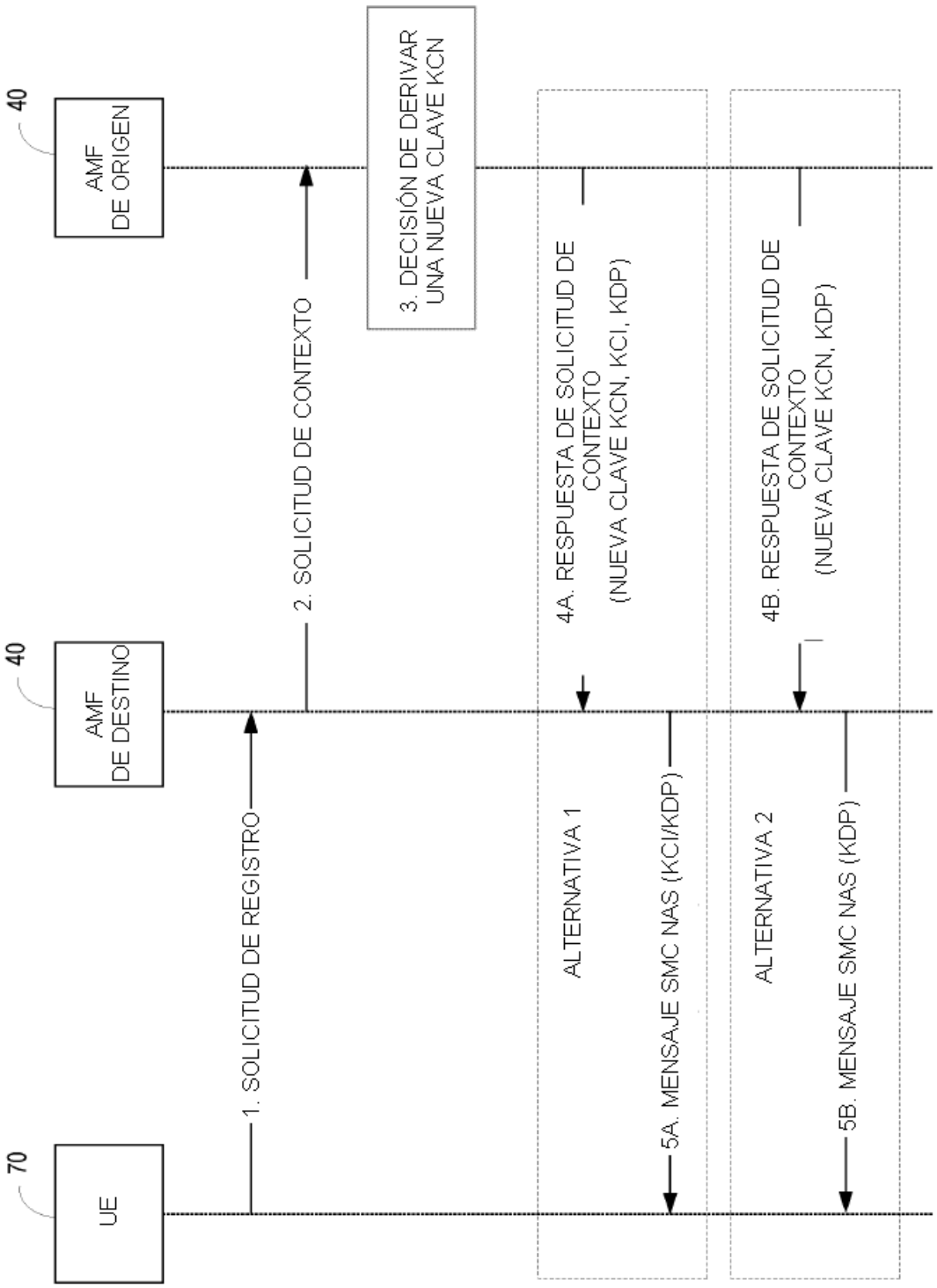
70
UE
40
AMF
DE DESTINO
40
AMF
DE ORIGEN
1. SOLICITUD DE REGISTRO
2. SOLICITUD DE CONTEXTO
3. DECISIÓN DE DERIVAR
UNA NUEVA CLAVE KCN
ALTERNATIVA 1
4A. RESPUESTA DE SOLICITUD DE
CONTEXTO
(NUEVA CLAVE KCN, KCI, KDP)
5A. MENSAJE SMC NAS (KCI/KDP)
ALTERNATIVA 2
4B. RESPUESTA DE SOLICITUD DE
CONTEXTO
(NUEVA CLAVE KCN, KDP)
5B. MENSAJE SMC NAS (KDP)

Figura 8

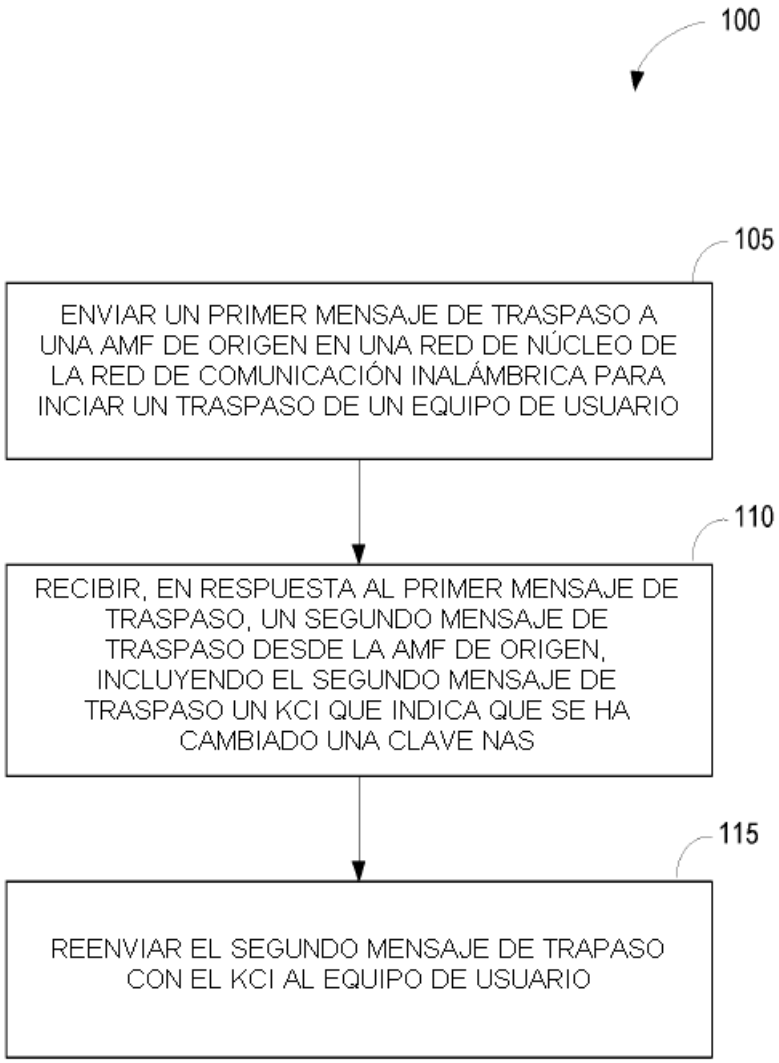
100
105
ENVIAR UN PRIMER MENSAJE DE TRASPASO A UNA AMF DE ORIGEN EN UNA RED DE NÚCLEO DE LA RED DE COMUNICACIÓN INALÁMBRICA PARA INICIAR UN TRASPASO DE UN EQUIPO DE USUARIO
110
RECIBIR, EN RESPUESTA AL PRIMER MENSAJE DE TRASPASO, UN SEGUNDO MENSAJE DE TRASPASO DESDE LA AMF DE ORIGEN, INCLUYENDO EL SEGUNDO MENSAJE DE TRASPASO UN KCI QUE INDICA QUE SE HA CAMBIADO UNA CLAVE NAS
115
REENVIAR EL SEGUNDO MENSAJE DE TRAPASO CON EL KCI AL EQUIPO DE USUARIO

Figura 9

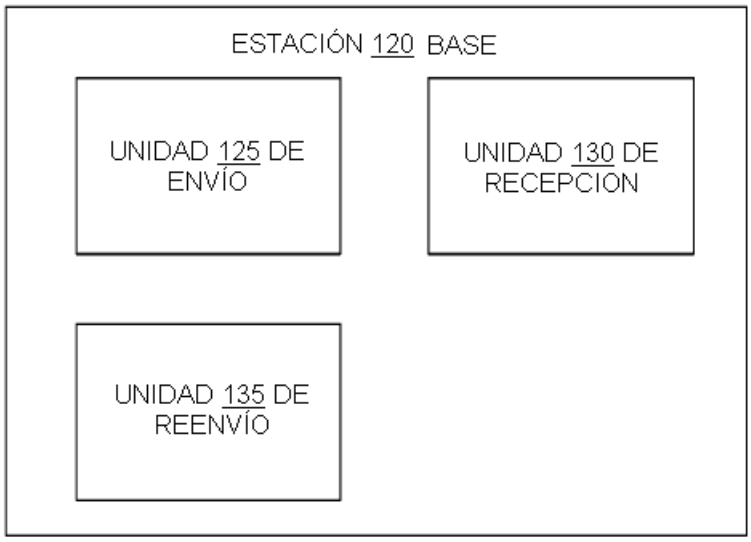

Figura 10

Figura 12

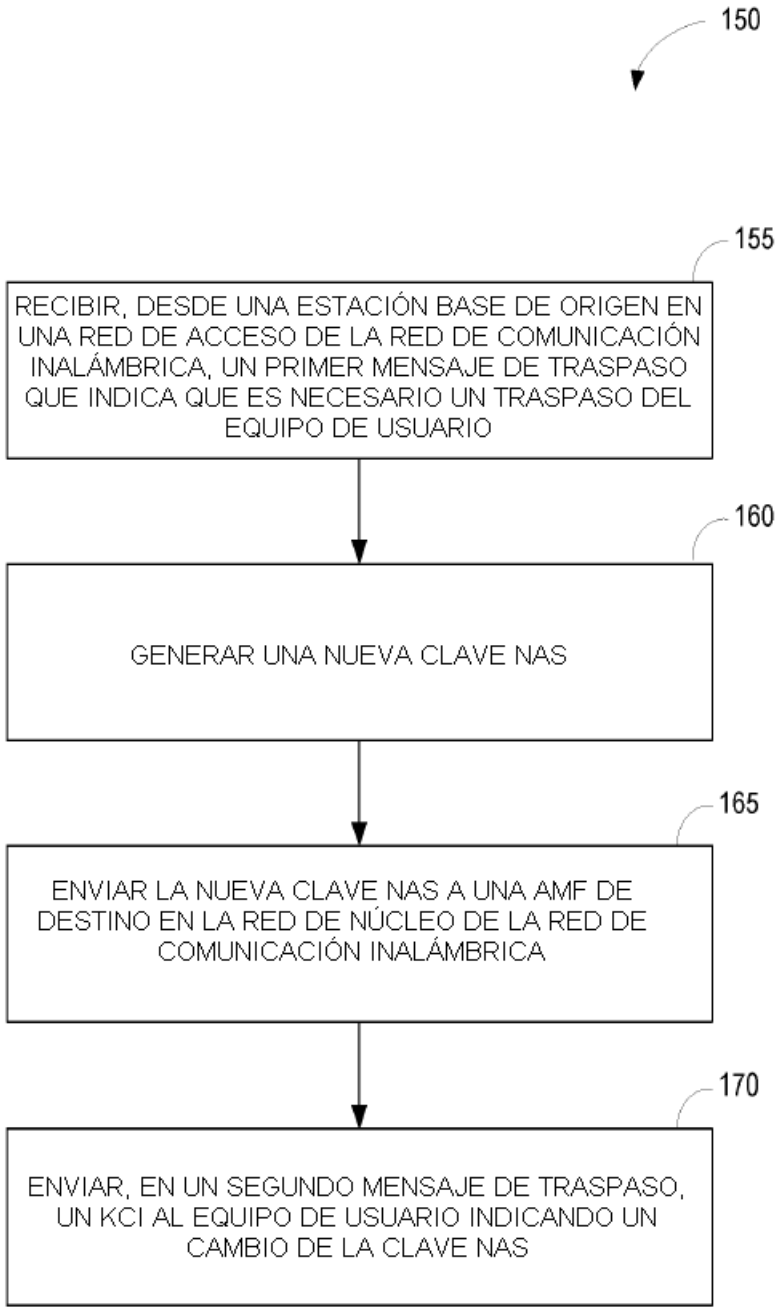
150
155
RECIBIR, DESDE UNA ESTACIÓN BASE DE ORIGEN EN UNA RED DE ACCESO DE LA RED DE COMUNICACIÓN INALÁMBRICA, UN PRIMER MENSAJE DE TRASPASO QUE INDICA QUE ES NECESARIO UN TRASPASO DEL EQUIPO DE USUARIO
160
GENERAR UNA NUEVA CLAVE NAS
165
ENVIAR LA NUEVA CLAVE NAS A UNA AMF DE DESTINO EN LA RED DE NÚCLEO DE LA RED DE COMUNICACIÓN INALÁMBRICA
170
ENVIAR, EN UN SEGUNDO MENSAJE DE TRASPASO, UN KCI AL EQUIPO DE USUARIO INDICANDO UN CAMBIO DE LA CLAVE NAS

Figura 11

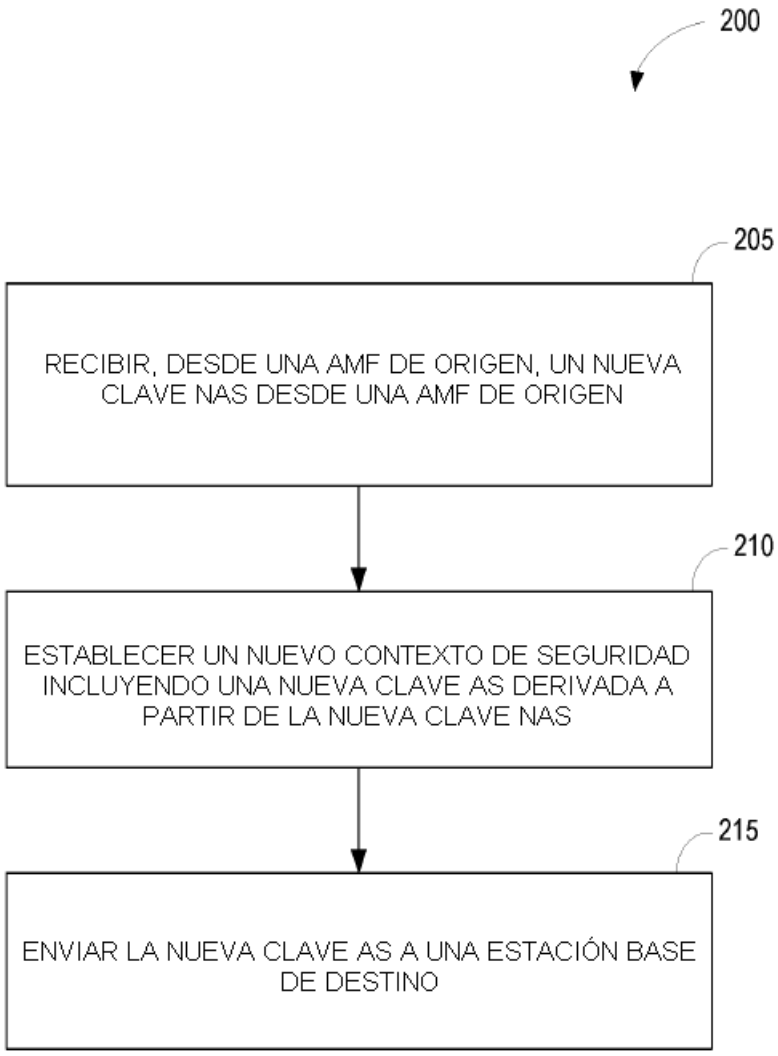
200
205
RECIBIR, DESDE UNA AMF DE ORIGEN, UN NUEVA CLAVE NAS DESDE UNA AMF DE ORIGEN
210
ESTABLECER UN NUEVO CONTEXTO DE SEGURIDAD INCLUYENDO UNA NUEVA CLAVE AS DERIVADA A PARTIR DE LA NUEVA CLAVE NAS
215
ENVIAR LA NUEVA CLAVE AS A UNA ESTACIÓN BASE DE DESTINO

Figura 13

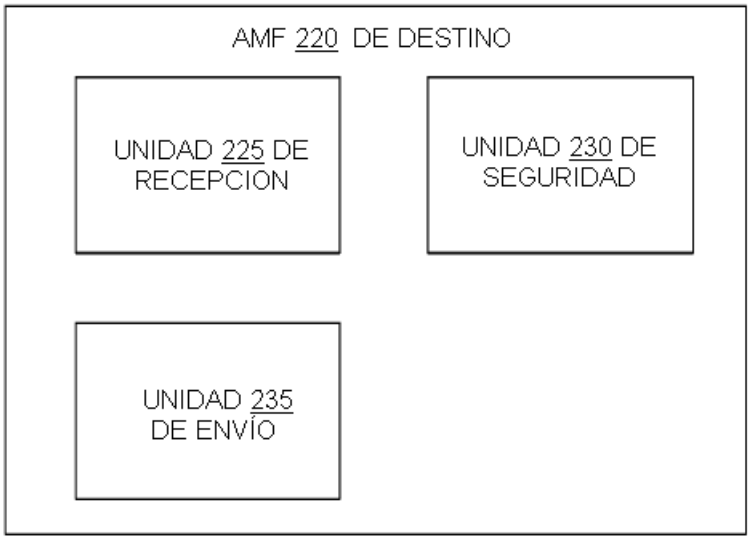

Figura 14

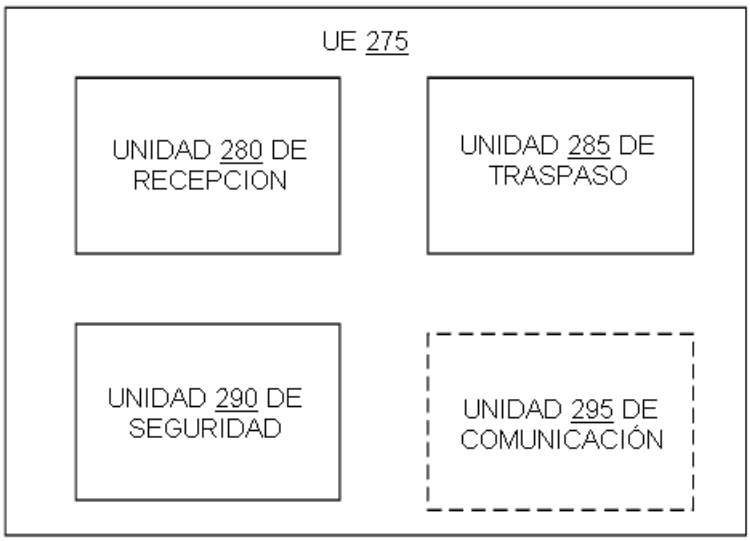

Figura 16

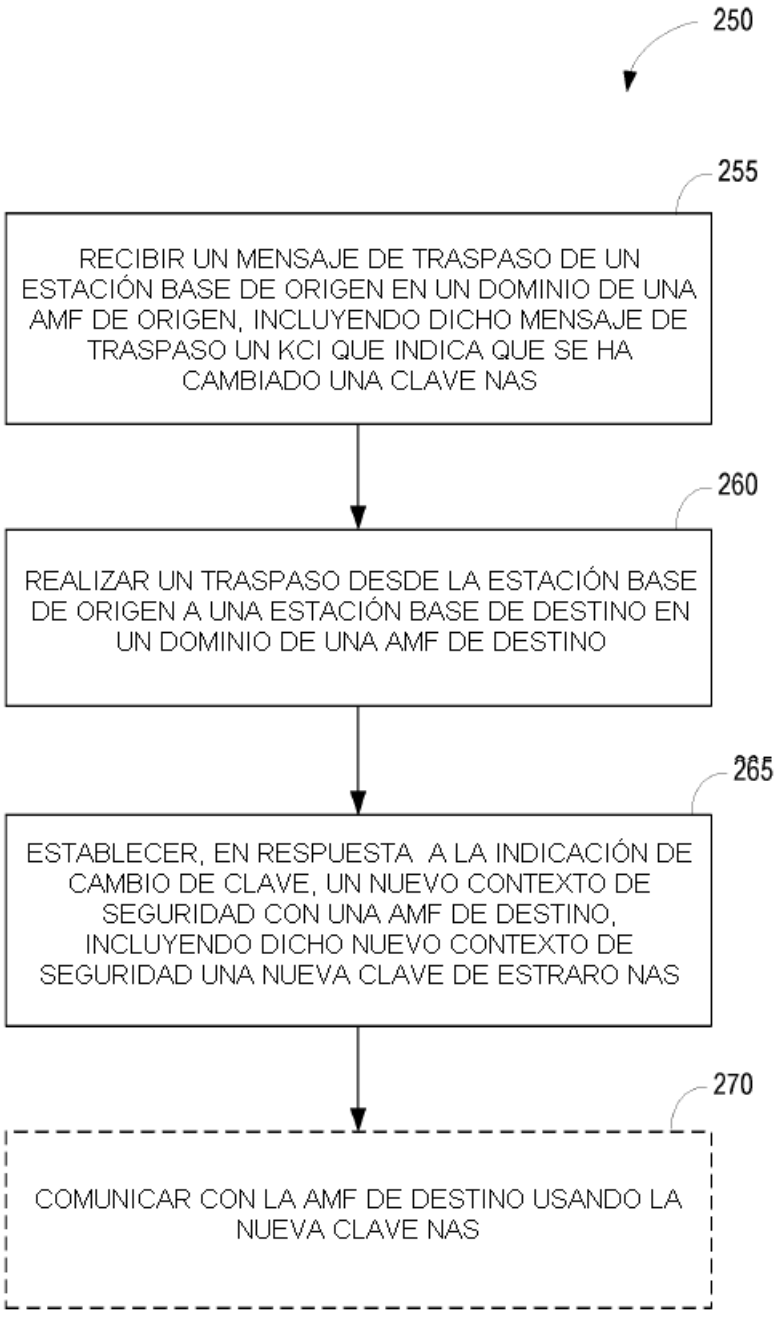
250
255
RECIBIR UN MENSAJE DE TRASPASO DE UN ESTACIÓN BASE DE ORIGEN EN UN DOMINIO DE UNA AMF DE ORIGEN, INCLUYENDO DICHO MENSAJE DE TRASPASO UN KCI QUE INDICA QUE SE HA CAMBIADO UNA CLAVE NAS
260
REALIZAR UN TRASPASO DESDE LA ESTACIÓN BASE DE ORIGEN A UNA ESTACIÓN BASE DE DESTINO EN UN DOMINIO DE UNA AMF DE DESTINO
265
ESTABLECER, EN RESPUESTA A LA INDICACIÓN DE CAMBIO DE CLAVE, UN NUEVO CONTEXTO DE SEGURIDAD CON UNA AMF DE DESTINO, INCLUYENDO DICHO NUEVO CONTEXTO DE SEGURIDAD UNA NUEVA CLAVE DE ESTRARO NAS
270
COMUNICAR CON LA AMF DE DESTINO USANDO LA NUEVA CLAVE NAS

Figura 15

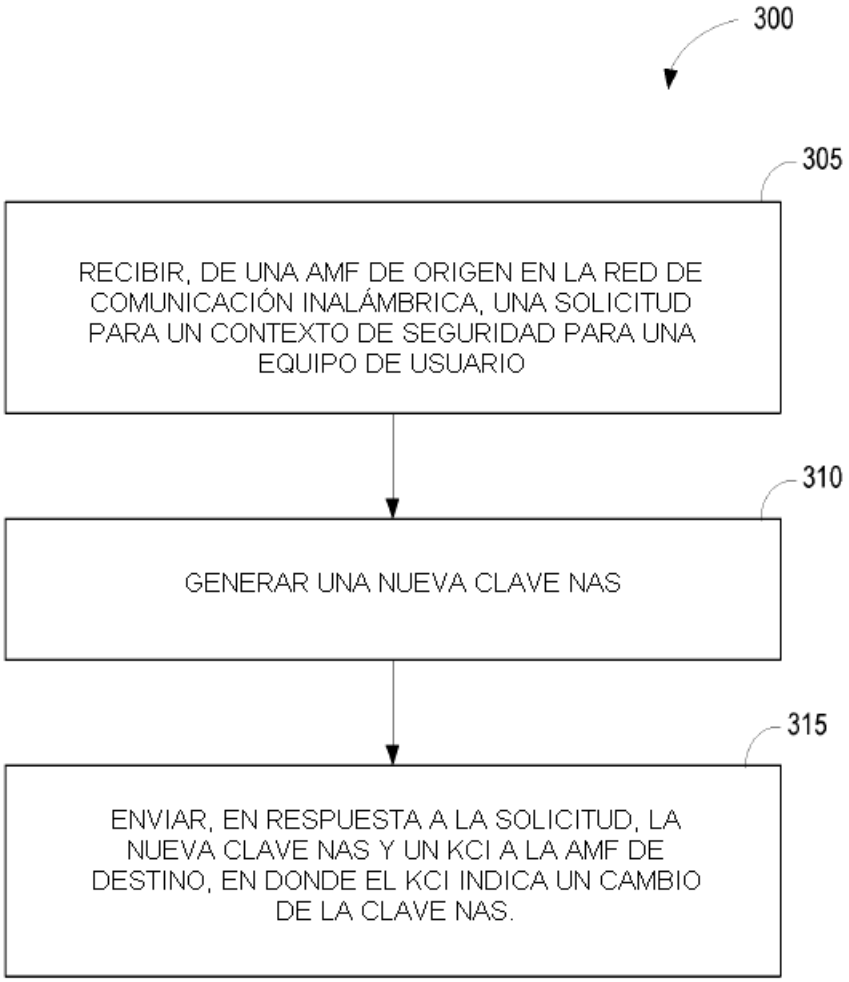
300
305
RECIBIR, DE UNA AMF DE ORIGEN EN LA RED DE COMUNICACIÓN INALÁMBRICA, UNA SOLICITUD PARA UN CONTEXTO DE SEGURIDAD PARA UNA EQUIPO DE USUARIO
310
GENERAR UNA NUEVA CLAVE NAS
315
ENVIAR, EN RESPUESTA A LA SOLICITUD, LA NUEVA CLAVE NAS Y UN KCI A LA AMF DE DESTINO, EN DONDE EL KCI INDICA UN CAMBIO DE LA CLAVE NAS.

Figura 17

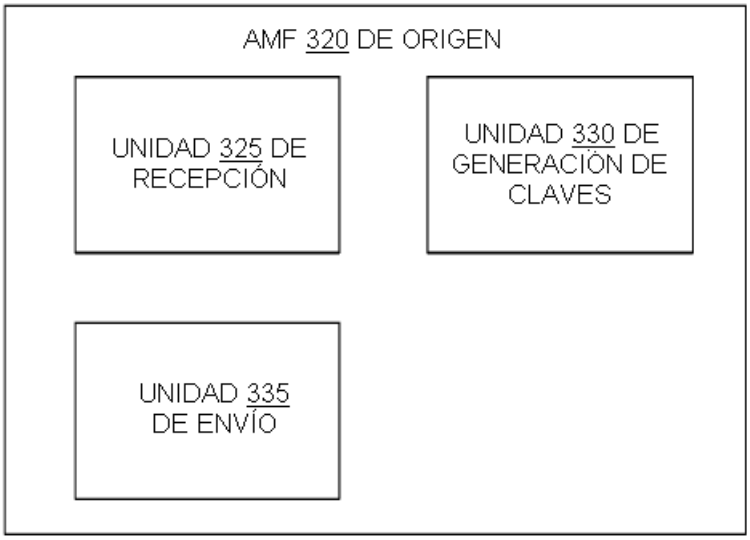

Figura 18

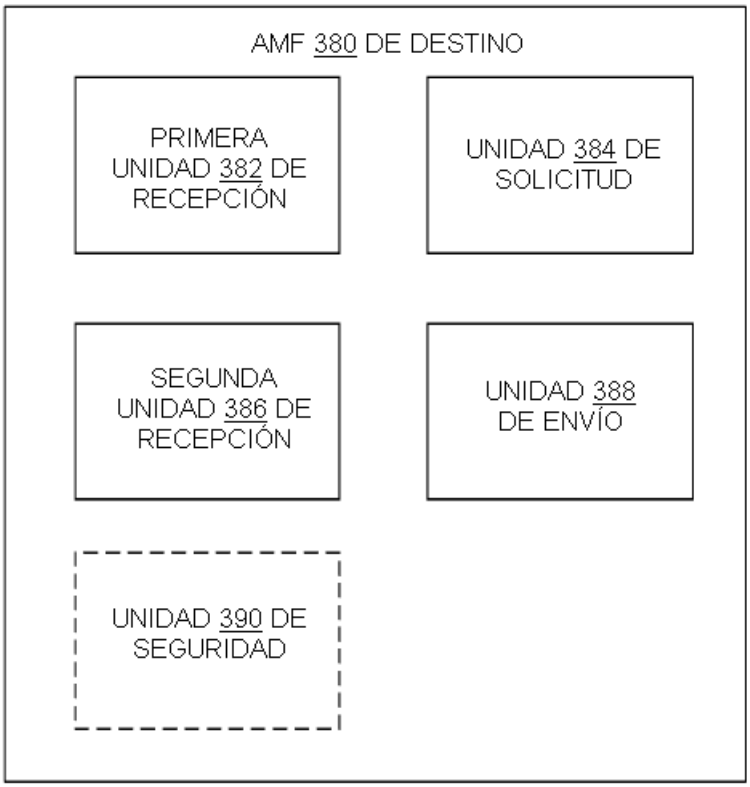

Figura 20

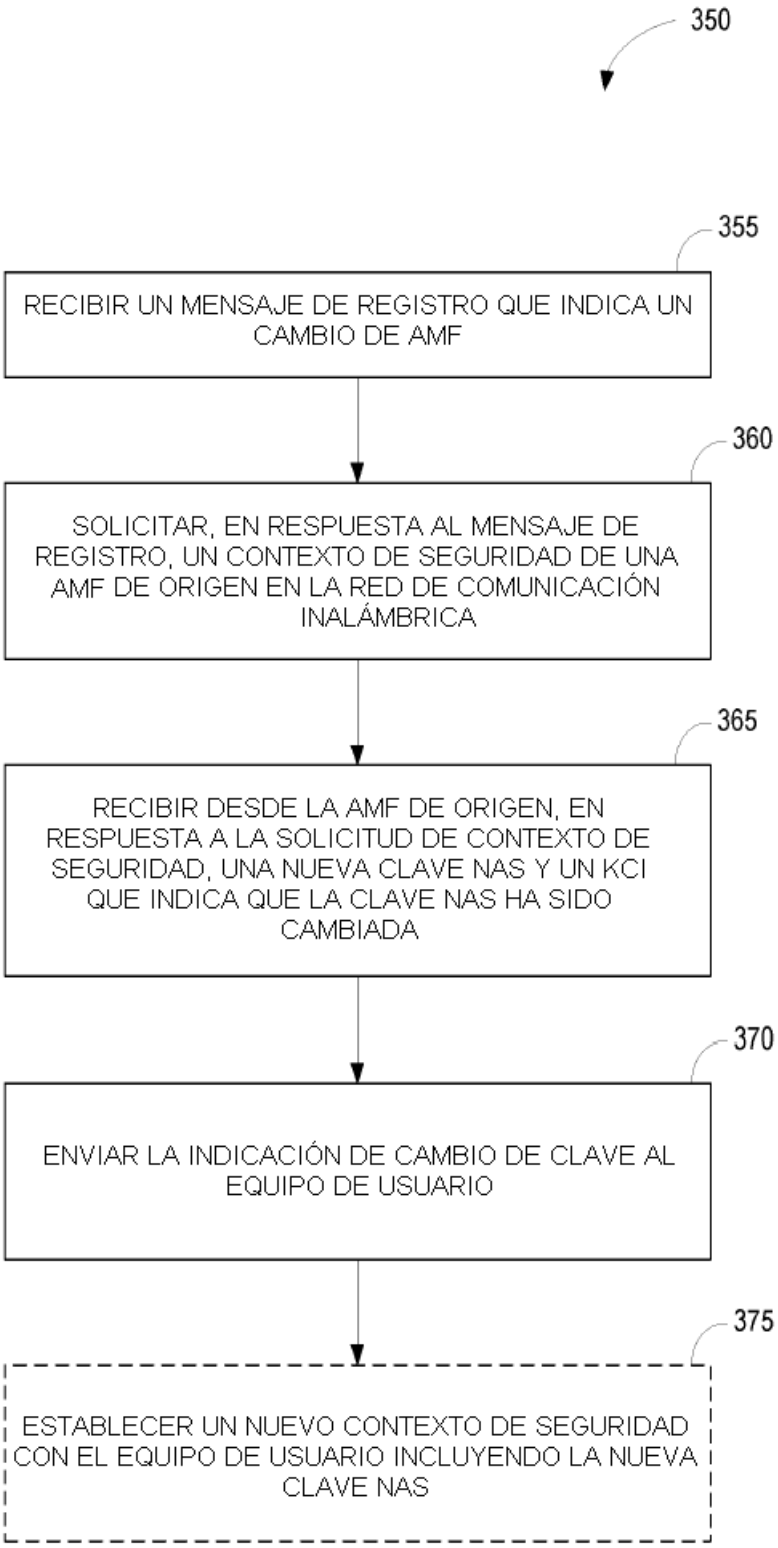
350
355
RECIBIR UN MENSAJE DE REGISTRO QUE INDICA UN CAMBIO DE AMF
360
SOLICITAR, EN RESPUESTA AL MENSAJE DE REGISTRO, UN CONTEXTO DE SEGURIDAD DE UNA AMF DE ORIGEN EN LA RED DE COMUNICACIÓN INALÁMBRICA
365
RECIBIR DESDE LA AMF DE ORIGEN, EN RESPUESTA A LA SOLICITUD DE CONTEXTO DE SEGURIDAD, UNA NUEVA CLAVE NAS Y UN KCI QUE INDICA QUE LA CLAVE NAS HA SIDO CAMBIADA
370
ENVIAR LA INDICACIÓN DE CAMBIO DE CLAVE AL EQUIPO DE USUARIO
375
ESTABLECER UN NUEVO CONTEXTO DE SEGURIDAD CON EL EQUIPO DE USUARIO INCLUYENDO LA NUEVA CLAVE NAS

Figura 19

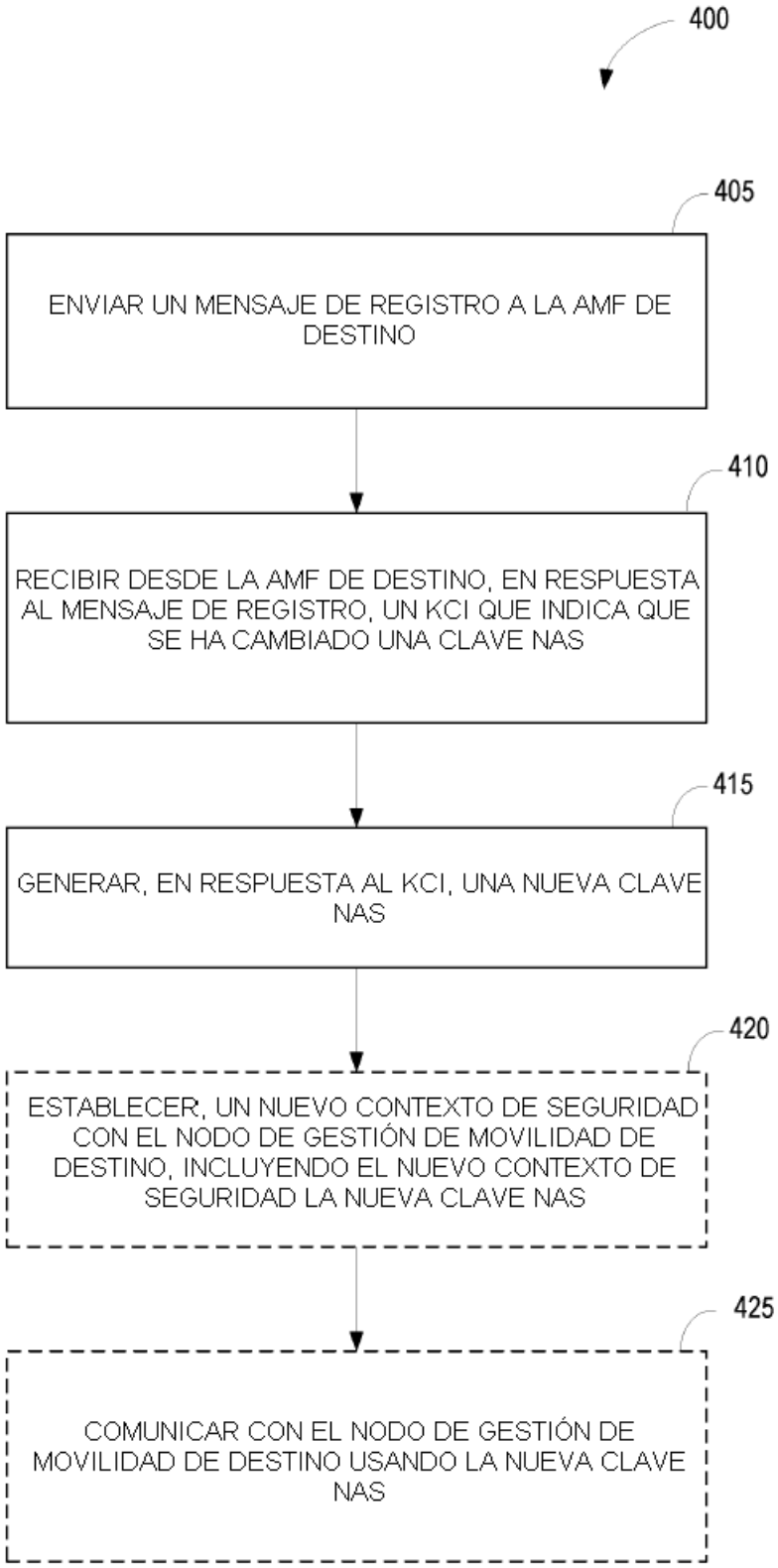
400
405
ENVIAR UN MENSAJE DE REGISTRO A LA AMF DE DESTINO
410
RECIBIR DESDE LA AMF DE DESTINO, EN RESPUESTA AL MENSAJE DE REGISTRO, UN KCI QUE INDICA QUE SE HA CAMBIADO UNA CLAVE NAS
415
GENERAR, EN RESPUESTA AL KCI, UNA NUEVA CLAVE NAS
420
ESTABLECER, UN NUEVO CONTEXTO DE SEGURIDAD CON EL NODO DE GESTIÓN DE MOVILIDAD DE DESTINO, INCLUYENDO EL NUEVO CONTEXTO DE SEGURIDAD LA NUEVA CLAVE NAS
425
COMUNICAR CON EL NODO DE GESTIÓN DE MOVILIDAD DE DESTINO USANDO LA NUEVA CLAVE NAS

Figura 21

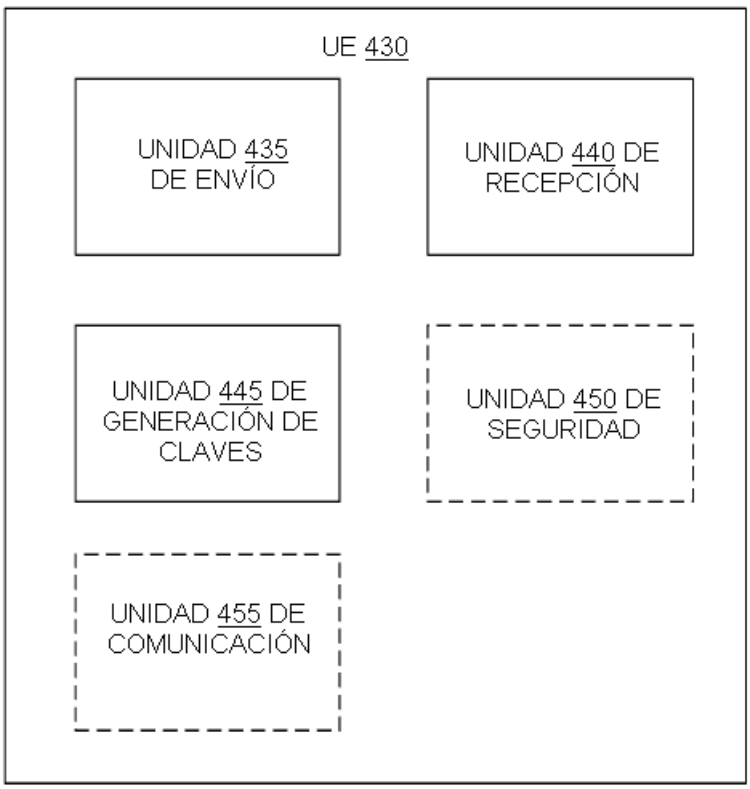
UE 430
UNIDAD 435 DE ENVÍO
UNIDAD 440 DE RECEPCIÓN
UNIDAD 445 DE GENERACIÓN DE CLAVES
UNIDAD 450 DE SEGURIDAD
UNIDAD 455 DE COMUNICACIÓN

Figura 22

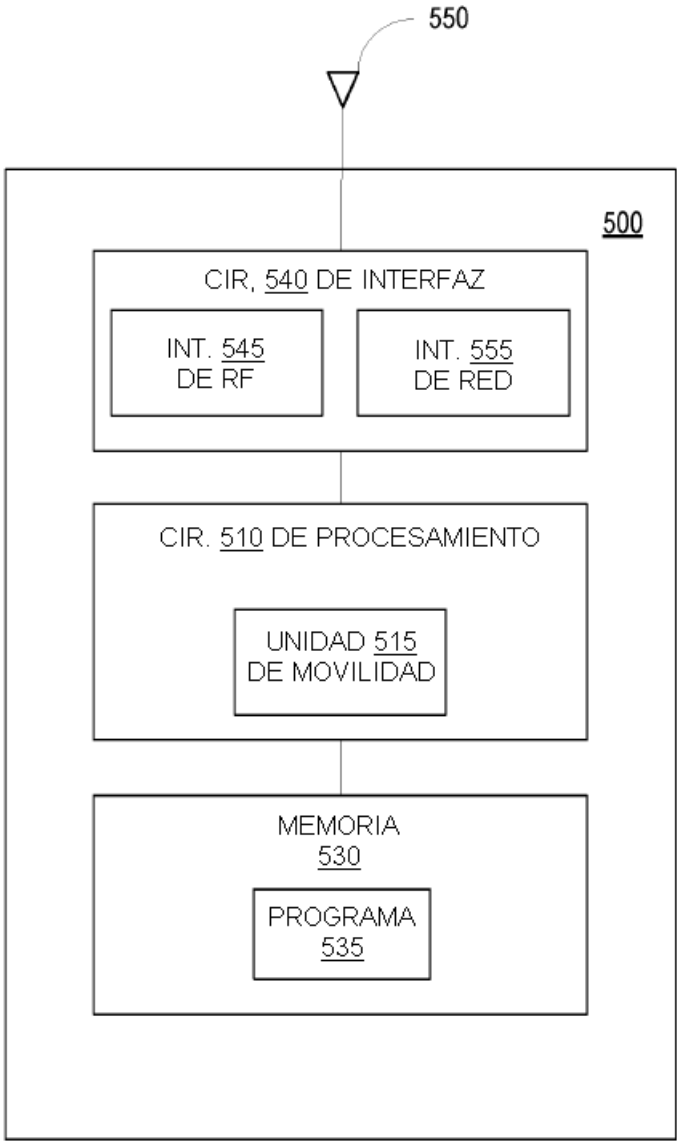
550
500
CIR, 540 DE INTERFAZ
INT. 545 DE RF
INT. 555 DE RED
CIR. 510 DE PROCESAMIENTO
UNIDAD 515 DE MOVILIDAD
MEMORIA 530
PROGRAMA 535

Figura 23

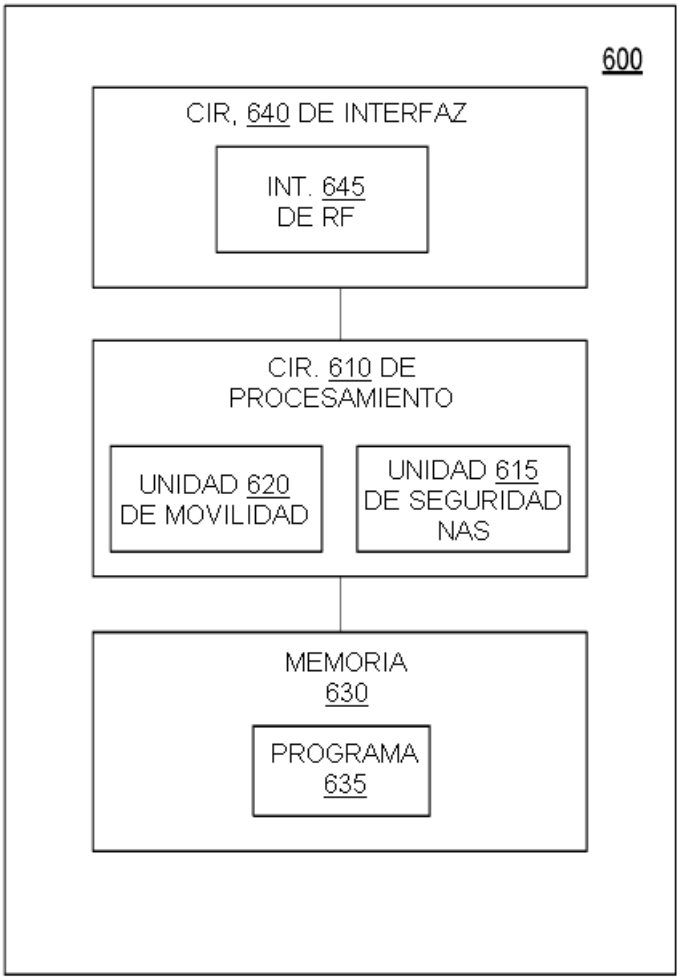
600
CIR, 640 DE INTERFAZ
INT. 645 DE RF
CIR. 610 DE PROCESAMIENTO
UNIDAD 620 DE MOVILIDAD
UNIDAD 615 DE SEGURIDAD NAS
MEMORIA 630
PROGRAMA 635

Figura 24

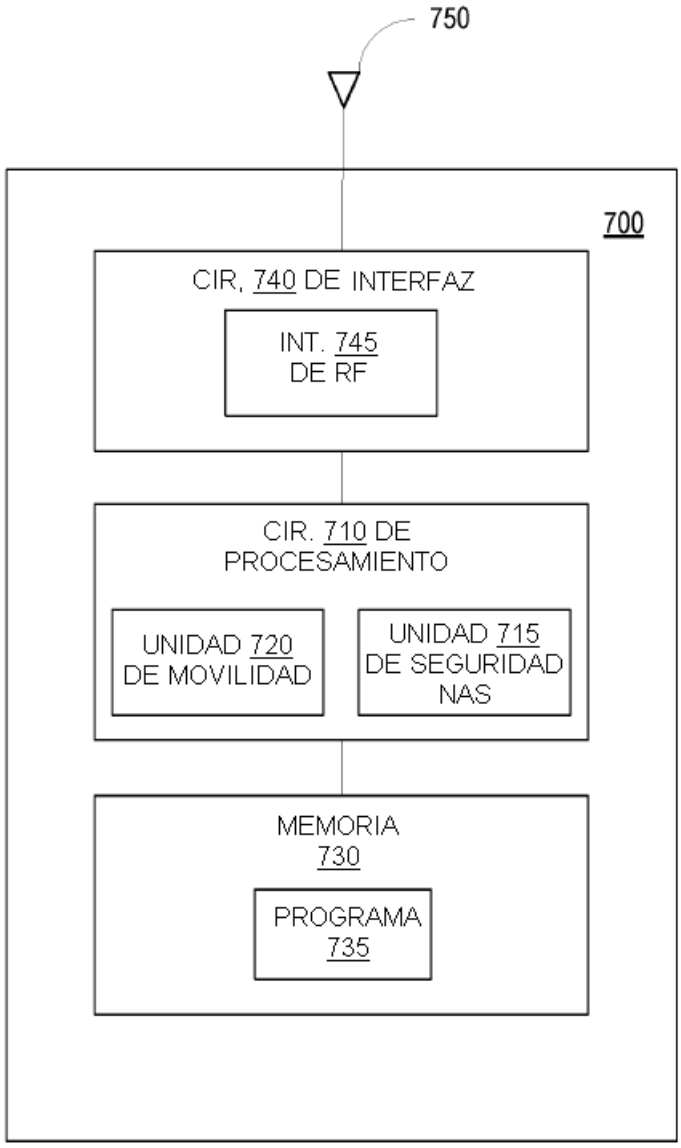
750
700
CIR, 740 DE INTERFAZ
INT. 745
DE RF
CIR. 710 DE
PROCESAMIENTO
UNIDAD 720
DE MOVILIDAD
UNIDAD 715
DE SEGURIDAD
NAS
MEMORIA
730
PROGRAMA
735

Figura 25