(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 388 427**

(51) Int. CI.:
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02728296 .1**
(96) Fecha de presentación: **07.05.2002**
(97) Número de publicación de la solicitud: **1402752**
(97) Fecha de publicación de la solicitud: **31.03.2004**

(54) Título: **Autenticación de mensajes de terminación en un sistema de telecomunicaciones**

(30) Prioridad:
11.05.2001 US 852915
02.04.2002 US 113944

(45) Fecha de publicación de la mención BOPI:
15.10.2012

(45) Fecha de la publicación del folleto de la patente:
15.10.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm , SE

(72) Inventor/es:
WALLENTIN, Pontus;
ELMDAHL, Per y
NORDSTRAND, Ingrid

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Autenticación de mensajes de terminación en un sistema de telecomunicaciones

CAMPO DE LA INVENCIÓN

La invención pertenece a la protección y a la seguridad de los sistemas de telecomunicaciones, y particularmente a la autenticación de ciertos mensajes que se utilizan para terminar un aspecto de las comunicaciones sobre una interfaz aérea que implica a una estación de telefonía móvil.

TÉCNICA RELACIONADA Y OTRAS CONSIDERACIONES

En un sistema de radio celular típico, las unidades de equipos de usuario (UEs – User Equipment, en inglés) se comunican por medio de una red de acceso por radio (RAN – Radio Access Network, en inglés) con una o más redes de núcleo. Las unidades de equipo de usuario (UEs – User Equipment, en inglés) pueden ser estaciones de telefonía móvil tales como teléfonos móviles (teléfonos “celulares”) y ordenadores portátiles con terminación de telefonía móvil, y así pueden ser, por ejemplo, dispositivos de telefonía móvil portátiles, de bolsillo, de mano, con ordenador incluido o montados en un coche que comunican voz y/o datos con la red de acceso por radio. Alternativamente, las unidades de equipo de usuario inalámbricas pueden ser dispositivos inalámbricos fijos, por ejemplo dispositivos/terminales de telefonía móvil fijos que forman parte de un bucle local inalámbrico o similar.

La red de acceso por radio (RAN – Radio Access Network, en inglés) cubre un área geográfica que está dividida en áreas de celdas, estando cada celda servida por una estación de base. Una celda es un área geográfica en la que el radio de cobertura es proporcionado por el equipo de la estación de base de radio en una instalación de estación de base. Cada celda está identificada por una identidad única, que es transmitida en la celda. Las estaciones de base se comunican sobre la interfaz aérea (por ejemplo frecuencias de radio) con las unidades de equipo de usuario (UE – User Equipment, en inglés) dentro del alcance de las estaciones de base. En la red de acceso por radio, varias estaciones de base están típicamente conectadas (por ejemplo, mediante líneas terrestres o microondas) a un controlador de red de radio (RNC – Radio Station Controller, en inglés). El controlador de red de radio, llamado también algunas veces controlador de estación de base (BSC – Base Station Controller, en inglés), supervisa y coordina varias actividades de las diferentes estaciones de base conectadas a él. Los controladores de red de radio están típicamente conectados a una o más redes de núcleo. La red de núcleo tiene dos dominios de servicio, con un RNC que tiene una interfaz hacia estos dos dominios.

Un ejemplo de una red de acceso por radio es la Red de Acceso por Radio Terrestre del Sistema de Telecomunicaciones mediante Telefonía Móvil Universal (UTRAN – Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network, en inglés). El UMTS es un sistema de tercera generación que en algunos aspectos se construye basándose en la tecnología de acceso por radio conocida como Sistema Global para comunicaciones Móviles (GSM - Global System for Mobile Communications, en inglés) desarrollada en Europa. La UTRAN es esencialmente una red de acceso por radio que proporciona acceso múltiple por división de código de banda ancha (WCDMA – Wideband Code Division Multiple Access, en inglés) a unidades de equipo de usuario (UEs – User Equipment, en inglés). El Proyecto de Colaboración de Tercera Generación (3GPP – Third Generation Partnership Project, en inglés) ha sido desarrollado para evolucionar más las tecnologías de red de acceso por radio basadas en UTRAN y en GSM.

Otros tipos de sistemas de telecomunicaciones que incluyen los siguientes: el sistema de Servicio Telefónico de Telefonía Móvil Avanzado (AMPS - Advanced Mobile Phone Service, en inglés); el sistema de AMPS de Banda Estrecha (NAMPS – Narrowband AMPS, en inglés); el Sistema de Comunicaciones de Acceso Total – TACS – Total Access Communications System, en inglés); el sistema Celular Digital Personal (PDS – Personal Digital Cellular, en inglés); el sistema Celular Digital de los Estados Unidos (USDC – United States Digital Cellular, en inglés); y el sistema de acceso múltiple por división de código (CDMA – Code Division Multiple Access, en inglés) descritos en el documento EIA/TIA IS-95.

Existen ciertos procedimientos en los sistemas de telecomunicaciones que esencialmente implican la terminación o el cese de algún tipo de interacción con una estación de telefonía móvil tal como una unidad de equipo de usuario. La interacción puede ser, por ejemplo, una conexión de radio entre la unidad de equipo de usuario y la red de acceso por radio (por ejemplo, una conexión de RRC), o el seguimiento de la unidad de equipo de usuario por la red de núcleo. En la situación de terminación de la conexión de radio con la red de acceso por radio, un mensaje tal como un mensaje de liberación puede iniciar la liberación de la conexión. En el caso en el que ya no es necesario que la red de núcleo realice un seguimiento a la unidad de equipo de usuario, puede emplearse un mensaje de separación para iniciar una operación de separación. Así, tanto el mensaje de liberación de conexión como el mensaje de separación son ejemplos de mensajes de terminación o de cese.

Como se explica a continuación, pueden aparecer problemas de seguridad si un participante no autorizado es capaz de iniciar de otro modo instancias no solicitadas y no deseadas de un mensaje de terminación o cese. Como precursor de una comprensión de las circunstancias en las cuales pueden aparecer tales problemas de seguridad,

se proporcionan a continuación comentarios breves y generalizados relativos a varios temas. Estos temas incluyen áreas de encaminamiento, áreas de ubicación, protocolos de señalización empleados entre la red de acceso por radio y la unidad de equipo de usuario (incluyendo modos y estados de modos de modelos de tales protocolos); y, fallo de un nodo de control de la red de acceso por radio. Estos temas culminan con otra información relativa a procedimientos de liberación y separación de conexión.

La topología de una red de acceso por radio puede ser conceptualizada en áreas o unidades mayores que celdas. Tomando la UTRAN como la red de acceso por radio de ejemplo, un Área de Encaminamiento de UTRAN (URA – Utran Routing Area, en inglés) es un área geográfica que comprende una o más celdas. Cada URA es identificada por una sola identidad que es transmitida en todas las celdas que pertenecen a la URA. Una URA puede comprender celdas controladas por más de un RNC. Una URA con más celdas en más de un RNC se superpone entre los RNCs, es decir, es una URA que se superpone.

Como otro ejemplo de UTRAN, un Área de Ubicación (LA – Location Area, en inglés) es un área geográfica que comprende una o más celdas. Cada LA está identificada por una única identidad enviada sobre el canal de transmisión, de la misma manera que la URA. No obstante, un área de ubicación es utilizada por la red de núcleo para realizar un seguimiento a la ubicación del UE (en modo de reposo y en modo conectado), mientras que la URA es utilizada por la red de acceso por radio para realizar un seguimiento a la ubicación del UE en modo conectado. Típicamente, un área de ubicación es geográficamente más grande que una URA. Para cada área de ubicación existen uno de varios RNCs que tienen celdas en esa área de ubicación particular. Se almacena una relación entre el área de ubicación y un RNC en la red de núcleo.

Las redes de acceso por radio típicamente tienen un protocolo de señalización particular empleado entre la red de acceso por radio y la unidad de equipo de usuario para soportar la gestión de recursos de radio. Por ejemplo, la UTRAN tiene un protocolo de señalización de capa 3 de Control de Recurso de Radio (RRC – Radio Resource Control, en inglés). Una unidad de equipo de usuario en el protocolo de RRC opera en un modelo de estado conceptualizado como con dos modos: un Modo de Reposo y un Modo Conectado. El Modo de Reposo es introducido tras el encendido. En Modo de Reposo no hay conexión entre la unidad de equipo de usuario (UE – User Equipment, en inglés) y la UTRAN. Cuando se establece una conexión de RRC, a la unidad de equipo de usuario (UE – User Equipment, en inglés) se le asigna una U-RNTI y la unidad de equipo de usuario (UE – User Equipment, en inglés) introduce el Modo Conectado. La U-RNTI (Identidad Temporal de Red de Radio de UTRAN – UTRAN Radio Network Temporary Identity, en inglés) es una identidad global, que puede ser utilizada en cualquier celda de la UTRAN. En Modo Conectado, el RNC a cargo de la conexión de RRC para este UE se denomina como RNC de Servicio (SRNC – Serving RNC, en inglés). La U-RNTI consiste en dos partes: la identidad de SRNC (que dentro de la UTRAN identifica al SRNC para este UE) y la RNTI de Servicio (S-RNTI – Serving RNTI, en inglés) que identifica la conexión de RRC dentro del SRNC particular.

Como se ilustra en la Fig. 11, dentro del Modo Conectado hay cuatro estados diferentes: estado de CELL_DCH, estado de CELL_FACH, estado de CELL_PDH y estado de URA_PCH. Como se resume brevemente a continuación, cada estado refleja un nivel de actividad diferente.

El estado de CELL_DCH se caracteriza, por ejemplo, por tener un canal dedicado (DCH – Dedicated Channel, en inglés) asignado a la unidad de equipo de usuario (UE – User Equipment, en inglés). La macro-diversidad puede ser utilizada entre DCHs de varias celdas. En el estado de CELL_DCH, hay un canal de control dedicado (DCCH – Dedicated Control Channel, en inglés) utilizado para la transmisión de mensajes de señalización entre la unidad de equipo de usuario (UE – User Equipment, en inglés) y la UTRAN.

En el estado de CELL_FACH, no se asigna ningún canal dedicado, sino que la unidad de equipo de usuario (UE – User Equipment, en inglés) escucha de manera continua un canal común (el FACH) en el enlace descendente que pertenece a la celda seleccionada. En el enlace ascendente, la unidad de equipo de usuario (UE – User Equipment, en inglés) típicamente utiliza un canal de acceso aleatorio (RACH – Random Access Channel, en inglés). En cada reselección de celda, la unidad de equipo de usuario (UE – User Equipment, en inglés) actualiza la red con su ubicación de celda actual. En este estado, hay un canal de control dedicado (DCCH – Dedicated Control Channel, en inglés) utilizado para la transmisión de mensajes de señalización entre la unidad de equipo de usuario (UE – User Equipment, en inglés) y la UTRAN. El DCCH es implementado añadiendo la Identidad Temporal de Red de Radio (U-RNTI o C-RNTI) a todos los mensajes de señalización, y dirigiendo así a un UE individual. Como se ha mencionado previamente, la U-RNTI (UTRAN RNTI – RNTI de UTRAN) es una identidad global, que puede ser utilizada en cualquier celda de la UTRAN. La C-RNTI (CEL RNTI - RNTI de Celda) es sólo significativa en una única celda, y tiene que ser reasignada en cada celda. Por otro lado, la C-RNTI es mucho más corta que la U-RNTI que ahorra espacio sobre la interfaz de radio cuando se utiliza. Existe también un CCCH (Canal de Control Común – Common Control CHannel, en inglés) en este estado, que se utiliza cuando la conexión al SRNC no está disponible, tal como tras la reselección de la celda sobre las fronteras del RNC, cuando el mensaje de ACTUALIZACIÓN DE CELDA o de ACTUALIZACIÓN DE URA es enviado al DRNC.

En el estado de CELL_PCH, la unidad de equipo de usuario (UE – User Equipment, en inglés) monitoriza un canal de localización (PCH – Paging Channel, en inglés) de una celda seleccionada. En el PCH, la unidad de equipo de

usuario (UE – User Equipment, en inglés) utiliza la recepción discontinua (DRX – Discontinuous Reception, en inglés) para ahorrar energía, y el esquema para cuándo escuchar es acordado entre la red y la unidad de equipo de usuario (UE – User Equipment, en inglés) basándose en la unidad de equipo de usuario (UE – User Equipment, en inglés). También en el estado de CELL_PCH la unidad de equipo de usuario (UE) actualiza la red con su ubicación de celda actual en la reselección de celda. No hay ninguna DCCH disponible en el estado de CELL-PCH. En el PCH, existen medios para dirigirse a unidades de equipo de usuario (UEs) individuales (utilizando la U-RNTI), pero la unidad de equipo de usuario (UE) no puede transportar ningún mensaje de señalización a la red.

El estado de URA_PCH es casi idéntico al estado de CELL_PCH. La diferencia es que la unidad de equipo de usuario (UE – User Equipment, en inglés) no sólo actualiza la red de su ubicación tras cruzar las fronteras de la URA. Como se ha mencionado anteriormente, la URA (Área de Registro de UTRAN - UTRAN Registration Area, en inglés)) es un grupo de celdas. Esto significa que en este estado la posición de la unidad de equipo de usuario (UE – User Equipment, en inglés) es en general conocida sólo a nivel de la URA.

Desgraciadamente, un nodo de control de una red de acceso por radio, tal como un controlador de red de radio (RNC – Radio Network Controller, en inglés) de la UTRAN puede experimentar un fallo que afecta seriamente al nodo de control, en todo o en parte. Cuando tal fallo ocurre, cierta información acerca del contexto de la unidad de equipo de usuario, conocida como el “contexto del UE” en la UTRAN, puede perderse, particularmente durante la reinicialización del nodo de control.

La información incluida en el contexto del UE comprende, entre otros, los siguientes parámetros: IMSI (la identidad de abonado de telefonía móvil internacional); C-ID; D-RNTI; e Identidad del RNC del DRNC en el cual está actualmente situada la unidad de equipo de usuario (UE – User Equipment, en inglés). La identidad de abonado de telefonía móvil internacional (IMSI – International Mobile Subscriber Identity, en inglés) [que comprende no más de quince dígitos] comprende tres componentes: un código de país para telefonía móvil (MCC – Mobile Country Code, en inglés) [tres dígitos]; un código de red para telefonía móvil (MNC – Mobile Network Code, en inglés) [dos o tres dígitos]; y un número de identificación de abonado móvil (MSIN – Mobile Subscriber Identification Number, en inglés). El parámetro D-RNTI es similar al parámetro S-RNTI, pero identifica la información del contexto de UE en el DRNC. El parámetro C-ID es la Identidad de Cella de donde el UE está actualmente situado. El parámetro C-ID no es aplicable a los UEs en el estado de URA_PCH, puesto que la ubicación de una unidad de equipo de usuario (UE – User Equipment, en inglés) en el estado de URA_PCH no es conocida a nivel de celda, sino por el contrario es conocida a nivel de URA (un grupo de celdas definido como una URA). Por lo que respecta al parámetro Identidad de RNC, se observa que en el estado de CELL_DCH podría haber muchos enlaces de radio (RLs – Radio Links, en inglés) simultáneos, así que podría concebirse que existan los mismos RNCs (al menos teóricamente) manejando líneas de conexiones al UE.

En caso de fallo, cuando se pierde la conexión de radio, la unidad de equipo de usuario (UE – User Equipment, en inglés) y la UTRAN entran en el Modo de Reposo cuando se detecta un fallo. La detección de un fallo es lo más rápido en el estado de CELL_DCH, dado que el canal físico se pierde en ese caso. Las unidades de equipo de usuario en el estado de CELL_DCH pueden esperar una pérdida de sincronización y, cuando se produce la recuperación, ir al estado de CELL_FACH después de haber seleccionado una celda adecuada. Durante la recuperación, intentan alcanzar la UTRAN en un canal de acceso aleatorio (tal como el RACH). Si eso falla, entran en el Modo de Reposo. Cuando hay una pérdida de una conexión de radio con la red de acceso por radio (por ejemplo, una pérdida de la conexión de RRC), las unidades de equipo de usuario en estados comparables con los CELL_FACH, CELL_PCH y URA_PCH no necesariamente se darán cuenta de la pérdida. Además, en los estados de CELL_FACH, CELL_PCH y URA_PCH, en las circunstancias en las cuales puede detectarse un fallo, tal detección de fallo es mucho más lenta puesto que se basa en una unidad de supervisión periódica cada cierto número de minutos establecido, donde la unidad de equipo de usuario (UE – User Equipment, en inglés) hace una CELL_UPDATE (Actualización de celda) periódica o una URA UPDATE (Actualización de URA) dependiendo del estado.

Si un RNC que pierde el contexto de UE (para un UE para el cual fue el SRNC) recibe una solicitud de localización originada en la red de núcleo, el RNC asume que la unidad de equipo de usuario está en modo de reposo. Por lo tanto, el RNC localizará a la unidad de equipo de usuario con la identidad del UE en la red de núcleo. No obstante, si la unidad de equipo de usuario está aún en el modo conectado, la unidad de equipo de usuario sólo detectará la localización utilizando la identidad en el modo conectado, que es la U-RNTI.

Como se muestra ahora brevemente y se explica de manera general, la identidad del UE en la red de núcleo (tal como la TMSI) no puede ser utilizada para la localización del UE en el modo conectado. En el modo de reposo la unidad de equipo de usuario lee la identidad del área de ubicación en el canal de transmisión y hace un registro hacia la red de núcleo cuando cambia de área de ubicación. Mediante el registro, la unidad de equipo de usuario recibe una nueva identidad de UE en la red de núcleo (TMSI), puesto que la TMSI sólo es válida dentro de un área de ubicación. En el modo conectado el RNC de servicio controla el área de ubicación en la cual está registrado hacia la red de núcleo. La red de núcleo conoce en qué área de ubicación está registrada la unidad de equipo de usuario, y enviará mediante la localización la solicitud de localización a cada RNC que tiene celdas en esa área de ubicación. La identidad de área de ubicación, en el modo conectado, es enviada siempre directamente a cada unidad de equipo

de usuario desde el SRNC en un canal de control dedicado. La unidad de equipo de usuario en el modo conectado ignora la identidad del área de ubicación en el canal de transmisión. De este modo, la unidad de equipo de usuario en el modo conectado puede establecerse en una celda, en cuyo canal de transmisión se envía una identidad de área de ubicación diferente de la ubicación en la cual es válida la TMSI.

Para asegurar que las unidades de equipo de usuario (para las cuales se han perdido los contextos en el RNC) son alcanzables por la localización originada en la red de núcleo tras la reinicialización del RNC, es importante poner tales unidades de equipo de usuario en el modo de reposo. Puesto que puede haber muchos contextos de UE perdidos en un peor escenario, puede ser necesaria una “liberación de masa” de unidades de equipo de usuario. Para “liberar” una conexión de radio tal como una conexión de RRC entre la red de acceso por radio (como UTRAN) y el terminal de telefonía móvil (como unidad de equipo de usuario), el terminal de telefonía móvil debe abandonar el modo conectado y entrar en el modo de reposo. Existen varios métodos conocidos para liberar tales conexiones de radio.

En un caso normal de liberación de una conexión de radio, ilustrado en el contexto del RRC de UTRAN, la red envía un mensaje de LIBERAR CONEXIÓN DE RRC a la unidad de equipo de usuario en el canal de control dedicado (Dedicated Control Channel, en inglés). La unidad de equipo de usuario reconoce la recepción del mensaje de liberación transmitiendo un LIBERACIÓN DE CONEXIÓN DE RRC COMPLETA, y entrando a continuación en el modo de reposo, de manera que el participante iniciador puede entrar también en el modo de reposo. Tras la liberación, la U-RNTI que fue asignada por la conexión puede ser reutilizada por otra conexión.

Se ha introducido una posibilidad en el WCDMA para transmitir el mensaje de LIBERACIÓN DE CONEXIÓN DE RRC en un canal de control común (CCCH – Common Control CHannel, en inglés). El propósito de esta solución es permitir que el DRNC libere la conexión hacia una unidad de equipo de usuario (UE – User Equipment, en inglés) dada si el SRNC no puede transmitir el mensaje (el DCCH se origina en el SRNC).

En una practica convencional, sólo una unidad de equipo de usuario (UE – User Equipment, en inglés) cada vez puede ser liberada utilizando el mensaje de LIBERACIÓN DE CONEXIÓN DE RRC enviado desde la UTRAN hacia la unidad de equipo de usuario (UE – User Equipment, en inglés). La liberación de la conexión de radio en una unidad de equipo de usuario basándose en una unidad de equipo de usuario es generalmente satisfactoria en la mayoría de las situaciones. No obstante, en una situación de fallo cuando todas las conexiones que pertenecen a un RNC (SRNC o DRNC) tienen que ser liberadas (como cuando se recibe el reinicio del RNC o una reinicialización desde la red de núcleo), esta práctica convencional conlleva una enorme cantidad de mensajes de señalización. Tal señalización masiva provoca una significativa carga en el nodo o los nodos de control de red de radio (RNC – Radio Network Control, en inglés), así como en la interfaz de radio. Puesto que los recursos son limitados, los mensajes de LIBERACIÓN DE CONEXIÓN DE RRC no pueden ser enviados instantáneamente a todos los UEs por ello la transmisión llevará algún tiempo. Este retardo típicamente provoca inconvenientes para el usuario. Además, el retardo aumenta el riesgo de que una U-RNTI, ya en uso por una primera unidad de equipo de usuario (UE – User Equipment, en inglés), sea prematuramente asignada a una nueva conexión. Además, en caso de reinicio de un nodo de control de red de radio (RNC – Radio Network Control, en inglés), el RNC puede olvidar qué U-RNTIs estaban asignadas a las unidades de equipo de usuario (UEs – User Equipment, en inglés) antes del reinicio.

A la vista de lo anterior, la liberación de varias conexiones de radio utilizando un solo mensaje (conocido como el “mensaje de liberación ómnibus”) ha sido propuesta en el documento US 2002 168984 A1, publicado el 14 Noviembre de 2002, y titulado “RELEASING PLURAL RADIO CONNECTIONS WITH OMNIBUS RELEASE MESSAGE”. El mensaje de liberación ómnibus hace posible ahorrar señalización y reducir el retardo dirigiéndose a múltiples UEs en el mismo mensaje de liberación en el CCCH o el PCCH.

Típicamente existe algún tipo de protocolo empleado por el UE y el dominio de la red de núcleo para soportar la movilidad, identificación y seguridad de los UEs, por ejemplo, un protocolo de Gestión de Movilidad (MM – Mobility Management, en inglés) se utiliza entre el UE y el dominio de la red de núcleo para soportar la movilidad, identificación y seguridad de los UEs. Un modelo de estado del UE de protocolo de MM se ilustra en la Fig. 12 con tres estados: un estado conectado de MM, un estado de reposo de MM y un estado separado de MM.

En el modo conectado mediante MM el móvil se comunica con el dominio de la red de núcleo sobre una conexión de señalización. La conexión de señalización requiere que se establezca una conexión de radio (por ejemplo, una conexión de RRC) entre el UE y la red de acceso por radio (esto es, el protocolo de RRC está en uno de los estados en el modo conectado). La ubicación del móvil es en este estado rastreada mediante las funciones de control de recurso de radio, utilizando por ejemplo transferencia, normalmente a nivel de celda utilizando el protocolo de RRC.

En el estado de reposo de MM, no hay ninguna comunicación en curso entre el dominio de la red de núcleo y el móvil específico. Puesto que puede haber dos protocolos de MM paralelos (uno para cada dominio de red de núcleo), la capa de RRC puede estar bien en modo de reposo o en modo conectado. La ubicación del móvil es rastreada en el nivel del área de registro y almacenada en el dominio de la red de núcleo. El móvil escucha la localización. Desde el dominio de la red de núcleo, el UE es alcanzable mediante localización en el área de registro.

En el estado separado de MM, la ubicación del móvil no es conocida por el dominio de la red de núcleo. El móvil está “desconectado”.

La operación de liberación es sólo una del tipo de operación en el cual algún tipo de interacción que implica a una estación de telefonía móvil (unidad de equipo de usuario) es terminada o cesada. En la operación de liberación una conexión del protocolo de señalización es el tipo de interacción que es terminada o cesada. Otro tipo de cese o de terminación de interacción es una operación de separación, que puede ocurrir (por ejemplo) cuando la estación de telefonía móvil se queda sin alimentación.

A la vista de lo anterior, se utiliza un procedimiento de separación para llevar a la unidad de equipo de usuario al estado separado de MM (véase la Fig. 12). El procedimiento de separación es típicamente ejecutado cuando el usuario pulsa el botón de “apagado” en la unidad de equipo de usuario con el fin de desconectar la alimentación. En esta situación, el mensaje de separación es enviado desde la unidad de equipo de usuario al dominio de la red de núcleo durante el apagado de la unidad de equipo de usuario. El dominio de la red de núcleo puede entonces marcar a esta unidad de equipo de usuario como separada. Esto hace posible evitar una innecesaria localización hacia las unidades de equipo de usuario apagadas en una solicitud de llamada de terminación mediante telefonía móvil.

Para ejecutar el procedimiento de separación, debe establecerse una conexión de señalización. Si no existe ninguna conexión de señalización (por ejemplo, si la unidad de equipo de usuario está en modo de reposo de MM) cuando el usuario pulsa el botón de “apagado”, la conexión de señalización necesita ser establecida primero. Y si no hay ninguna conexión de señalización para ningún otro dominio de red de núcleo implicada actualmente, la conexión de radio necesitará también ser establecida.

Aspectos básicos de un procedimiento de separación convencional se ilustran en la Fig. 13, en la que se asume que la conexión de señalización ya está establecida (la capa de MM para este dominio de red de núcleo está en estado conectado con MM) Como etapa 15-1, la unidad de equipo de usuario (UE) envía un mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI en la conexión de señalización a la red de núcleo. El mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI pasa de manera transparente a través de la red de acceso por radio hasta el nodo de red de núcleo (por ejemplo, hasta el nodo de MSC en este ejemplo). El mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI incluye una identidad de la unidad de equipo de usuario (tal como la TMSI o posiblemente la IMSI). Cuando el nodo de red de núcleo recibe el mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI, la red de núcleo inicia una liberación de la conexión de señalización, enviando (como etapa 15-2) un mensaje de LIBERACIÓN DE IU al RNC. La red de acceso por radio (el nodo RNC) responde a la red de núcleo (avisando de que la liberación de la conexión de señalización será llevada a cabo) devolviendo (como etapa 15-3) un mensaje de LIBERACIÓN DE IU COMPLETA al nodo de red de núcleo. La red de núcleo puede ahora marcar la unidad de equipo de usuario como en estado separado con MM. Si en este momento se recibe cualquier llamada de terminación, la red de núcleo no necesita localizar a la unidad de equipo de usuario puesto que la red de núcleo asumirá que la unidad de equipo de usuario no es alcanzable, y simplemente contestará con un mensaje de señal o de voz alertando al participante llamante de que al participante llamado no es alcanzable por el momento.

Si la capa de MM paralela para cualquier dominio de la red de núcleo no tiene una conexión de señalización, como etapa X-4 la red de acceso por radio iniciará el procedimiento de liberación de conexión de RRC a la unidad de equipo de usuario. El procedimiento de liberación de conexión de RRC liberará en este caso tanto la conexión de señalización como la conexión de radio (por ejemplo, la conexión de RRC). Si hay otra conexión de señalización establecida para el otro dominio de CN, la red de acceso por radio mantendrá la conexión de RRC, y sólo liberará la conexión de señalización enviando un mensaje de LIBERACIÓN DE CONEXIÓN DE SEÑALIZACIÓN.

Después de transmitir el mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI, la unidad de equipo de usuario inicializa un temporizador para supervisar la liberación de la conexión de señalización. Si la conexión de señalización no es liberada por la red antes de la expiración de este temporizador, por ejemplo si alguno de los mensajes no tiene éxito (por ejemplo el mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI o de LIBERACIÓN DE CONEXIÓN DE RRC), el UE liberará la conexión de señalización localmente y entrará en estado separado con MM.

En el lado de la red, la liberación de la estación de base de señalización es también supervisada. Si la unidad de equipo de usuario no responde (en el caso anterior con la última conexión de señalización, la red de acceso por radio borrará toda la información acerca de la unidad de equipo de usuario y asumirá que el canal de radio se ha perdido.

Puesto que la unidad de equipo de usuario está a punto de desconectarse cuando se ejecuta el procedimiento de separación, el procedimiento de separación debe ser rápido. Para acelerar el procedimiento de separación, no se requiere iniciar funciones de seguridad como la encriptación para estos mensajes. Si el encriptado fuese a iniciarse, se necesitarían varios mensajes incluyendo un posible procedimiento de autenticación entre el UE y la red de núcleo.

Un inconveniente del mensaje de señalización ómnibus aludido previamente es que un participante no amigo puede utilizar este mensaje de manera nefasta pero eficiente para liberar unidades de equipo de usuario. Puesto que el mensaje tiene que ser enviado desencriptado y que incluye información disponible públicamente, este mensaje puede, si está disponible para un intruso, ser una seria amenaza para la seguridad.

Un problema de seguridad similar aparece con respecto al procedimiento de separación con su mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI, que convencionalmente no está protegido por ninguna función de seguridad, como autenticación y/o cifrado y/o integridad. Esto significa, por ejemplo, que un intruso puede enviar el mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI en representación de otra unidad de equipo de usuario incluyendo la identidad del UE en el mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI. Puesto que la red de núcleo, como parte del manejo de los casos fallidos de este procedimiento, marcará la unidad de equipo de usuario como separada incluso si la unidad de equipo de usuario no respondiese a la solicitud de liberar la conexión de señalización, marcará al UE como separado, esta unidad de equipo de usuario no podrá recibir ninguna llamada. Esto sucederá incluso si la unidad de equipo de usuario en realidad no se separase. Así, podría ser posible separar un grupo de unidades de equipo de usuario separándolas una por una, cíclicamente a través de todo el intervalo de valores de las identidades de unidad de equipo de usuario (por ejemplo, utilizando una unidad de equipo de usuario falsa). Además, los documentos US-B1 6173173, WO 01/80591 y US 4.984.290 se refieren a problemas similares.

Lo que se necesita, por lo tanto, como se describe en esta memoria, es un sistema de autenticación que evite la terminación de interacción no autorizada con un nodo de telefonía móvil tal como una unidad de equipo de usuario.

BREVE COMPENDIO

La presente invención se refiere a un método en un primer nodo de acuerdo con la reivindicación 1, a un método en un segundo nodo de acuerdo con la reivindicación 12, a un primer nodo de acuerdo con la reivindicación 13, a un segundo nodo de acuerdo con la reivindicación 25 y a una red de comunicación de acuerdo con la reivindicación 26.

Un mecanismo de autenticación blinda a una red de comunicaciones frente a solicitudes no autorizadas de terminación o cese de interacción con un nodo de telefonía móvil. En un modo de operación de autenticación de liberación, el mecanismo de autenticación protege frente a un mensaje de liberación de conexión no autorizado dirigido a un nodo de telefonía móvil de la red, por ejemplo, una estación de telefonía móvil tal como una unidad de equipo de usuario, frustrando por ello un intento de solicitud de un procedimiento de liberación de conexión no autorizado para el nodo de telefonía móvil.

En sus modos de operación, el mecanismo de autenticación implica a un primer nodo de la red de comunicaciones en el cual se proporciona una clave de autenticación. La clave de autenticación puede ser generada (por ejemplo seleccionada) por el primer nodo o asignada al primer nodo. El primer nodo de la red utiliza la clave de autenticación para obtener unos indicios de autenticación relativos a la clave de autenticación. El primer nodo proporciona los indicios de autenticación a un segundo nodo de la red. Subsiguientemente, cuando una operación de terminación de interacción de de telefonía móvil va a ocurrir (por ejemplo, liberación o separación de la conexión), el primer nodo incluye la clave de autenticación en un mensaje de terminación transmitido sobre una interfaz aérea entre el primer nodo y el segundo nodo. Como condición para llevar a cabo una operación que termina la interacción con el nodo de telefonía móvil, el segundo nodo confirma que la clave de autenticación (que fue incluida en el mensaje de terminación de interacción) está, en realidad, relacionada con los indicios de autenticación.

En el modo de operación de autenticación de procedimiento, en una implementación de ejemplo el primer nodo (que proporciona los indicios De autenticación al segundo nodo de la red) es un nodo de red de acceso por radio (por ejemplo, un controlador de red de radio) y el segundo nodo es un nodo de telefonía móvil (por ejemplo, una unidad de equipo de usuario). El nodo de red de acceso por radio proporciona los indicios de autenticación al nodo de telefonía móvil en un primer mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés) (por ejemplo un mensaje de establecimiento de conexión de control de recurso de radio (RRC – Radio Resource Control, en inglés), y el nodo de red de acceso por radio incluye la clave de autenticación en un segundo mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés) (por ejemplo un mensaje de procedimiento de conexión de control de recurso de radio (RRC - Radio Resource Control, en inglés). El nodo de telefonía móvil confirma que la clave de autenticación incluida en el segundo mensaje de control de recurso de radio (RRC - Radio Resource Control, en inglés) se refiere a los indicios de autenticación como condición para llevar a cabo la operación de procedimiento de conexión.

En el modo de operación de autenticación de separación, en una implementación de ejemplo el primer nodo (que proporciona los indicios de autenticación al segundo nodo de la red) es un nodo de telefonía móvil (por ejemplo, una unidad de equipo de usuario) y el segundo nodo es un nodo de red de núcleo (por ejemplo, un MSC). El nodo de telefonía móvil puede proporcionar los indicios de autenticación a la red de núcleo mediante la ocurrencia de un evento predeterminado (por ejemplo, el registro de un nodo de telefonía móvil con la red de núcleo). A continuación, cuando se inicia una operación de separación, el nodo de telefonía móvil incluye la clave de autenticación, por ejemplo, en un mensaje de separación (por ejemplo, un mensaje de indicación de separación de IMSI). Como condición para llevar a cabo su parte de la operación de separación, el nodo de red de núcleo confirma primero que

la clave de autenticación comunicada al nodo de red de núcleo en el mensaje de separación se refiere a los indicios de autenticación recibidos previamente. En una implementación, el nodo de telefonía móvil utiliza el IMSI o el TMSI del nodo de telefonía móvil para generar los indicios de autenticación que son proporcionados a la red de núcleo, y asimismo el nodo de red de núcleo utiliza el IMSI o el TMSI del nodo de telefonía móvil para confirmar que la clave de autenticación se refiere a los indicios de autenticación.

Como escenario de implementación de modos de autenticación, los indicios de autenticación se refieren a la clave de autenticación siendo iguales a la clave de autenticación. En otro escenario más seguro, los indicios de autenticación son referidos a la clave de autenticación mediante una función. Una función de ejemplo para el escenario más seguro son los indicios de autenticación son un código de autenticación que se refiere a la clave de autenticación mediante una función de Kasumi. Para su uso en esta memoria, tal función de Kasumi puede ser expresada como C=Kasumi(M)CLAVE DE VALIDACIÓN, donde: M es un parámetro derivado de una identidad de un nodo de telefonía móvil; CLAVE DE VALIDACIÓN es un parámetro derivado de una clave de autenticación; y C son los indicios de autenticación (por ejemplo, el código de autenticación). Pueden emplearse varias técnicas para obtener el parámetro M y el parámetro CLAVE DE VALIDACIÓN. Por ejemplo, M puede obtenerse a partir de varias (por ejemplo, dos) instancias concatenadas del U-RNTI del nodo de telefonía móvil; el parámetro CLAVE DE VALIDACIÓN puede ser obtenido a partir de varias (por ejemplo, dos) instancias concatenadas de la clave de autenticación. Como otro ejemplo, M puede por el contrario ser obtenido a partir de una o de varias instancias concatenadas de la representación binaria de la identidad del UE de la red de núcleo (CN – Core Network, en inglés), por ejemplo, la IMSI del nodo de telefonía móvil. La representación binaria de la IMSI puede ser construida concatenando la re prestación binaria de cada uno de los 15 dígitos (donde cada dígito está representado por cuatro bits) y rellenando con ceros binarios hasta que el resultado resulta ser 64 bits. En otro ejemplo más, M se obtiene a partir de varias (por ejemplo, dos) instancias concatenadas de la TMSI o de la P-TMSI (cada una de ellas es 32 bits) del nodo de telefonía móvil. La identidad de UE de la CN puede ser particularmente apropiada en un modo de separación en el cual la U-RNTI no está disponible en la red de núcleo.

Mediante la recepción de la clave de autenticación incluida en el mensaje de terminación (por ejemplo, el mensaje de procedimiento de conexión o el mensaje de separación), el segundo nodo lleva a cabo varias acciones. En este sentido, el segundo nodo determina unos indicios de autenticación calculados utilizando la clave de autenticación incluida en el mensaje de terminación. El segundo nodo confirma a continuación que los indicios de autenticación calculados representan los indicios de autenticación proporcionados previamente al segundo nodo por el primer nodo.

Además de pertenecer a los métodos de autenticación brevemente resumidos anteriormente así como a redes de comunicaciones que implementan los mismos, la presente invención pertenece también a los nodos implicados en tal implementación, por ejemplo, el primer nodo que almacena una clave de autenticación y que utiliza la clave de autenticación para obtener unos indicios de autenticación relativos a la clave de autenticación, y el segundo nodo que confirma que los indicios de autenticación correctos fueron incluidos en el mensaje de terminación. Como se ha indicado, en el modo de operación de autenticación de liberación el primer nodo puede ser un nodo de red de acceso por radio (por ejemplo, un controlador de red de radio) y un segundo nodo puede ser el nodo de telefonía móvil (por ejemplo, una unidad de equipo de usuario). En el modo de autenticación de separación, el primer nodo es el nodo de telefonía móvil (por ejemplo, una unidad de equipo de usuario) y el segundo nodo puede ser un nodo de red de núcleo.

En una implementación de ejemplo, el primer nodo incluye medios para hacer que se le proporcionen indicios de autenticación al segundo nodo, así como una unidad de autenticación que incluye la clave de autenticación en un mensaje de terminación. El mensaje de terminación es transmitido sobre una interfaz aérea entre el primer nodo y el segundo nodo.

En una implementación de ejemplo, el segundo nodo incluye una unidad de autenticación que confirma que la clave de autenticación incluida en el mensaje de terminación se refiere a los indicios de autenticación como condición para llevar a cabo una operación de terminación. La unidad de autenticación incluye medios para determinar unos indicios de autenticación calculados utilizando una clave de autenticación incluida en un mensaje de terminación, y medios para confirmar que los indicios de autenticación calculados representan los indicios de autenticación almacenados en la memoria como condición para llevar a cabo una operación de terminación. En el modo de autenticación de separación, el segundo nodo (por ejemplo, un nodo de red de núcleo) incluye una memoria que almacena una asociación del nodo de telefonía móvil con unos indicios de autenticación (habiendo sido transmitidos los indicios de autenticación desde el nodo de telefonía móvil sobre una interfaz aérea).

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los anteriores y otros objetos, características y ventajas de la invención resultarán evidentes a partir de la descripción más particular que sigue de realizaciones preferidas tal como se ilustran en los dibujos que se acompañan en los cuales los caracteres de referencia se refieren a las mismas partes en las diferentes vistas. Los dibujos no están necesariamente a escala, haciéndose por el contrario énfasis en ilustrar los principios de la invención.

La Fig. 1A es una vista diagramática de dos nodos de un sistema de comunicaciones y de las acciones básicas implicadas en establecer la interacción entre ellos hasta un punto pertinente para ilustrar la operación de terminación de autenticación de acuerdo con una primera implementación de ejemplo.

La Fig. 1B es una vista diagramática de los dos nodos de un sistema de comunicaciones y de las acciones básicas implicadas en terminar la interacción entre ellos hasta un punto pertinente para ilustrar la operación de autenticación de terminación de acuerdo con la primera implementación de ejemplo.

La Fig. 2A es una vista diagramática de dos nodos de un sistema de comunicaciones y de las acciones básicas implicadas en establecer la interacción entre ellos hasta un punto pertinente para ilustrar la operación de autenticación de terminación de acuerdo con una segunda implementación de ejemplo.

La Fig. 2B es una vista diagramática de los dos nodos de un sistema de comunicaciones y de las acciones básicas implicadas en terminar la interacción entre ellos hasta un punto pertinente para ilustrar la operación de autenticación de terminación de acuerdo con la segunda implementación de ejemplo.

La Fig. 3 es una vista diagramática de un sistema de comunicaciones de telefonía móvil de ejemplo que tiene mecanismos de autenticación de acuerdo con un modo de operación de autenticación de liberación.

La Fig. 4 (2380-336) es una vista diagramática que muestra, con más detalle, porciones de una implementación representativa del sistema de comunicaciones de telefonía móvil de ejemplo de la Fig. 3.

La Fig. 5A y la Fig. 5B ilustran una manera de ejemplo para llevar a cabo el modo de operación de autenticación de liberación que utiliza la implementación de la Fig. 1A y la Fig. 1B.

La Fig. 6A y la Fig. 6B ilustran una manera de ejemplo para llevar a cabo el modo de operación de autenticación de liberación que utiliza la implementación de la Fig. 2A y la Fig. 2B.

La Fig. 7 es una vista diagramática del sistema de comunicaciones de telefonía móvil de ejemplo que tiene mecanismos de autenticación de acuerdo con un modo de operación de autenticación de separación.

La Fig. 8A y la Fig. 8B ilustran una manera de ejemplo para llevar a cabo el modo de operación de autenticación de separación que utiliza la implementación de la Fig. 2A y la Fig. 2B.

La Fig. 9A y la Fig. 9B son vistas diagramáticas de formatos de ejemplo de mensajes de establecimiento de conexión de control de recurso de radio (RRC – Radio Resource Control, en inglés), y muestran campos o elementos en los que pueden incluirse una clave o indicios de liberación de autenticación.

Las Fig. 10A - Fig. 10E son vistas diagramáticas de formatos de ejemplo de mensajes de liberación de conexión de control de recurso de radio (RRC – Radio Resource Control, en inglés), y muestran campos o elementos en los que pueden incluirse una clave o indicios de liberación de autenticación.

La Fig. 11 es una vista diagramática que muestra modos y estados de una unidad de equipo de usuario (UE) pertienentes para la presente invención.

La Fig. 12 es una vista diagramática que muestra estados del protocolo de gestión de movilidad (MM – Mobility Management, en inglés) pertinentes para la presente invención.

La Fig. 13 es una vista diagramática que muestra aspectos básicos de un procedimiento de separación convencional.

DESCRIPCIÓN DETALLADA

En la siguiente descripción, con el propósito de explicación y no de limitación se exponen detalles específicos tales como arquitecturas, interfaces, técnicas, etc. particulares con el fin de proporcionar una completa comprensión de la presente invención. No obstante, resultará evidente para los expertos en la materia que la presente invención puede ser puesta en práctica en otras realizaciones que parten de estos detalles específicos. En otros casos, se omiten descripciones detalladas de dispositivos, circuitos y métodos bien conocidos, para no oscurecer la descripción de la presente invención con un detalle innecesario. Además, bloques funcionales individuales se muestran en algunas de las figuras. Resultará evidente para los expertos en la materia que las funciones pueden ser implementadas de varias maneras.

La Fig. 1A y la Fig. 1B muestran dos nodos N_i y N_r de una red de comunicaciones. Los dos nodos N_i y N_r se comunican sobre una interfaz aérea representada por la línea de trazos de la Fig. 1A y la Fig. 1B. Puede haber nodos intermedios (tales como un nodo de estación de base) situados o funcionalmente intermedios entre los dos nodos N_i y N_r. Uno de los dos nodos N_i y N_r es un nodo de telefonía móvil, por ejemplo un nodo inalámbrico llamado a veces estación de telefonía móvil, terminal de telefonía móvil o unidad de equipo de usuario. En aras de la simplicidad, el nodo de telefonía móvil se denominará a menudo en lo que sigue en esta memoria unidad de equipo

de usuario, aunque debe entenderse que todos los términos anteriores así como otros términos comparables son también apropiados. El otro de los dos nodos N_i y N_r es un nodo fijo implicado en algún tipo de interacción con el nodo de telefonía móvil. Por ejemplo, este nodo fijo podría ser un nodo de una red de acceso por radio (RAN – Radio Access Network, en inglés) o un nodo de una red de núcleo.

De particular importancia para la presente invención es un proceso de terminación que termina un aspecto particular de la interacción en la cual participan el N_i y el N_r. El proceso de terminación implica a un mecanismo de autenticación que hace a la red de comunicaciones, y por ello a los dos nodos N_i y N_r, blindados frente a solicitudes para la terminación o el cese de la interacción no autorizados entre los dos nodos N_i y N_r. Como se explica de manera más completa a continuación, si la interacción entre los dos nodos N_i y N_r es una conexión de radio, en un modo de operación de autenticación de liberación el mecanismo de autenticación protege frente a un mensaje de liberación de conexión no autorizada dirigido a un nodo de la red de telefonía móvil, frustrando por ello un intento de solicitar un procedimiento de terminación de conexión no autorizada relativa a una conexión que implica al nodo de telefonía móvil. De manera similar, en un modo de operación de autenticación de separación también elaborado en lo que sigue en esta memoria, el mecanismo de autenticación protege contra un mensaje de separación no autorizada transmitido de manera engañosa en nombre del nodo de telefonía móvil, frustrando por ello un intento de solicitar un procedimiento de terminación no autorizado para el nodo de telefonía móvil.

El nodo N_i es el nodo de inicio de solicitud de terminación, y se muestra en la Fig. 1A y la Fig. 1B comprendiendo un autenticador de terminación 100_i y una función de detección/notificación de terminación/fallo 101. El Nodo N_r es el nodo de respuesta a solicitud de terminación, que tiene su propia versión de un autenticador de terminación 100_r. El autenticador de terminación 100_i trabaja junto con otras funciones del nodo N_i, que incluyen una función de detección/notificación de terminación/fallo 101, la función de establecimiento de interacción 102 y la función de terminación de interacción 103. De manera similar, el autenticador de terminación 100_r trabaja junto con otras funciones del N_r, que incluyen la función de terminación de interacción 104 y la función de establecimiento de interacción 105. Resultará evidente que los dos nodos N_i y N_r tienen ambos otras numerosas funciones no especificadas descritas en esta memoria, pero comprendidos por otros medios por el experto en la materia de acuerdo con diferentes implementaciones.

En la realización de la Fig. 1A y la Fig. 1B, el autenticador de terminación 100_i incluye un selector de clave 106 y una memoria de almacenamiento de clave 107, mientras que el autenticador de terminación 100_r incluye una memoria de almacenamiento de claves 108 y el validador de clave 110. Estas divisiones funcionales son para proporcionar una ilustración de las operaciones del autenticador de terminación 100_i y el autenticador de terminación 100_r, y no son críticas sino por el contrario, de ejemplo. Resultará evidente que estas funciones pueden ser distribuidas o asignadas de varias maneras, incluyendo utilizar uno o más circuitos de hardware individuales, utilizando software que funciona junto con un microprocesador digital programado de manera adecuada o un ordenador de propósito general, que utiliza un circuito integrado para una aplicación específica (ASIC – Application Specific Integrated Circuit, en inglés), y/o utilizando uno o más procesadores de señal digital (DSPs – Digital Signal Processors, en inglés).

Acciones o etapas básicas mostradas de manera representativa en la Fig. 1A y la Fig. 1B muestran cómo, en una implementación de ejemplo, el autenticador de terminación 100_i y el autenticador de terminación 100_r proporcionan autenticación de manera que el nodo receptor de la solicitud de terminación N_r puede estar seguro de que un mensaje de solicitud de terminación es verdadero, es decir, viene del nodo apropiado (por ejemplo, el nodo N_i). La Fig. 1A muestra las acciones básicas implicadas en establecer la interacción entre el nodo N_i y el Nodo N_r hasta el punto pertinente para ilustrar la operación del autenticador de terminación 100_i y del autenticador de terminación 100_r. La Fig. 1B, por otro lado, muestra acciones básicas implicadas en la terminación de la interacción que son pertinentes para el autenticador de terminación 100i y el autenticador de terminación 100_r.

Como acción 1-0, el nodo N_i selector de clave 106 selecciona o si no obtiene (por ejemplo, se le asigna) una clave de autenticación de terminación. La clave de autenticación de terminación puede ser (por ejemplo) un número aleatorio. Como sección 1-1, la clave de autenticación es almacenada en la memoria de almacenamiento de claves 107. La memoria de almacenamiento de claves 107 es un dispositivo de memoria (por ejemplo, RAM no volátil o disco duro) que sobrevive a una reinicialización del nodo N_i. En un aspecto de implementación, la clave de autenticación está asociada con una pluralidad de nodos de solicitud-respuesta de terminación, no sólo con un nodo N_r. Por ejemplo, en un modo en el cual el nodo N_i es un nodo de control de red de acceso por radio (RAN – Radio Access Network, en inglés) (por ejemplo, RNC), la clave de autenticación está asociada con un grupo de UEs (o, con todos los UEs que tienen este RNC como el RNC Servidor).

Cuando se va a establecer una interacción entre el nodo Ni y el nodo N_r, la función de establecimiento de interacción 102 del nodo N_i obtiene la clave de autenticación de la memoria de almacenamiento de claves 107, como se representa mediante la acción 1-2. La clave de autenticación es proporcionada a una rutina de inclusión de claves 112 de la función de establecimiento de interacción 102, la cual incluye la clave de autenticación en un mensaje de establecimiento de interacción que es enviado como acción 1-3 desde el nodo N_i hasta el nodo N_r. La transmisión del mensaje de establecimiento de interacción, con su clave de autenticación incluida, está preferiblemente en un

canal encriptado. Como acción 1-4, el nodo N_r almacena la clave de autenticación en su memoria de almacenamiento de claves 108 (que es también preferiblemente una memoria no volátil).

La Fig. 1B muestra la función de detección/notificación de terminación/fallo 101 considerablemente enviando a continuación, como acción 1-5, una notificación para la función de terminación de interacción 103, de que la interacción con el nodo N_r (bien el nodo N_r solo o un grupo de nodos a los cuales pertenece el nodo N_r) debe ser terminada. Cuando se recibe tal notificación, como acción 1-6 la función de terminación de interacción 103 obtiene la clave de autenticación de la memoria de almacenamiento de clave 107 (o del selector de clave 106). La clave de autenticación es proporcionada a una rutina de inclusión de clave 114 de la función de terminación de interacción 103, la cual incluye la clave de autenticación en un mensaje de terminación de interacción que es enviado como acción 1-7 sobre la interfaz aérea desde el nodo N_i al nodo N_r.

Tras la recepción del mensaje de terminación enviado como acción 1-7, como acción 1-8 la función de terminación de interacción 104 envía la clave de autenticación que se acaba de recibir al validador de clave 110. Además, como acción 1-9 la función de terminación de interacción 104 solicita que la clave de autenticación almacenada de la memoria de almacenamiento de clave 108 del autenticador 100_r sea enviada como acción 1-10 al validador de clave 110. Como acción 1-11, el validador de clave 110 compara la clave de autenticación recibida en el mensaje de terminación (por ejemplo recibida en el mensaje 1-7) con su clave de autenticación almacenada recibida previamente y almacenada en la memoria de almacenamiento de clave 108. Si hay una coincidencia de las dos claves como acción 1-11, la función de terminación de interacción 104 es así notificada (acción 1-12) de manera que la función de terminación de interacción 104 del nodo N_r considera el mensaje de terminación de la acción 1-7 como autenticado, y sigue con la terminación. Si no hay coincidencia en la acción 1-11, el mensaje de terminación no es autenticado (porque, por ejemplo, posiblemente el mensaje de terminación fue enviado por un intruso llevando a cabo un rechazo del ataque al servicio), y el nodo N_r simplemente ignora el mensaje de terminación.

Un inconveniente de la implementación de la Fig. 1A y la Fig. 1B es que la clave de autenticación es enviada antes de que haya sido realmente utilizada. Un intruso posiblemente podría hacer uso de la clave de autenticación, una vez obtenida, para liberar el nodo N_r de cualquier manera (bien el propio nodo N_r o un grupo de nodos que incluyen al nodo N_r). Por ejemplo, si el nodo N_r es un nodo de telefonía móvil (por ejemplo una unidad de equipo de usuario), un intruso con una suscripción normal puede obtener la clave de liberación de autenticación de un UE puesto que el UE almacena la clave de autenticación, y a continuación utilizar la clave para liberar todos los demás UEs que recibieron la misma clave. Una solución podría ser que la clave esté almacenada en el UE de una manera en la que no se pueda acceder fácilmente a la clave de autenticación, tal como en una tarjeta de SIM. Pero, en cualquier caso, tal solución es altamente dependiente de que la clave sea enviada de antemano en un canal encriptado. Por ejemplo, si la encriptación no está activada, esta solución no resuelve el problema.

La Fig. 2A y la Fig. 2B por lo tanto muestran una implementación mejorada, en la cual elementos con la misma referencia mantienen los mismos números y las acciones con la misma referencia tienen números de sufijo similares. En la implementación de la Fig. 2A y la Fig. 2B, el selector de clave 106 del nodo N_r selecciona (acción 2-0) la clave de autenticación como en la implementación previa, y almacena (acción 2-1) la clave de autenticación en la memoria de almacenamiento de clave 107. Cuando la interacción va a ser establecida entre el nodo N_i y el nodo N_r, como acción 2-2A la función de establecimiento de interacción 102 va a buscar la clave de autenticación. A continuación, como acción 2-2B, la función de establecimiento de interacción 102 utiliza la clave de autenticación como entrada a un generador de indicios 116. El generador de indicios 116 es preferiblemente una función de un solo sentido, que extrae a la función de establecimiento de interacción 102 unos indicios o código de autenticación. Los indicios de autenticación están así relacionados con la clave de autenticación mediante la función del generador de indicios 116. Los indicios de autenticación son proporcionados a una rutina de inclusión de indicios 112 de la función de autenticación de interacción 102, que incluye los indicios de autenticación en un mensaje de establecimiento de interacción que es enviado como acción 2-3 desde el nodo N_i al Nodo N_r. La transmisión del mensaje de establecimiento de interacción, con sus indicios de autenticación incluidos, es preferiblemente en un canal encriptado. Como acción 2-4, el nodo N_r almacena los indicios de autenticación en su memoria de almacenamiento de indicios 108 (que es también preferiblemente una memoria no volátil).

Como en la implementación anterior, la Fig. 2B muestra la función de detección/notificación de terminación/fallo 101 enviando a continuación considerablemente, como acción 2-5, una notificación a la función de terminación de interacción 103 de que la interacción con el nodo N_r (bien el nodo N_r solo o un grupo de nodos a los cuales pertenece el nodo N_r) debe ser terminada. Cuando se recibe tal notificación, como acción 2-6 la función de terminación de interacción 103 obtiene la clave de autenticación de la memoria de almacenamiento de clave 107 (o el selector de clave 106). La clave de autenticación es proporcionada a una rutina de inclusión de clave 114 de la función de terminación de interacción 103, que incluye la clave de autenticación en un mensaje de terminación de interacción que es enviado como acción 2-7 sobre la interfaz aérea desde el nodo N_i al Nodo N_r.

Tras la recepción del mensaje de terminación enviado como acción 2-7, como acción 2-8A la función de terminación de interacción 104 envía la clave de autenticación que se acaba de recibir al generador de indicios 118. Además, como acción 2-9 la función de terminación de interacción 104 solicita que los indicios de autenticación almacenados

de la memoria de almacenamiento de indicios 108 del autenticador de terminación 100, sean enviados como acción 2-10A al validador de clave 110.

Como acción 2-8B, el generador de indicios 118 utiliza la clave de autenticación que se acaba de recibir (recibida en el mensaje de terminación de la acción 2-7) para calcular unos indicios correspondientes. A este respecto, el generador de indicios 118 del nodo N_r opera en la misma función de un solo sentido como generador 116 del nodo N_i de manera que si la clave de autenticación apropiada fuese incluida en el mensaje de terminación de la acción 2-7, el generador de indicios 118 calcularía los mismos indicios de autenticación como determinados previamente por el generador de indicios 116.

La acción 2-10B muestra al generador de indicios 118 enviando al validador de clave 110 los indicios calculados por el generador de indicios 118. Como acción 2-11, el validador de clave 110 compara los indicios de autenticación calculados por el generador de indicios 118 (basándose en la clave de autenticación recibida en el mensaje de terminación (por ejemplo, recibido en el mensaje 2-7)) con los indicios de autenticación almacenados recibidos previamente y que están almacenados en la memoria de almacenamiento de indicios 108. Si existe una coincidencia de los dos indicios como acción 2-11, la función de terminación de interacción 104 es así notificada (acción 2-12), de manera que la función de terminación de interacción 104 del nodo N_r considera el mensaje de terminación como acción 2-7 como autenticado, y sigue con la terminación. Si no hay ninguna coincidencia en la acción 2-11, el mensaje de terminación no es autenticado y el nodo N_r simplemente ignora el mensaje de terminación.

De lo anterior, puede verse que la implementación de la Fig. 1A y la Fig. 1B es un caso especial (simplificado) de la implementación más general de la Fig. 2A y la Fig. 2B. A la vista de esto, para realizar la implementación de la Fig. 1A y la Fig. 1B, el generador de indicios 116 puede elegir la clave de autenticación real como seleccionada por el selector de clave 106 para ser los indicios de autenticación. En otras palabras, en la implementación de la Fig. 1A y la Fig. 1B, los indicios de autenticación se relacionan con la clave de autenticación siendo iguales a la clave de autenticación.

Como se ha mencionado anteriormente, en la implementación de la Fig. 2A y la Fig. 2B los indicios de autenticación están relacionados con la clave de autenticación mediante una función. Una función de ejemplo que extrae un código de autenticación que está relacionado con la clave de autenticación es una función de Kasumi. Tal función de Kasumi puede ser expresada como $C=Kasumi(M)_{CLAVE\ DE\ AUTENTICACIÓN}$, donde: M es un parámetro obtenido a partir de una identidad del nodo de telefonía móvil; CLAVE DE AUTENTICACIÓN es un parámetro obtenido a partir de la clave de autenticación; y C son los indicios de autenticación (por ejemplo, el código de autenticación). Pueden emplearse varias técnicas para obtener el parámetro M y el parámetro CLAVE DE AUTENTICACIÓN. Por ejemplo, M puede ser obtenido a partir de varias ocurrencias concatenadas (por ejemplo, dos) de la U-RNTI del nodo de telefonía móvil; el parámetro CLAVE DE AUTENTICACIÓN puede ser obtenido a partir de varias ocurrencias (por ejemplo dos) concatenadas de la clave de autenticación. Como otro ejemplo, M puede por el contrario ser obtenido a partir de una o de varias ocurrencias concatenadas de la representación binaria de la identidad del UE de la red de núcleo (CN – Core Network, en inglés), por ejemplo, la IMSI del nodo de telefonía móvil. La representación binaria de la IMSI puede ser construida concatenando la representación binaria de cada uno de los 15 dígitos (donde cada dígito está representado por cuatro bits) y rellenando con ceros binarios hasta que el resultado es 64 bits. En otro ejemplo más, M es obtenido a partir de varias ocurrencias concatenadas (por ejemplo dos) de la TMSI o de la P-TMSI (cada una de ellas es de 32 bits) del nodo de telefonía móvil. La identidad del UE de la red de núcleo puede ser particularmente apropiada en un modo de separación en el cual la U-RNTI no está disponible en la red de núcleo.

Tanto para la implementación de la Fig. 1A/Fig. 1B como para la implementación de la Fig. 2A/Fig. 2B, hay dos modos de operación de ejemplo, como se ha indicado previamente. En un modo de operación de autenticación de liberación, el mecanismo de autenticación (por ejemplo, el autenticador de terminación 100_i y el autenticador de terminación 100_r) protegen frente a un mensaje de liberación de conexión no autorizada dirigido a un nodo de telefonía móvil de la red, por ejemplo, una estación de telefonía móvil tal como una unidad de equipo de usuario, frustrando por ello un intento de solicitud de un procedimiento de liberación de conexión no autorizada relativa a una conexión que implica al nodo de telefonía móvil. En un modo de operación de autenticación de separación, el mecanismo de autenticación protege frente a un mensaje de separación no autorizada transmitido engañosamente en nombre de un nodo de telefonía móvil, frustrando por ello un intento de solicitud de un procedimiento de separación no autorizada para el nodo de telefonía móvil.

Los dos modos de ejemplo pueden ser llevados a la práctica en varios tipos de redes de comunicación que implican a una interfaz aérea, por ejemplo, utilizando varios tipos de redes de acceso por radio. En aras de la simplicidad y sólo a modo de ejemplo, los dos modos se describen a continuación en esta memoria en el contexto de un sistema de telecomunicaciones de telefonía móvil universal (UMTS – Universal Mobile Telecommunications System, en inglés) 10 mostrado en la Fig. 3 y en la Fig. 7. Una red de núcleo externa, orientada a la conexión, representativa, mostrada como una nube 12 puede ser por ejemplo la Red Telefónica Conmutada Pública (PSTN – Public Switched Telephone Network, en inglés) y/o la Red Digital de Servicios Integrados (ISDN – Integrated Services Digital Services, en inglés). Una red de núcleo externa, sin conexión, representativa, mostrada como una nube 14, puede ser por ejemplo la Internet. Ambas redes de núcleo están acopladas a sus correspondientes nodos de servicio 16.

La red orientada a la conexión PSTN/ISDN 12 está conectada a un nodo de servicio orientado a la conexión tal como un Centro de Conmutación para Telefonía Móvil (MSC – Mobile Switching Center, en inglés) que proporciona servicios de circuitos conmutados, mientras que la red orientada a sin conexión Internet 14 está conectada a través de un nodo de soporte de Servicio de Radio en Paquetes General de Puerta de Enlace (GGSN – Gateway General packet radio service (GPRS) Support Node, en inglés) a un Nodo de Servicio de Servicio de radio en paquetes general (SGSN – General paquet radio service (GPRS) Service Node, en inglés), estando el último adaptado para proporcionar servicios del tipo de paquetes conmutados.

Cada uno de los nodos de servicio de la red de núcleo se conecta a una Red de Acceso por Radio Terrestre de UMTS (UTRAN – UMTS Terrestrial Radio Access Network, en inglés) 24 sobre una interfaz de red de acceso por radio (RAN – Radio Access Network, en inglés) denominada interfaz de Iu. La UTRAN 24 incluye uno o más controladores de red de radio (RNCs – Radio Network Controllers, en inglés) 26 y una o más estaciones de base (BS – Base Station, en inglés) 28. En aras de la simplicidad, la UTRAN 24 de la Fig. 3 y de la Fig. 7 se muestra sólo con dos nodos RNC, particularmente el RNC 26_1 y el RNC 26_2. Cada RNC 26 está conectado a dos o más estaciones de base (BS – Base Station, en inglés) 28. Por ejemplo, y de nuevo en aras de la simplicidad, se muestran dos nodos de estación de base conectados a cada RNC 26. A la vista de esto, el RNC 26_1 sirve a la estación de base $28_{1\text{-}1}$ y la estación de base $28_{1\text{-}2}$, mientras que el RNC 26_2 sirve a la estación de base $28_{2\text{-}1}$ y a la estación de base $28_{2\text{-}2}$. Resultará evidente que un número de estaciones de base diferente pueden ser servidas por cada RNC y que los RNCs no necesitan servir al mismo número de estaciones de base. Además, la Fig. 3 y la Fig. 7 muestran que un RNC puede estar conectado sobre una interfaz de Iu a uno más de otros RNCs en la UTRAN 24. Además, resultará también evidente para los expertos en la materia que una estación de base es algunas veces denominada en el sector como una estación de base de radio, un nodo B o un nodo-B.

Debe entenderse que al menos uno y probablemente más de los RNCs de la red de acceso por radio tienen una interfaz a una o más redes de núcleo. Además, con el fin de soportar la continuación de conexiones establecidas cuando el UE se está moviendo entre celdas controladas por diferentes RNCs en la Red de Acceso por Radio, una Red de Señalización (por ejemplo, el Sistema de Señalización Nº 7) permite a los RNCs llevar a cabo la señalización de RNC-RNC requerida.

En las realizaciones ilustradas, en aras de la simplicidad cada estación de base 28 se muestra sirviendo a una celda. Cada celda está representada por un círculo que rodea a la estación de base respectiva. Resultaré evidente para los expertos en la materia, no obstante, que una estación de base puede servir para comunicarse a través de la interfaz aérea para más de una celda. Por ejemplo, dos celdas pueden utilizar recursos situados en las mismas instalaciones de estación de base. Además, cada celda puede estar dividida en uno o más sectores, teniendo cada sector una o más celdas/portadoras.

Una unidad de equipo de usuario (UE – User Equipment, en inglés), tal como la unidad de equipo de usuario (UE – User Equipment, en inglés), 30 mostrada en la Fig. 3 y en la Fig. 7, se comunica con una o más celdas o con una o más estaciones de base (BS – Base Station, en inglés) 28 sobre una interfaz de radio o aérea 32. Cada uno de la interfaz de radio 32, la interfaz de Iu, la interfaz de Iub, y la interfaz de Iur se muestran mediante líneas de trazo y punto en la Fig. 3 y en la Fig. 7.

Preferiblemente, el acceso por radio se basa en el Acceso Múltiple por División de Código de Banda Ancha (WCDMA – Wideband Code Division Multiple Access, en inglés) siendo los canales de radio individuales asignados utilizando códigos de difusión de CDMA. Por supuesto, pueden emplearse otros métodos de acceso. El WCDMA proporciona un gran ancho de banda para servicios de multimedios y para otras demandas de alta velocidad de transmisión así como características robustas como proporcionar diversidad y los receptores de RAKE para asegurar una alta calidad.

Pueden existir diferentes tipos de canales entre una de las estaciones de base 28 y las unidades de equipo de usuario (UEs. User Equipment units, en inglés) 30 para el transporte de datos de control y de usuario. Por ejemplo, en la dirección de transmisión o de enlace descendente hay varios tipos de canales de emisión que incluyen un canal de transmisión general (BCH – Broadcast CHannel, en inglés), un canal de localización (PCH – Paging CHannel, en inglés), un canal de control común (CPICH – Common PIlot CHannel, en inglés), y un canal de acceso para transmisión (FACH – Forward Access CHannel, en inglés) para proporcionar varios otros tipos de mensajes de control a las unidades de equipo de usuario (UEs – User Equipment, en inglés). El Canal de Acceso para Transmisión (FACH – Forward Access CHannel, en inglés) se utiliza también para transportar datos de usuario. En la dirección inversa o de enlace ascendente, un canal de acceso aleatorio (RACH – Random Access CHannel, en inglés) es empleado por las unidades de equipo de usuario (UEs – User Equipment units, en inglés) siempre que se desee un acceso para llevar a cabo el registro de la ubicación, la iniciación de una llamada, la respuesta a una localización y otros tipos de operaciones de acceso. El canal de acceso aleatorio (RACH – Random Access CHannel, en inglés) se utiliza también para transportar ciertos datos de usuario, por ejemplo, datos de paquetes de mejor esfuerzo, por ejemplo, aplicaciones de navegadores de la Red. Pueden asignarse canales dedicados (DCH – Dedicated CHannels, en inglés) para transportar comunicaciones de llamadas sustantivas con una unidad de equipo de usuario (UE).

La Fig. 4 muestra aspectos generales seleccionados de una unidad de equipo de usuario (UE) 30 y nodos ilustrativos tales como un controlador de red de radio 26 y una estación de base 28. La unidad de equipo de usuario (UE) 30 mostrada en la Fig. 4 incluye una unidad de procesamiento de datos y de control 31 para controlar varias operaciones requeridas por la unidad de equipo de usuario (UE – User Equipment, en inglés). La unidad de procesamiento de datos y de control 31 del UE proporciona señales de control así como datos a un transceptor 33 de radio conectado a una antena 35.

El controlador de red de radio 26 y la estación de base 28 de ejemplo tal como se muestran en la Fig. 4 son nodos de red de radio que incluyen cada uno una unidad de procesamiento de catos y de control 36 y 37, respectivamente, para llevar a cabo numerosas operaciones de radio y de procesamiento de datos requeridas para conducir las comunicaciones entre el RNC 26 y las unidades de equipo de usuario (UE – User Equipment, en inglés) 30. Parte del equipo controlado por la unidad de procesamiento de datos y de control 37 de la estación de base incluye varios transceptores 38 de radio conectados a una o más antenas 39.

La Fig. 3 ilustra un ejemplo de un modo de operación de autenticación de liberación. En el modo de autenticación de liberación de ejemplo ilustrado, un nodo de control de red de acceso por radio sirve como primer nodo o nodo N_i, es decir, el nodo que proporciona los indicios/clave de autenticación y que emite el mensaje de terminación. En este sentido, la Fig. 3 muestra el controlador de red de radio (RNC – Radio Network Controller, en inglés) 26_1 incluyendo el autenticador de terminación 100_i y el nodo de telefonía móvil o la unidad de equipo de usuario 30 incluyendo el autenticador de terminación 100_r.

Las Fig. 5A y la Fig. 5B ilustran una manera de ejemplo para llevar a cabo el modo de operación de autenticación de liberación que utiliza la implementación de la Fig. 1A/Fig. 1B. En la Fig. 5A y en la Fig. 5B, el nodo de red de acceso por radio (por ejemplo, el controlador de red de radio (RNC – Radio Network Controller, en inglés) 26_1) proporciona los indicios de autenticación al nodo de telefonía móvil (por ejemplo, la unidad de equipo de usuario 30) en un primer mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés) (por ejemplo, un mensaje de establecimiento de conexión de control de recurso de radio (RRC – Radio Resource Control, en inglés)), e incluye la clave de autenticación en un segundo mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés) (por ejemplo, un mensaje de liberación de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés). La unidad de equipo de usuario 30 confirma que la clave de autenticación incluida en el segundo mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés) está relacionada con los indicios de autenticación como condición para llevar a cabo la operación de liberación de conexión.

En la Fig. 5A y la Fig. 5B, los elementos de la misma referencia mantienen los mismos números y las acciones de la misma referencia tienen número de sufijo similares que en Fig. 1A y la Fig. 1B, respectivamente. En la Fig. 5A y la Fig. 5B, la clave de autenticación es una clave de autenticación de liberación que está asociada a la unidad de equipo de usuario 30 ó a un grupo de unidades de equipo de usuario (o, a todos los UEs que tienen este RNC 26_1 como el RNC de Servicio). La clave de liberación de autenticación es seleccionada (acción 5-0), almacenada de una manera que sobrevive a la reinicialización del RNC 26_1 (acción 5-1), y a los que se fue a buscar (acción 5-2) para su inclusión en un mensaje de establecimiento de conexión enviado a la unidad de equipo de usuario 30 junto con un procedimiento de establecimiento de conexión.

En la Fig. 5A y la Fig. 5B, el procedimiento de establecimiento de conexión, con su envío de un mensaje de establecimiento de conexión apropiado, es repetido para cada unidad de equipo de usuario, típicamente en el establecimiento de la conexión de RRC y siempre que la U-RNTI para un UE cambia, tal como en la recolocación del SRNC. En el ejemplo ilustrado, el mensaje de establecimiento de conexión es un mensaje de establecimiento de conexión del control de recurso de radio (RRC). La clave de liberación de autenticación es enviada en un canal encriptado, por ejemplo, el canal de control dedicado (DCCH – Dedicated Control CHannel, en inglés). En este sentido, la Fig. 5A y la Fig. 5B muestran un formateador de canal (DCCH) 119 que comprende el controlador de red de radio (RNC) 26_1 que está implicado en la transmisión del mensaje de establecimiento de conexión de la acción 5-3. Cuando la unidad de equipo de usuario 30 recibe la clave de liberación de autenticación, la unidad de equipo de usuario 30 almacena la clave de autenticación en una memoria de almacenamiento de clave 108.

Cuando el controlador de red de radio (RNC) 26_1 necesita liberar una o varias unidades de equipo de usuario en el CCCH o en el PCCH (por ejemplo después de que el RNC ha llevado a cabo la reinicialización cuando se han perdido los contextos del UE), el controlador de red de radio (RNC) 26_1 incluye la clave de liberación de autenticación en el mensaje de liberación representado como acción 5-7. Como se ha mencionado anteriormente, el mensaje de liberación puede ser un mensaje de liberación de conexión del control de recurso de radio (RNC).

Cuando la unidad de equipo de usuario 30 recibe el mensaje de liberación de la acción 5-7, el validador de clave 110 compara en el mensaje de liberación recibido la clave de liberación de autenticación con su clave de liberación de autenticación almacenada recibida previamente, como se comprende junto con la descripción previa de la Fig. 1B. Si hay una coincidencia, la unidad de equipo de usuario 30 considera el mensaje como autenticado y sigue con la liberación (es decir, entra en el modo de reposo). Si no hubiese ninguna coincidencia, la liberación no es autenticada y la unidad de equipo de usuario simplemente ignora el mensaje.

La Fig. 6A y la Fig. 6B ilustran una manera de ejemplo para llevar a cabo el modo de operación de autenticación de liberación utilizando la implantación de la Fig. 2A/Fig. 2B. De nuevo en la Fig. 6A y en la Fig. 6B, el nodo de red de acceso por radio (por ejemplo, el controlador de red de radio (RNC) 26_1 proporciona los indicios de liberación de autenticación al nodo de telefonía móvil (por ejemplo, a la unidad de equipo de usuario 30), e incluye la clave de liberación de autenticación en un segundo mensaje del control de recurso de radio (RRC – Radio Resource Control, en inglés) (por ejemplo, un mensaje de liberación de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés)). La unidad de equipo de usuario 30 confirma que la clave de liberación de autenticación incluida en el segundo mensaje del control de recurso de radio (RRC – Radio Resource Control, en inglés) está relacionada con los indicios de liberación de autenticación como condición para llevar a cabo la operación de liberación de conexión.

En la Fig. 6A y en la Fig. 6B, elementos con la misma referencia mantienen los mismos números y acciones con la misma referencia tienen números de sufijo similares a los de la Fig. 2A y la Fig. 2B, respectivamente. En la Fig. 6A y la Fig. 6B, los indicios de liberación de autenticación están asociados a una unidad de equipo de usuario con un grupo de unidad de equipo de usuarios (o bien, a todos los UEs que tienen este RNC 26_1 como el RNC de Servicio). La clave de liberación de autenticación es seleccionada (acción 6-0) y almacenada de una manera que sobrevive a una reinicialización del RNC 26_1 (acción 6-1).

Cuando se establece una conexión de RRC con una unidad de equipo de usuario tal como la unidad de equipo de usuario 30, el RNC de servicio 26_1 asigna una U-RNTI a la unidad de equipo de usuario 30. Como se ha explicado previamente, la U-RNTI (UTRAN Radio Network Temporary Identity, en inglés) es una identidad global que identifica a la unidad de equipo de usuario 30 para la UTRAN. El SRNC 26_1 utiliza la clave de liberación de autenticación (que se ha ido a buscar en la acción 6-2A) junto con la U-RNTI como entrada (véase la acción 6-2B) al generador de indicios 116. El generador de indicios 116 es una función F de un solo sentido que utiliza la U-RNTI y la clave de liberación de autenticación para generar los indicios de liberación de autenticación. Los indicios de liberación de autenticación sirven como un código de liberación de autenticación individual del UE. La función F de un solo sentido del generador de indicios 116 se diseña de una manera que la clave de liberación de autenticación no puede ser obtenida a partir de la U-RNTI y del código de liberación de autenticación individual del UE.

La rutina de inclusión de indicios 112 incluye los indicios de liberación de autenticación en un mensaje de establecimiento de conexión enviado a la unidad de equipo de usuario 30 junto con un procedimiento apropiado o con una coyuntura apropiada. Tales procedimientos/coyunturas apropiados incluyen (por ejemplo) lo siguiente: un procedimiento de establecimiento de conexión; cada vez que una nueva U-RNTI es reasignada (utilizando, por ejemplo, el mensaje de Información de Movilidad de la UTRAN o el mensaje de Reconfiguración de Canal de Transporte); después de que se ha iniciado el cifrado, pero no junto con la reasignación de una U-RNTI, típicamente utilizando el mensaje de Información de Movilidad de la UTRAN. En la realización de ejemplo ilustrada, el mensaje de establecimiento de conexión representado por la acción 6-3 es un mensaje del control de recurso de radio (RRC – Radio Resource Control, en inglés) (por ejemplo, un mensaje de establecimiento de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés)). Como en la Fig. 5A y en la Fig. 5B, los indicios de liberación de autenticación son enviados en un canal encriptado, por ejemplo, el canal de control dedicado (DCCH – Dedicated Control CHannel, en inglés). Por lo tanto, la Fig. 6A y la Fig. 6B muestran también un formateador de canal (DCCH) 119 que comprende el controlador de red de radio (RNC – Radio Network Controller, en inglés) 26_1 estando implicado en la transmisión del mensaje de establecimiento de conexión de la acción 6-3. Cuando la unidad de equipo de usuario 30 recibe los indicios de liberación de autenticación, la unidad de equipo de usuario 30 almacena los indicios de liberación de autenticación en la memoria de almacenamiento de indicios 108.

Así, el controlador de rad de radio (RNC – Radio Network Controller, en inglés) 26_1 envía los indicios de liberación de autenticación, que sirven como código de liberación de autenticación individual del UE, a la unidad de equipo de usuario 30. Como en la Fig. 5A y la Fig. 5B, este procedimiento con su transmisión del código de liberación de autenticación individual del UE es repetido para cada unidad de equipo de usuario, y es típicamente llevado a cabo poco después del establecimiento de la conexión de RRC (esto es, cuando la U-RNTI es asignada por primera vez) al UE respectivo, y siempre que la U-RNTI para un UE cambie (tal como en una reasignación del SRNC). La clave individual del UE debe ser enviada en un canal encriptado, por ejemplo, el canal de control dedicado (DCCCH). Si el canal no está encriptado, puede utilizarse una unidad de protección de integridad para impedir que un intermediario actúe como una falsa estación de base asignando códigos de liberación de autenticación individuales para el UE falsos (también puede combinarse con la encriptación). En cualquier caso, el SRNC puede elegir utilizar o no la encriptación cuando envía el código de liberación De autenticación individual para el UE.

Cuando el RNC necesita liberar uno o varios URs en el CCCH o en PCCH (por ejemplo después de una reinicialización del RNC cuando se han perdido los contextos del UE), de manera similar a la de la Fig. 2B el controlador de red de radio (RNC RRC – Radio Network Control, en inglés) 26_1 incluye la clave de liberación De autenticación en el mensaje de liberación (acción 6-7). Cuando la unidad de equipo de usuario 30 recibe el mensaje de liberación de la acción 6-7, el validador de clave 110 de la unidad de equipo de usuario 30 utiliza la clave de liberación de autenticación y la U-RNTI como entrada (véase la acción 6-8A) al generador de indicios 118 el cual, debe recordarse, es una función F de un solo sentido que proporciona un código de liberación de autenticación individual para el UE (por ejemplo, indicios de liberación de autenticación) como salida. Como acción 6-11, el

validador de clave 110 de la unidad de equipo de usuario 30 compara a continuación el código de liberación de autenticación individual para el UE calculado (obtenido del generador de indicios 118 y aplicado como acción 6-10B al validador de clave 110) con su código de liberación de autenticación individual para el UE recibido previamente. Si hay una coincidencia en el validador de clave 110, la unidad de equipo de usuario 30 considera el mensaje como validado y sigue con la liberación (es decir, entra en el modo de reposo). Si no hubiese ninguna coincidencia, la liberación no es validada y la unidad de equipo de usuario 30 simplemente ignora el mensaje de la acción 6-3.

La Fig. 7 ilustra un ejemplo del modo de operación de autenticación de separación. En el modo de operación de autenticación de separación, en una implantación de ejemplo el primer nodo (que proporciona los indicios de autenticación al segundo nodo de la red) es un nodo de telefonía móvil (por ejemplo, una unidad de equipo de usuario 30) y el segundo nodo es un nodo de red de núcleo (por ejemplo, un MSC). De este modo, en el modo de autenticación de separación de ejemplo ilustrado, la unidad de equipo de usuario o el nodo de telefonía móvil sirven como el primer nodo o nodo N_i, es decir, el nodo que proporciona los indicios/clave de autenticación y que emite el mensaje de separación. En este sentido, la Fig. 7 muestra la unidad de equipo de usuario 30 incluyendo el autenticador de terminación 100_i y el nodo de MSC 190 incluyendo el autenticador de terminación 100_r.

En el modo de autenticación de separación, el nodo de telefonía móvil puede proporcionar los indicios de autenticación a la red de núcleo cuando se da la ocurrencia de un evento predeterminado (por ejemplo, el registro de un nodo de telefonía móvil con la red de núcleo). A continuación, cuando se inicia una operación de separación, el nodo de telefonía móvil 30 incluye la clave de autenticación, por ejemplo, en un mensaje de separación (por ejemplo, un mensaje de indicación de separación de IMSI). Como condición para llevar a cabo esta parte de la operación de separación, el nodo de red de núcleo confirma primero que la clave de autenticación comunicada al nodo de red de núcleo en el mensaje de separación está relacionada con los indicios de autenticación recibidos previamente. En una implementación, el nodo de de telefonía móvil utiliza la IMSI o la TMSI del nodo de telefonía móvil para generar los indicios de autenticación que son proporcionas a la red de núcleo, y asimismo el nodo de red de núcleo utiliza la IMSI o la TMSI del nodo de telefonía móvil para confirmar que la clave de autenticación está relacionada con los indicios de autenticación.

Como se muestra con más detalle en la Fig. 8A y en la Fig. 8B, el autenticador de terminación 100_i de la unidad de equipo de usuario 30 trabaja junto con otras funciones de la unidad de equipo de usuario, que incluyen la función de detección/notificación de separación 701, la función de establecimiento (registro) de interacción 702 y la función de terminación (separación) de interacción 703. De manera similar, el autenticador de terminación 100_r funciona junto con otras funciones del nodo MSC 198, que incluyen la función de terminación de interacción 704 y la función de establecimiento de interacción 705. De nuevo, resultará evidente que tanto la unidad de equipo de usuario 30 como el nodo MSC 198 tienen otras numerosas funciones no específicamente descritas en esta memoria, pero que son de otra forma conocidas para el experto en la materia.

En la realización de la Fig. 8A y la Fig. 8B, el autenticador de terminación 100_i incluye un selector de clave 706, una memoria de almacenamiento de clave 707, un generador de indicios 716, mientras que el autenticador de terminación 100_r incluye una memoria de almacenamiento de clave 708, un validador de clave 710, un generador de indicios 718. Una vez más, estas divisiones funcionales son para proporcionar una ilustración de las operaciones del autenticador de terminación 100i y del autenticador de terminación 100r, y no son críticas, sino más bien a modo de ejemplo. De nuevo resultará evidente que estas funciones pueden estar distribuidas o asignadas de varias maneras, incluyendo utilizar uno o más circuitos de hardware individuales, utilizar software que funciona junto con un microprocesador digital programado adecuadamente o un ordenador de propósito general, utilizar un circuito integrado específico para una aplicación (ASIC – Application Specific Integrated Circuit, en inglés), y/o utilizar uno o más procesadores de señal digital (DSPs – Digital Signal Processors, en inglés).

Excepto como se explica específicamente a continuación, las operaciones del autenticador de terminación 100_i y del autenticador de terminación 100_r en el modo de operación de autenticación por separación son generalmente análogas a las realizaciones previas. En general, las operaciones de varios componentes y funcionalidades son comparables a los respectivos elementos de realizaciones anteriores que tienen los mismos números de referencia de dos dígitos de orden inferior. En aras de la simplicidad, sólo se describe una implementación del modo de autenticación de separación de acuerdo con la implementación de la Fig. 2A y de la Fig. 2B, particularmente con referencia a la Fig. 8A y a la Fig. 8B. Como se recordará, la implementación de la Fig. 2A y de la Fig. 2B incluye la generación y al transmisión de los indicios de separación de autenticación, los cuales en la Fig. 8A y en la Fig. 8B corresponden a los indicios de separación de autenticación. Se comprenderá fácilmente cómo el modo de autenticación de separación puede ser implementado utilizando la Fig. 1A y la Fig. 1B (en las cuales los indicios de separación de autenticación son iguales a la clave de separación de autenticación).

En el caso de Fig. 8A y de la Fig. 8B, el selector de clave 706 de la unidad de equipo de usuario 30 como acción 8-0 selecciona la clave de separación de autenticación. La clave de separación de autenticación es almacenada en la memoria de almacenamiento de clave 707 (acción 8-1). Como acción 8-2A la función de autenticación de interacción 702 va a buscar la clave de separación de autenticación de la memoria de almacenamiento de clave 707 (o del selector de clave 706) y el generador de indicios 716 proporciona con la identidad del UE (tal como la IMSI o la TMSI) y la clave de separación de autenticación, obteniendo a su vez (véase la acción 8-2B) unos indicios de

terminación. En el modo de autenticación por separación, los indicios de terminación son el código de separación de autenticación, que sirve como código de separación de autenticación individual del UE.

De una manera similar a ciertas realizaciones previas, el generador de indicios 716 es una función F de un solo sentido. En la Fig. 8A, el generador de indicios 716 recibe, como entrada, tanto la clave de separación de autenticación como la identidad del UE (tal como la IMSI o la TMSI) calculan el código de separación de autenticación individual del UE.

En algún punto predeterminado en el tiempo, por ejemplo durante un procedimiento de registro en el cual la unidad de equipo de usuario 30 se registra con la red de núcleo, el código de separación de autenticación individual del UE (por ejemplo, el índice de separación de autenticación) es transmitido a la red de núcleo, por ejemplo durante el procedimiento de registro. Siguiendo con este ejemplo y utilizando el registro como el evento predeterminado para provocar la transmisión de los indicios de autenticación de separación (código), Fig. 8A muestra la transmisión de los indicios de autenticación de separación (código) como acción 8-3 en un mensaje de registro de la unidad de equipo de usuario. Cuando se recibe el mensaje de la acción 8-3 en la red de núcleo, por ejemplo, en el nodo MCS 198, los indicios (código) de autenticación de autenticación de separación son almacenados en la memoria de almacenamiento de indicios 708.

Cuando la función de detección/notificación de separación 101 determina que el usuario desea que se realice una operación de separación (por ejemplo, el usuario desconecta la unidad de equipo de usuario 30), como acción 8-5 (véase la Fig. 8B) la función de terminación de interacción 703 es así notificada. La función de terminación de interacción 703 prepara un mensaje de separación (tal como un mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI, por ejemplo), y haciendo esto como acción 8-6 obtiene la clave de autenticación de separación de la memoria de almacenamiento de clave 707. La clave de autenticación de separación es incluida en el mensaje de separación enviado como acción 8-7.

Cuando el nodo de red de núcleo (por ejemplo, el nodo MSC 198) recibe el mensaje de INDICACIÓN DE SEPARACIÓN DE IMSI de la acción 8-7, como acción 8-8A el nodo de red de núcleo utiliza la clave de separación de autenticación como entrada al generador de indicios 718 (la función F de un solo sentido) junto con la identidad del UE (tal como la IMSI o la TMSI). Como acción 8-8B, el generador de indicios 718 calcula un código de separación de autenticación individual para el UE, el cual es enviado al validador de clave 710 como acción 8-10B. El código de separación de autenticación individual para el UE es comparado como acción 8-11 por el validador de clave 710 con el código de separación de autenticación individual para el UE almacenado obtenido como acción 8-10A de la memoria de almacenamiento de clave 708. Si el validador de clave 710 determina que hay una coincidencia, el nodo MSC 198 continúa con el procedimiento de liberación de conexión de radio (incluyendo marcar el UE como separado). Si no se determina ninguna coincidencia por el validador de clave 710, el nodo MSC 198 ignora el mensaje de separación de la acción 8-7, es decir, el estatus del registro de la unidad de equipo de usuario 30 no ha cambiado, y el nodo MSC 198 continúe el procedimiento de liberación de conexión de radio (véase la Fig. 13).

Los generadores de indicios descritos anteriormente, que sirven como función F de un solo sentido, pueden ser implementados de un número de maneras diferentes. Como ejemplo, los generadores de indicios son implementados utilizando una función de cifrado de bloques de Kasumi tal como la descrita en el documento 3GPP TS 35.202: 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspect; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Documento 2: Especificación de Kasumi. Encriptar un mensaje que consiste en un bloque de bits, se define en la Expresión 1.

Expresión 1: $C=KASUMI(M)_{CLAVE}$

En la Expresión 1, M es normalmente un mensaje, cuando se utiliza KASUMI como función de encriptación. C es la salida, normalmente el mensaje encriptado. CLAVE es la clave bajo la cual está encriptado el mensaje. C y M son cantidades de 64 bits, y CLAVE es una cantidad de 128 bits.

Los generadores de indicios de la presente invención no utilizan la función de cifrado de bloques de Kasumi para encriptar un mensaje. Por el contrario, los generadores de indicios utilizan la función de cifrado de bloques de Kasumi de acuerdo con la Expresión 1 de la siguiente manera:

M está construido a partir de una identidad del nodo de telefonía móvil. Por ejemplo, M puede ser obtenido a partir de varias (por ejemplo, dos) ocurrencias concatenadas de la U-RNTI del nodo de telefonía móvil. Como M es una cantidad de 64 bits y la U-RNTI es una cantidad de 32 bits, M comprende varias (por ejemplo, dos) ocurrencias concatenadas de la identidad del nodo de telefonía móvil. Como otro ejemplo, M puede por el contrario ser obtenido de una o de varias ocurrencias concatenadas de la IMSI de la representación binaria del nodo de telefonía móvil. La representación binaria de la IMSI puede ser construida concatenando la representación binaria de cada uno de los 15 dígitos (donde cada dígito está representado por cuatro bits) y rellenando con ceros binarios hasta que el resultado es 64 bits. En otro ejemplo más, M se obtiene de varias (por ejemplo, dos) ocurrencias concatenadas de la TMSI o de la P-TMSI (cada una de ellas de 32 bits) del nodo de telefonía móvil.

CLAVE está construido a partir de la clave de separación de autenticación o de la clave de liberación de autenticación. Dado que estas claves son cantidades de 64 bits, CLAVE se construye de varias (por ejemplo, dos) ocurrencias concatenadas de la clave de separación de autenticación o de la clave de liberación de autenticación.

La C resultante se utiliza como el código de separación de autenticación individual para el UE o el código de liberación de autenticación individual para el UE, y es una cantidad de 64 bits.

Una ventaja importante de utilizar la función de Kasumi es que esta función está ya soportada por los terminales y redes de telefonía móvil existentes puesto que se utiliza para llevar a cabo la encriptación o la protección de integridad. Debe observarse que 64 bits para las claves y códigos se ven en la actualidad como una longitud razonable, tanto desde el punto de vista de la seguridad como de la cabecera de la interfaz de radio. Como breve análisis de un ataque de búsqueda de clave exhaustivo, debe considerarse el hecho de que actualmente un PC ordinario puede típicamente encriptar 80 Mbit/s utilizando Kasumi, debe asumirse 128 Mbit para un límite superior. A 64 bits por bloque, esto proporciona aproximadamente 2*10^6 bloques por segundo. Cambiar la clave cada 24 horas y asumir que la clave correcta es encontrada después de que se ha buscado en la mitad del espacio de clave, esto conduce a la Expresión 2.

Expresión 2: 2^longitud(clave)*1/estación de base 1/(estación de base10^6)>=24 h

Resolviendo la Expresión 2 para la longitud(clave) se llega a la Expresión 3.

Expresión 3: longitud(clave)>=38 bits.

Esto es, la longitud de la clave de 38 bits es necesaria para un sistema marginalmente seguro. Una longitud de 64 bits proporciona un margen de 26 bits o de 67*10^6, que se considera suficientemente seguro. Una protección aun mayor será el resultado de utilizar una clave más larga, por ejemplo utilizando todo el espacio de la clave de 128 bits disponible en Kasumi. También, puede utilizarse un código más largo (tal como 128 bits). En ese caso, las claves y códigos pueden ser transportados en dos etapas. La primera parte de la clave (o del código) es enviada en un mensaje y la segunda parte en un mensaje, enviado más tarde. Cuando el móvil ha recibido ambas partes, son concatenadas y utilizadas como entrada a la función de un solo sentido.

Debe observarse que los UEs recibirán la localización incluso después de la reinicialización del RNC y por lo tanto las llamadas y paquetes terminados pueden ser encaminados hacia los UEs.

Con los mecanismos de autenticación descritos anteriormente, será más difícil que un intruso libere las conexiones de radio. Sólo la red de comunicaciones segura, por ejemplo, la UTRAN, tendrá la capacidad de liberar conexiones, proporcionando por ello una mejor protección frente a los ataques de denegación de servicio.

Los mecanismos descritos anteriormente harán más difícil que un intruso separe una unidad de equipo de usuario. Sólo la propia unidad de equipo de usuario tendrá la capacidad de indicar la separación hacia la red de núcleo. Todas las unidades de equipo de usuario activas recibirán la localización y por lo tanto los llamados paquetes de terminación pueden ser encaminados hacia las unidades de equipo de usuario.

En la Fig. 5A/Fig. 5B y la Fig. 6A/Fig. 6B, el nodo de red de acceso por radio (por ejemplo, un controlador de red de radio (RNC – Radio Network Controller, en inglés) 26_1 proporciona la clave de liberación de autenticación (en el caso de la Fig. 5A/Fig. 5B) o los indicios de liberación de autenticación (en el caso de la Fig. 6A/Fig. 6B al nodo de telefonía móvil (por ejemplo, una unidad de equipo de usuario 30) en un primer mensaje del control de recurso de radio (RRC) (por ejemplo, un mensaje de establecimiento de conexión del control de recurso de radio (RRC - Radio Resource Controller, en inglés), e incluye la clave de autenticación en un segundo mensaje del control de recurso de radio (RRC - Radio Resource Controller, en inglés) (por ejemplo, un mensaje de liberación de conexión del control de recurso de radio (RRC - Radio Resource Controller, en inglés)).

La Fig. 9A y la Fig. 9B ilustran un formato de ejemplo de los mensajes de establecimiento de conexión del control de recurso de radio (RRC - Radio Resource Controller, en inglés) de ejemplo, y muestran campos o elementos en los que la clave de liberación de autenticación (en el caso de la Fig. 5A/Fig. 5B) o los indicios de liberación de autenticación (en el caso de la Fig. 6A/Fig. 6B) pueden ser incluidos en ellos.

Las Fig. 10A – Fig. 10E ilustran formatos de ejemplo de mensajes de liberación de conexión del control de recurso de radio (RRC) de ejemplo, y muestran campos o elementos en los que la clave de liberación de autenticación (en el caso de la Fig. 5A/Fig. 5B) o los indicios de liberación de autenticación (en el caso de la Fig. 6A/Fig. 6B) pueden ser incluidos en ellos.

Como se muestra en la Fig. 9A, el mensaje de establecimiento de conexión (ESTABLECIMIENTO DE CONEXIÓN DEL RRX) incluye típicamente (entre otras cosas) los siguientes elementos de información: Identidad del CN del UE (9A-1); U-RNTI (9A-2); indicios de liberación de autenticación (9A-K); e, información de asignación de canal (9A-3).

Como se muestra en la Fig. 9B, el mensaje de INFORMACIÓN DE MOVILIDAD DE UTRAN incluye (entre otras cosas) los siguientes elementos de información: Nueva U-RNTI (9B-1); indicios de liberación de autenticación (9B-K); e, identidad de área de ubicación (9B-2).

Como se muestra en la Fig. 10A, el mensaje de LIBERACIÓN DE CONEXIÓN DE RRC (cuando se utiliza en el CCCH para liberar un grupo de UEs) incluye típicamente (entre otras cosas) los siguientes elementos de información: grupo de U-RNTI (10A-1); causa de Liberación (10A-2); y, clave de liberación de autenticación (10A-K).

Como se muestra en la Fig. 10B, el mensaje de LIBERACIN DE CONEXIÓN DE RRC (cuando se utiliza en el CCCH para liberar un único UE) incluye típicamente (entre otras cosas) los siguientes elementos de información: U-RNTI (10B-1); Causa de liberación (10B-2); y, clave de liberación de autenticación (10B-K).

Como se muestra en la Fig. 10C, el mensaje de LIBERACIÓN DE CONEXIÓN DE RRC (cuando se utiliza en el DCCH para liberar un único UE) incluye típicamente (entre otras cosas) los siguientes elementos de información: Causa de liberación (10C-2); y, clave de liberación de autenticación (10C-K).

Como se muestra en la Fig. 10D, el mensaje de TIPO DE LOCALIZACIÓN 1 (para su uso en el canal de localización cuando se libera a un único UE) incluye típicamente (entre otras cosas) los siguientes elementos de información: U-RNTI (10D-1); causa de liberación (10D-2); y, clave de liberación de autenticación (10D-K).

Como se muestra en la Fig. 10D, el mensaje de LOCALIZACIÓN DE TIPO 1 (para su uso en el canal de localización cuando libera un grupo de UEs) incluye típicamente (entre otras cosas) los siguientes elementos de información: grupo de U-RNTI (10E-1); causa de liberación (10E-2); y, clave de liberación de autenticación (10E-K).

El “grupo de U-RNTI” es un elemento de información que, por ejemplo, es utilizado junto con los mensajes de la Fig. 10A y la Fig. 10E, y es una generalización de la U-RNTI en el mensaje de liberación genérico con capacidad de liberación ómnibus. Como se muestra en la Tabla 1, el elemento de información del grupo U-RNTI comprende un campo discriminador de grupo o subelemento que indica que el mensaje está dirigido a “todos los UEs” o que los receptores del mensaje deben ser determinados utilizando el campo de “máscara de U-RNTI” o subelemento. En el primer caso en el que el mensaje de campo de discriminador del grupo es puesto a “todos los UEs”, el mensaje se dirige a todos los UEs que reciben el mensaje. Si el mensaje del campo de discriminador de grupo es puesto a “máscara de U-RNTI), un valor de U-RNTI y un índice de máscara de bit de U-RNTI se incluyen también. El último indica qué bits de la U-RNTI que deben coincidir con la U-RNTI del UE. Así, el grupo de U-RNTI es utilizado para identificar un grupo de UEs que tienen una conexión de RRC.

TABLA 1

Nombre del Elemento/grupo de Información	Necesidad	Multi	Tipo y referencia	Descripción de la semántica	Versión
ELECCIÓN discriminador de grupo	MP				REL-5
> Todos				(ningún dato)	REL-5
> Máscara de U-RNTI					REL-5
>> U-RNTI	MP		U-RNTI 10.3.3.47	Los bits que son menos significativos que la posición de bit indicada por la máscara de bits de la U-RNTI serán ignorados	REL-5
>> Índice de máscara de bit de la U-RNTI	MP		Enumerada (b1, b2,…b31)	Los valores b1 a b19 indican posiciones de bit en la S-RNTI. Los valores b20 a b31 indican posiciones de bit en la identidad del SRNC	REL-5

Así, el mensaje de terminación de interacción (por ejemplo, el mensaje de la acción 1-7, la acción 2-7, la acción 5-7 ó la acción 6-7) puede estar dirigido a una unidad de equipo de usuario individual o a un grupo de unidades de equipo de usuario, o a todas las unidades de equipo de usuario para las cuales el controlador de red de radio (RNC - Radio Network Controller, en inglés) 26_1 sirve como SRNC. Más información relativa a dirigir un mensaje de terminación de interacción a varias unidades de equipo de usuario y el un mensaje de liberación ómnibus se describe en la Solicitud de Patente de los Estados Unidos de Número de Serie 09/852.915, presentada el 11 de Mayo de 2001, y titulada “RELEASING PLURAL RADIO CONNECTIONS WITH OMNIBUS RELEASE MESSAGE”, incorporada como referencia en esta memoria.

Los conceptos de autenticación y las implementaciones anteriores pueden ser aplicados en cualquier sistema de comunicaciones de telefonía móvil, como GSM o WCDMA. Aunque el WCDMA ha sido utilizado con vistas a ilustracion y referencia, la invención no está limitada a ningún tipo particular de red de telefonía móvil.

Aunque la invención ha sido descrita junto con lo que actualmente se considera la realización más práctica y preferida, debe entenderse que la invención no debe estar limitada a la realización explicada, sino todo lo contrario, pretende cubrir varias modificaciones y disposiciones equivalentes incluidas dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método en un primer nodo (N_i) de una red de comunicaciones que comprende un primer nodo (N_i) y un segundo nodo (N_r),

caracterizado por

(1) proporcionar una clave de autenticación en el citado primer nodo (N_i) de la red de comunicación

(2) obtener unos indicios de autenticación relacionados con la clave de autenticación por medio de una función;

(3) proporcionar los indicios de autenticación obtenidos al citado segundo nodo (N_r) de la red con un mensaje de establecimiento, y a continuación subsiguientemente

(4) incluir la clave de autenticación en un mensaje de terminación de interacción transmitido sobre una interfaz aérea entre el primer nodo y el segundo nodo.

2. El método de acuerdo con la reivindicación 1, en el que los indicios de autenticación están relacionados con la clave de autenticación siendo iguales a la clave de autenticación.

3. El método de acuerdo con la reivindicación 1, en el que los indicios de autenticación C son un código de autenticación, que está relacionado con la clave de autenticación mediante una función de Kasumi C=Kasumi(M)$_{\text{CLAVE DE AUTENTICACIÓN}}$ y en la que:

M es un parámetro obtenido de una identidad de un nodo de telefonía móvil de la red de comunicación;

CLAVE DE AUTENTICACIÓN es un parámetro obtenido a partir de la clave de autenticación.

4. El método de acuerdo con la reivindicación 3, en el que M es obtenido a partir de una U-RNTI del nodo de telefonía móvil y de una identidad de UE de la red de núcleo del nodo de telefonía móvil.

5. El método de acuerdo con la reivindicación 3, en el que el parámetro CLAVE DE AUTENTICACIÓN es obtenido a partir de la clave de autenticación partiendo de varias ocurrencias concatenadas de la clave de autenticación.

6. El método de acuerdo con la reivindicación 1, en el que el primer nodo es un nodo de red de acceso por radio y el segundo nodo es un nodo de telefonía móvil,

proporcionando el nodo de red de acceso por radio los indicios de autenticación al nodo de telefonía móvil en un primer mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés);

incluyendo el nodo de acceso por radio la clave de autenticación en un segundo mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés).

7. El método de acuerdo con la reivindicación 6, en el que el primer mensaje de control de recurso de radio (RRC – Radio Resource Control, en inglés) es un mensaje de establecimiento de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés) y el segundo mensaje del control de recurso de radio (RRC – Radio Resource Control, en inglés) es un mensaje de liberación de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés).

8. El método de acuerdo con la reivindicación 6, en el que el nodo de red de acceso por radio proporciona los indicios de autenticación al nodo de telefonía móvil junto con uno de lo que sigue:

un mensaje de establecimiento de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés);

cuando se asigna una nueva U-RNTI;

después de que el cifrado ha sido iniciado.

9. El método de acuerdo con la reivindicación 1, en el que el primer nodo es un nodo de telefonía móvil y el segundo nodo es un nodo de red de núcleo,

proporcionando el nodo de telefonía móvil los indicios de autenticación al nodo de red de núcleo cuando tiene lugar un evento de terminación De interacción.

10. El método de acuerdo con la reivindicación 9, en el que el nodo de telefonía móvil comunica la clave de autenticación al nodo de red de núcleo por medio de un mensaje de indicación de separación de IMSI.

11. El método de acuerdo con la reivindicación 9, en el que el nodo de telefonía móvil utiliza una IMSI o una TMSI del nodo de telefonía móvil para generar los indicios de autenticación que son proporcionados a la red de núcleo cuando tiene lugar el evento predeterminado.

12. Un método en un segundo nodo (N_r) de una red de comunicación

caracterizado por

(1) unos indicios de autenticación del primer nodo (N_i) de la red con un mensaje de establecimiento

(2) recibir de un primer nodo (N_i) de la red de comunicación una clave de autenticación incluida en un mensaje de terminación de interacción recibido transmitido sobre una interfaz aérea entre el primer nodo y el segundo nodo,

(3) calcular unos indicios de autenticación utilizando la clave de autenticación incluida en el mensaje de terminación de interacción recibido;

(4) confirmar que los indicios de autenticación calculados coinciden con los indicios de autenticación recibidos del primer nodo como condición para llevar a cabo una operación de terminación de interacción y sólo llevando a cabo la operación de terminación de interacción si los indicios de autenticación calculados coinciden con los indicios de autenticación recibidos del primer nodo.

13. Un primer nodo (N_i) es una red de comunicación que comprende un primer nodo (N_i) y un segundo nodo (N_r),

caracterizado por

un medio para almacenar una clave de autenticación;

un medio para obtener unos indicios de autenticación relacionados con la citada clave de autenticación por medio de una función;

un medio para hacer que los indicios De autenticación sean proporcionados a un segundo nodo (N_r) con un establecimiento de mensaje;

una unidad de autenticación (100_i) dispuesta para incluir la clave de autenticación en un mensaje de terminación de interacción, que es transmitida sobre una interfaz aérea entre el primer nodo y el segundo nodo.

14. El nodo de acuerdo con la reivindicación 13, en el que los indicios de autenticación están relacionados con la clave de autenticación siendo iguales a la clave de autenticación.

15. El nodo de acuerdo con la reivindicación 13, en el que los indicios de autenticación C son un código de autenticación, que están relacionado con la clave de autenticación por medio de una función de Kasumi $C=Kasumi(M)_{CLAVE\ DE\ AUTENTICACIÓN}$ y en la que:

M es un parámetro derivado de una identidad de un nodo de telefonía móvil de la red de comunicación;

CLAVE DE AUTENTICACIÓN es un parámetro derivado de la clave de autenticación.

16. El nodo de acuerdo con la reivindicación 15, en el que M es obtenido a partir de uno de la U-RNTI del nodo de telefonía móvil y de una identidad de UE de la red de núcleo del nodo de telefonía móvil.

17. El nodo de acuerdo con la reivindicación 15, en el que CLAVE DE AUTENTICACIÓN es obtenido a partir de la clave de autenticación a partir de varias instancias concatenadas de la clave de autenticación.

18. El nodo de acuerdo con la reivindicación 13, en el que el primer nodo es un nodo de red de acceso por radio y el segundo nodo es un nodo de de telefonía móvil que comprende

un medio para proporcionar los indicios de autenticación al nodo de telefonía móvil en un mensaje de establecimiento de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés);

un medio para incluir la clave de autenticación en un mensaje de liberación de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés).

19. El nodo de acuerdo con la reivindicación 18, en el que el medio para proporcionar los indicios de autenticación proporcionan los citados indicios junto con uno de lo siguiente:

un mensaje de establecimiento de conexión del control de recurso de radio (RRC – Radio Resource Control, en inglés);

cuando se asigna una nueva U-RNTI;

después de que se ha iniciado el cifrado.

20. El nodo de acuerdo con la reivindicación 13, en el que el primer nodo es un nodo de telefonía móvil y el segundo nodo es un nodo de red de núcleo en una red de comunicación, que comprende

un medio para proporcionar los indicios de autenticación a la red de núcleo cuando se da la ocurrencia de un evento predeterminado;

un medio para comunicar la clave de autenticación a la red de núcleo cuando se da la ocurrencia de un evento de terminación de interacción.

21. El nodo de acuerdo con la reivindicación 20, en el que el evento predeterminado es el registro de un nodo de telefonía móvil con el nodo de red de núcleo.

22. El nodo de acuerdo con la reivindicación 20, en el que la operación de terminación de interacción es una operación de separación.

23. El nodo de acuerdo con la reivindicación 20, en el que el nodo de telefonía móvil utiliza un mensaje de indicación de separación de IMSI para comunicar la clave de autenticación al nodo de red de núcleo.

24. El nodo de acuerdo con la reivindicación 20, en el que el nodo de telefonía móvil utiliza una IMSI o una TMSI del nodo de telefonía móvil para generar los indicios de autenticación que se proporcionan a la red de núcleo cuando se da la ocurrencia del evento predeterminado.

25. Un segundo nodo (N_r) en una red de comunicación que comprende un primer nodo (N_i) y un segundo nodo (N_r)

caracterizado por

un medio para recibir unos indicios de autenticación con un mensaje de establecimiento transmitido sobre una interfaz aérea desde el primer nodo;

un medio para recibir desde un primer nodo (N_i) de la red de comunicación una clave de autenticación incluida en un mensaje de terminación de interacción transmitido sobre una interfaz aérea entre el primer nodo y el segundo nodo;

un medio para calcular unos indicios de autenticación utilizando la clave de autenticación incluida en el mensaje de terminación de interacción recibida;

una unidad de autenticación dispuesta para confirmar que los indicios de autenticación calculados coinciden con los indicios de autenticación recibidos desde el primer nodo.

26. Una red de comunicación

caracterizada por

un primer nodo (N_i) de acuerdo con una de las reivindicaciones 13-24 y un segundo nodo (N_r) de acuerdo con la reivindicación 25.

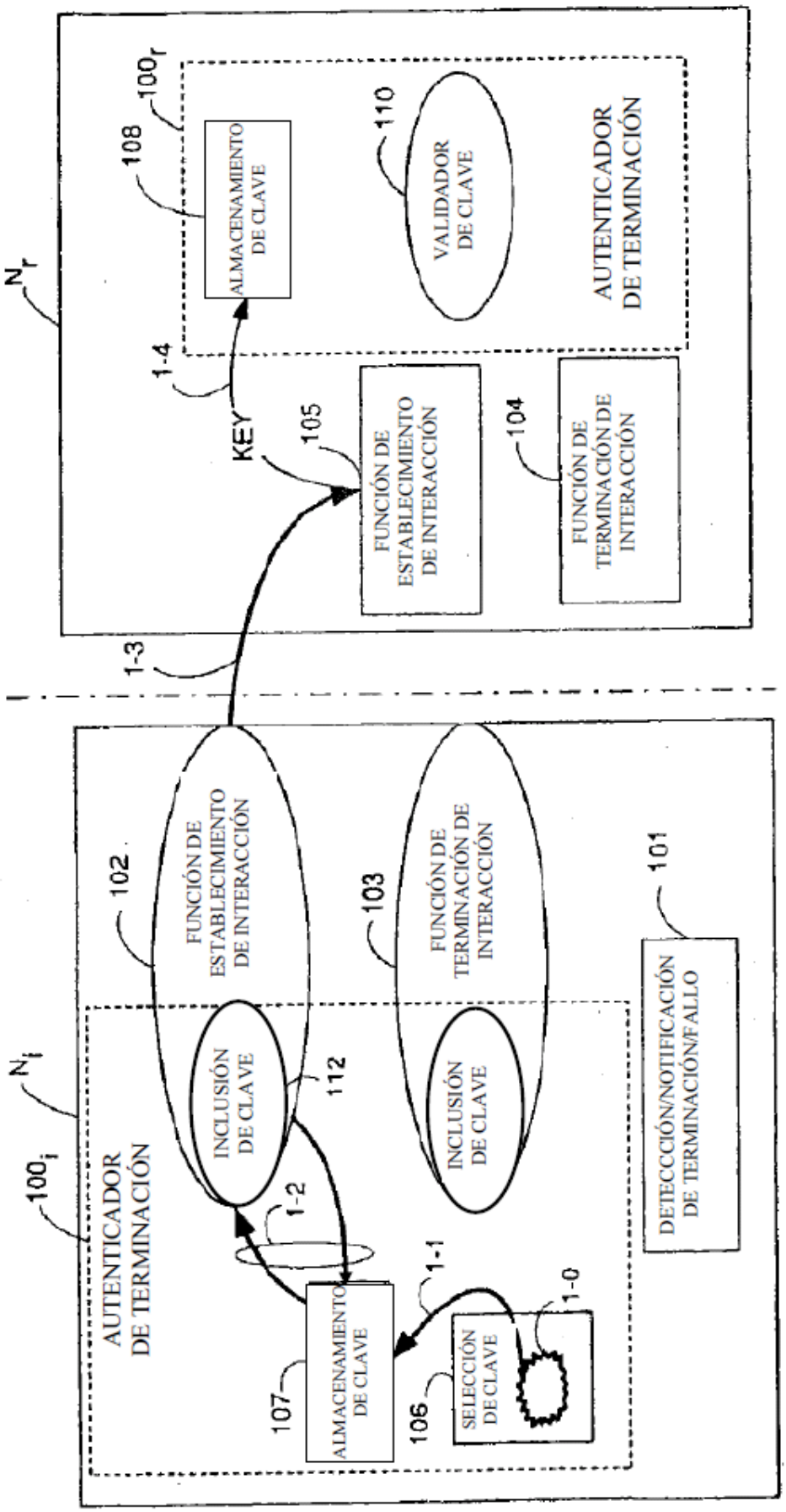

N_r
100_r
108
ALMACENAMIENTO DE CLAVE
110
VALIDADOR DE CLAVE
AUTENTICADOR DE TERMINACIÓN
1-4
KEY
105
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
104
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
1-3
N_i
100_i
AUTENTICADOR DE TERMINACIÓN
102
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
INCLUSIÓN DE CLAVE
112
1-2
103
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
INCLUSIÓN DE CLAVE
101
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
1-1
1-0
107
ALMACENAMIENTO DE CLAVE
106
SELECCIÓN DE CLAVE

Fig. 1A

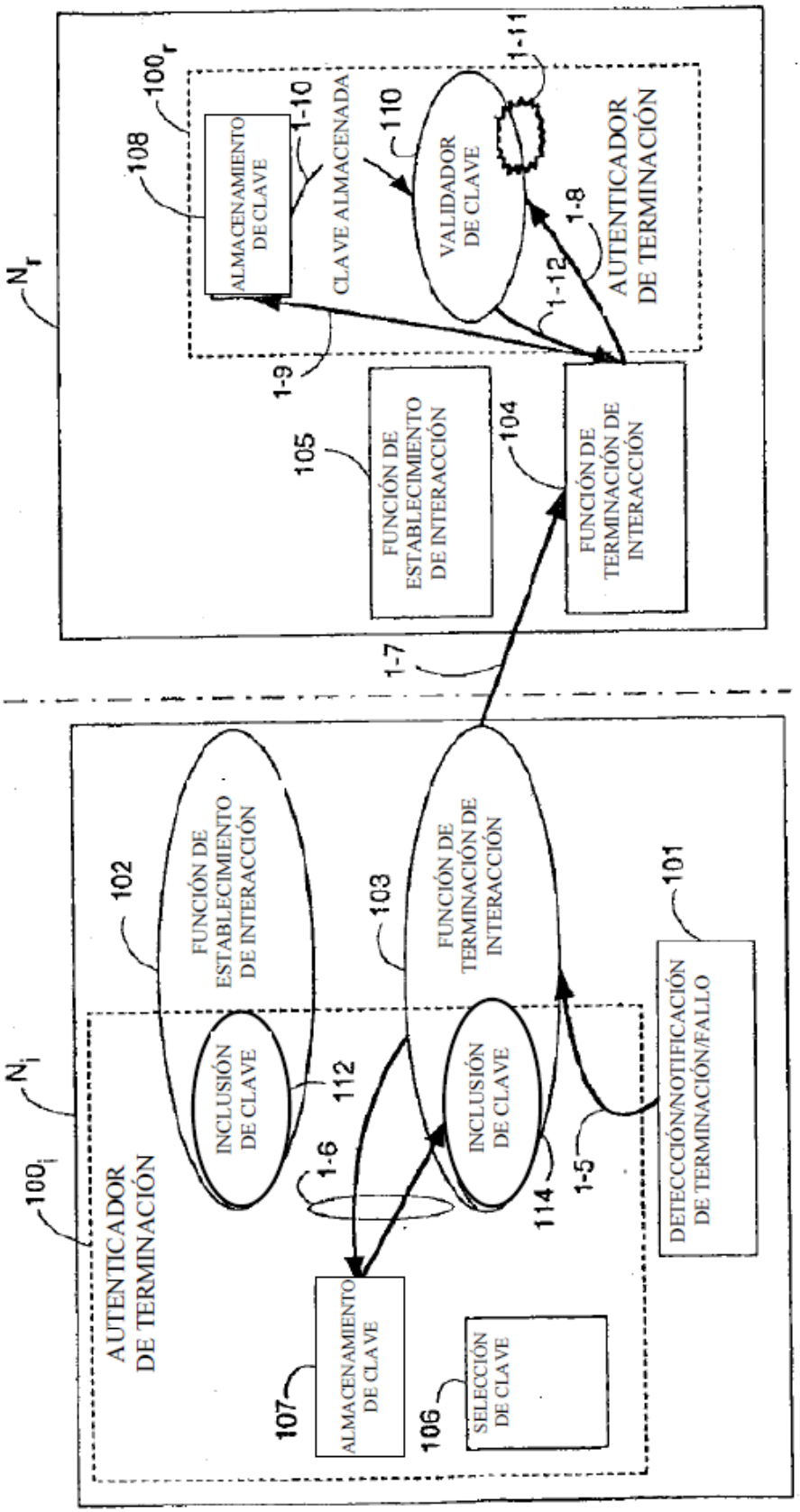

N_r
100_r
108
ALMACENAMIENTO DE CLAVE
1-10
CLAVE ALMACENADA
110
VALIDADOR DE CLAVE
1-11
1-8
1-12
AUTENTICADOR DE TERMINACIÓN
1-9
105
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
104
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
1-7
N_i
100_i
AUTENTICADOR DE TERMINACIÓN
102
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
INCLUSIÓN DE CLAVE
112
1-6
103
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
INCLUSIÓN DE CLAVE
114
1-5
101
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
107
ALMACENAMIENTO DE CLAVE
106
SELECCIÓN DE CLAVE

Fig. 1B

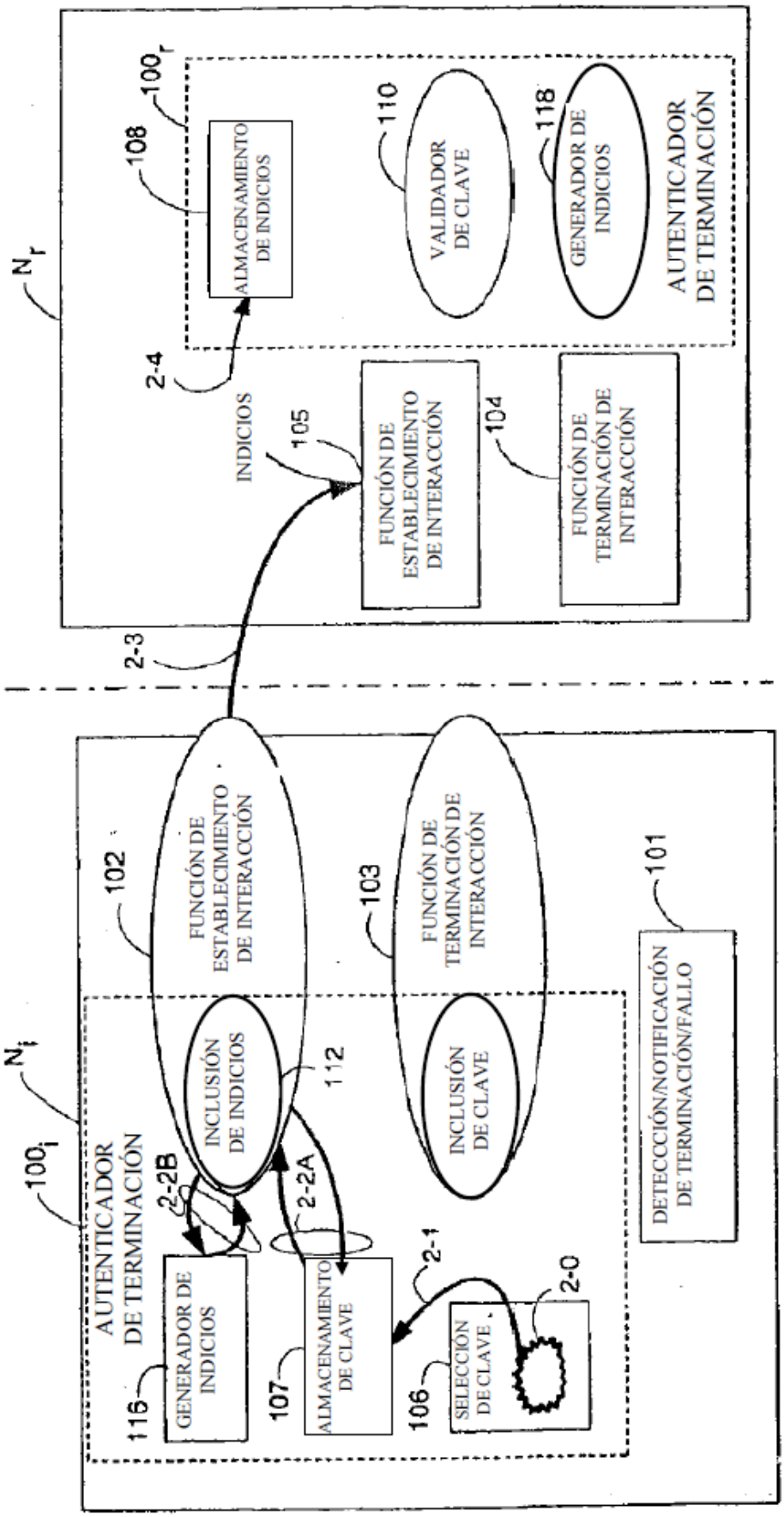

N_r
100_r
108
ALMACENAMIENTO DE INDICIOS
110
VALIDADOR DE CLAVE
118
GENERADOR DE INDICIOS
AUTENTICADOR DE TERMINACIÓN
2-4
INDICIOS
105
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
104
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
2-3
N_i
100_i
AUTENTICADOR DE TERMINACIÓN
102
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
103
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
101
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
INCLUSIÓN DE INDICIOS
112
INCLUSIÓN DE CLAVE
2-2B
2-2A
2-1
2-0
116
GENERADOR DE INDICIOS
107
ALMACENAMIENTO DE CLAVE
106
SELECCIÓN DE CLAVE

Fig. 2A

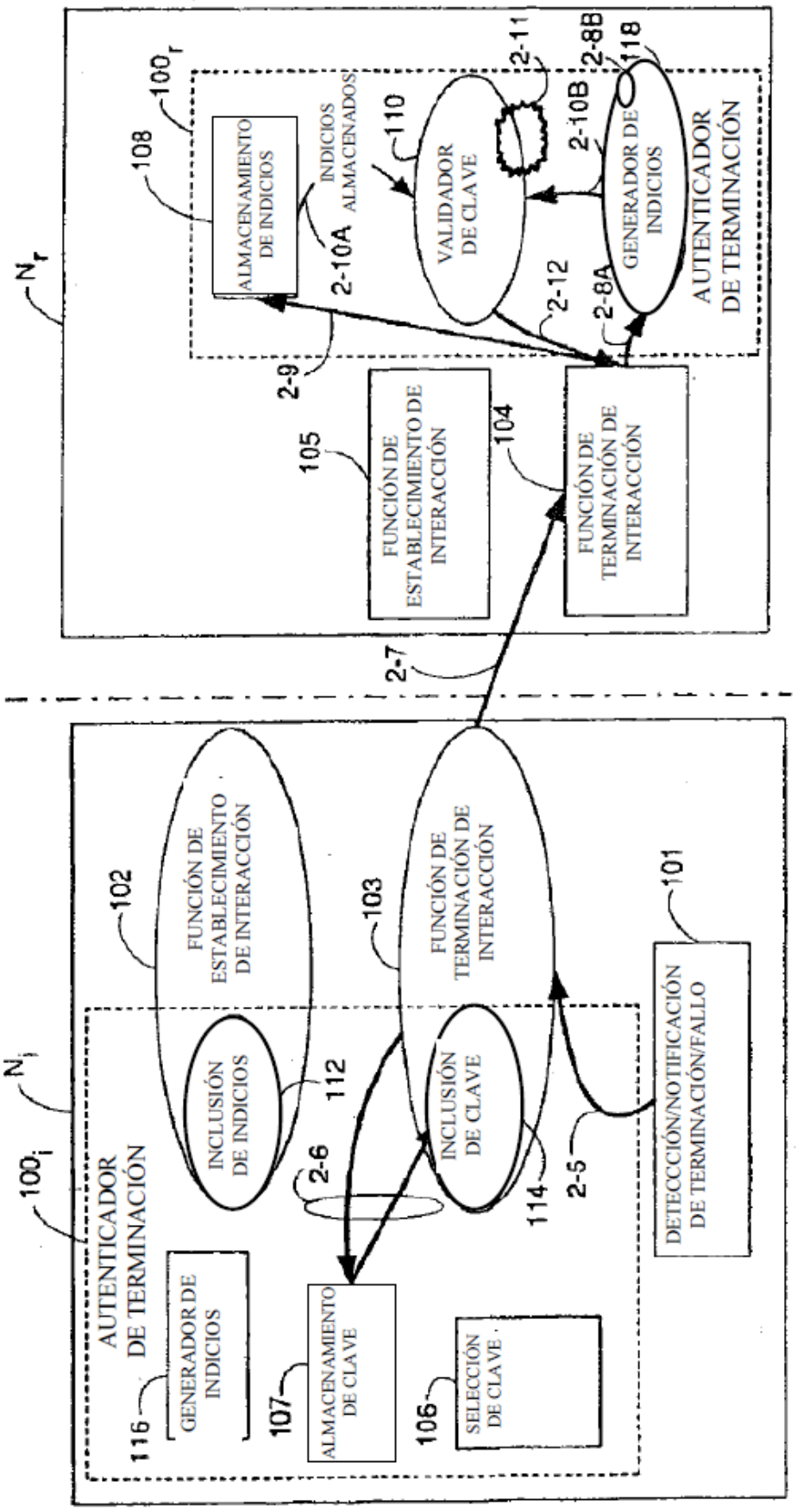
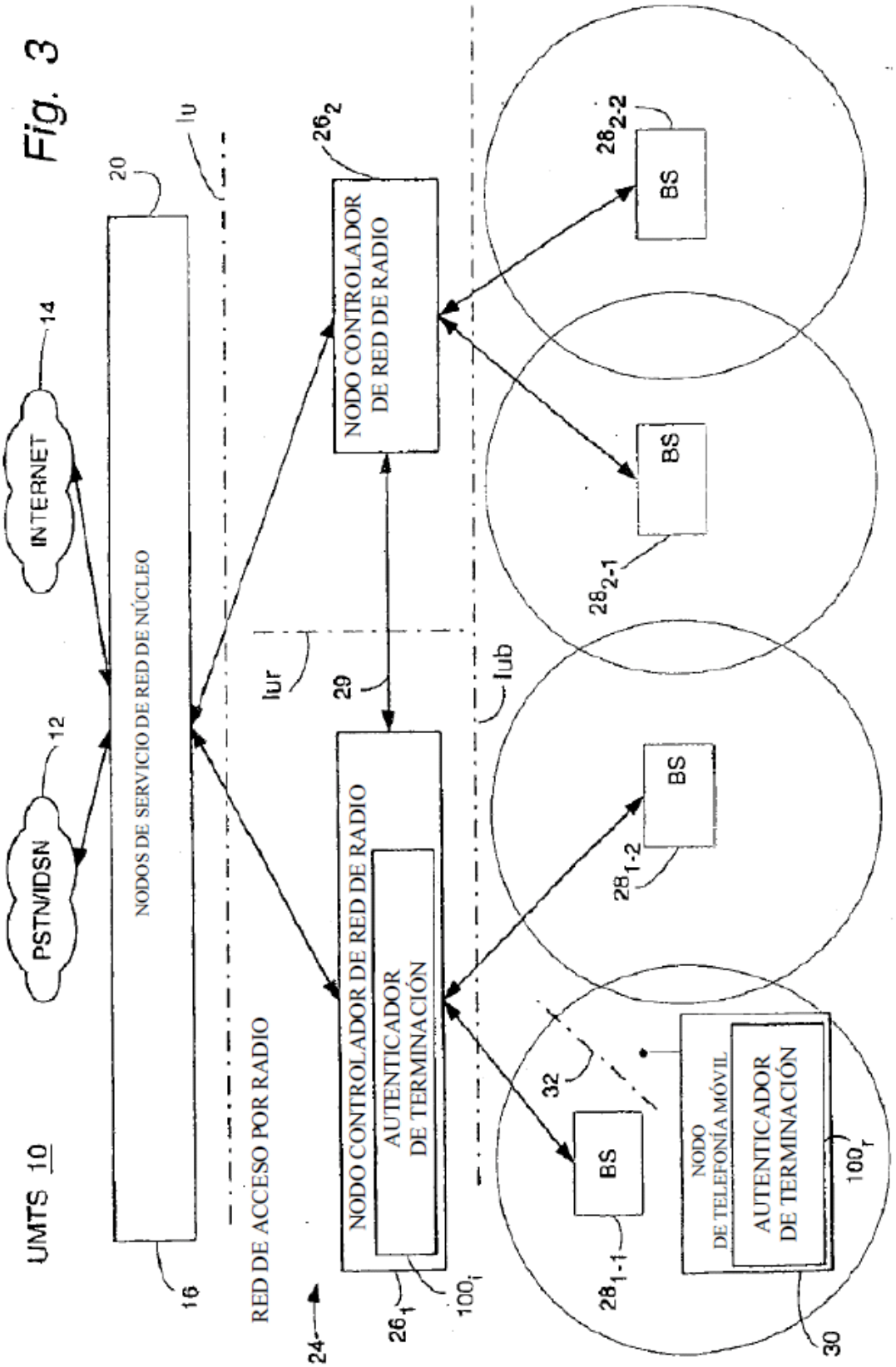

N_r
100_r
108
ALMACENAMIENTO DE INDICIOS
INDICIOS ALMACENADOS
2-10A
110
VALIDADOR DE CLAVE
2-11
2-10B
2-8B
118
GENERADOR DE INDICIOS
AUTENTICADOR DE TERMINACIÓN
2-12
2-8A
2-9
105
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
104
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
2-7
N_i
100_i
AUTENTICADOR DE TERMINACIÓN
102
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
103
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN
101
INCLUSIÓN DE INDICIOS
112
INCLUSIÓN DE CLAVE
2-6
114
2-5
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
116
GENERADOR DE INDICIOS
107
ALMACENAMIENTO DE CLAVE
106
SELECCIÓN DE CLAVE

Fig. 2B

Fig. 3


UMTS 10
INTERNET
14
PSTN/IDSN
12
NODOS DE SERVICIO DE RED DE NÚCLEO
20
16
Iu
RED DE ACCESO POR RADIO
24
NODO CONTROLADOR DE RED DE RADIO
AUTENTICADOR DE TERMINACIÓN
26_1
100_i
Iur
29
Iub
26_2
NODO CONTROLADOR DE RED DE RADIO
BS
28_{1-1}
BS
28_{1-2}
BS
28_{2-1}
BS
28_{2-2}
32
NODO DE TELEFONÍA MÓVIL
AUTENTICADOR DE TERMINACIÓN
100_r
30

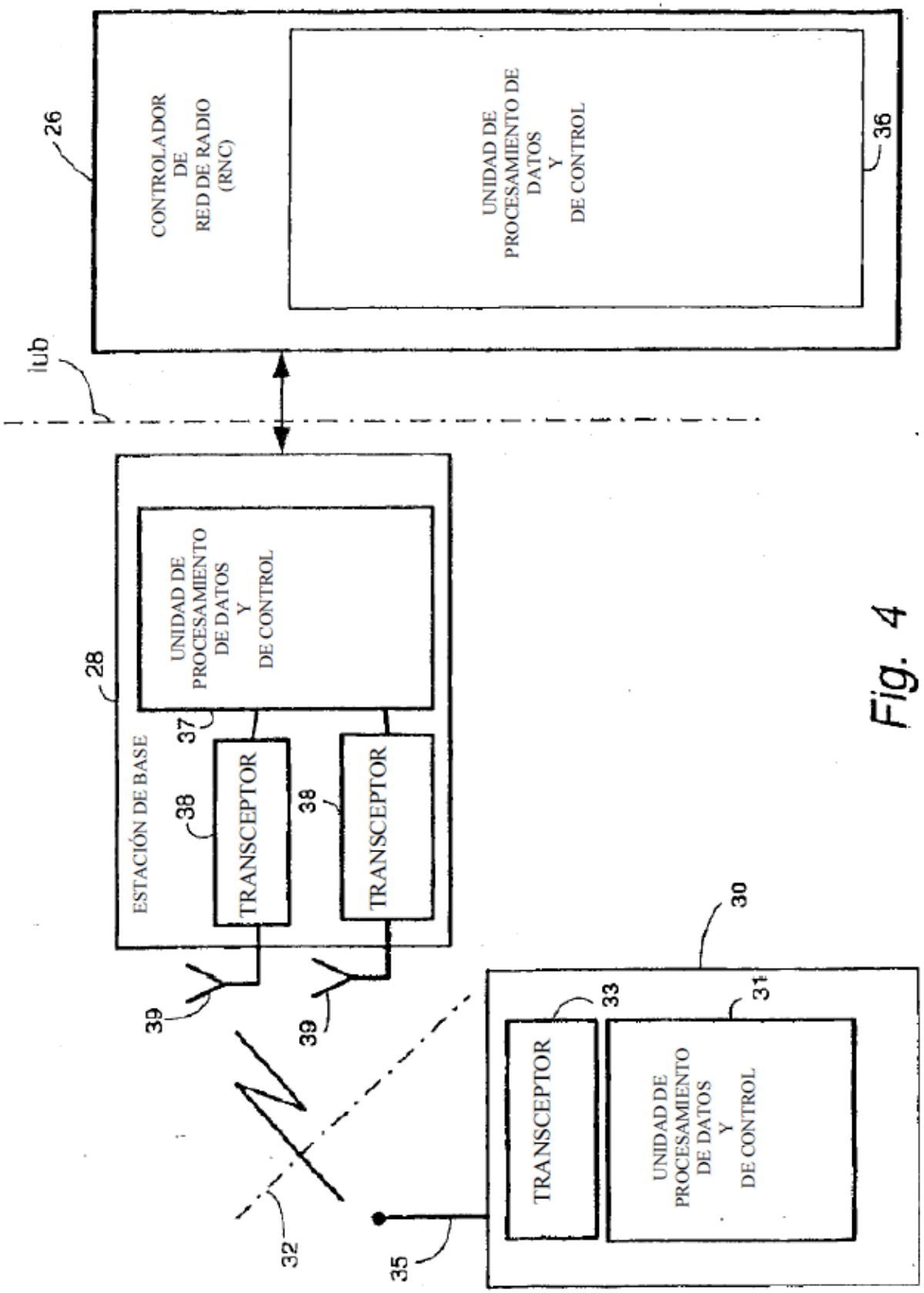

26
CONTROLADOR DE RED DE RADIO (RNC)
UNIDAD DE PROCESAMIENTO DE DATOS Y DE CONTROL
36
Iub
28
ESTACIÓN DE BASE
UNIDAD DE PROCESAMIENTO DE DATOS Y DE CONTROL
37
38
TRANSCEPTOR
38
TRANSCEPTOR
39
39
30
33
TRANSCEPTOR
31
UNIDAD DE PROCESAMIENTO DE DATOS Y DE CONTROL
32
35

Fig. 4

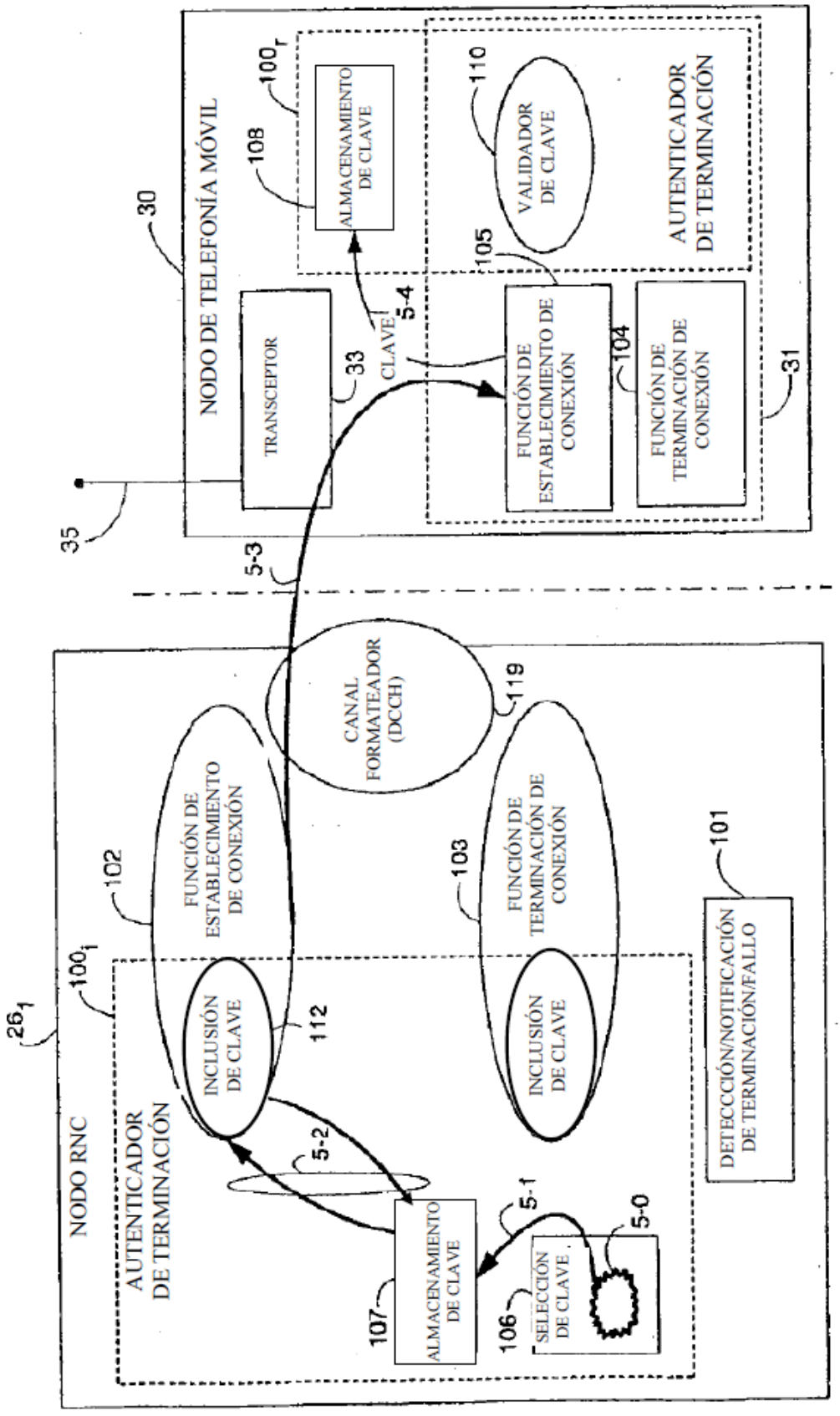

NODO DE TELEFONÍA MÓVIL
30
TRANSCEPTOR
33
35
ALMACENAMIENTO DE CLAVE
108
100r
VALIDADOR DE CLAVE
110
AUTENTICADOR DE TERMINACIÓN
105
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
104
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
31
CLAVE
5-4
5-3
NODO RNC
261
AUTENTICADOR DE TERMINACIÓN
100i
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
102
CANAL FORMATEADOR (DCCH)
119
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
103
INCLUSIÓN DE CLAVE
112
INCLUSIÓN DE CLAVE
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
101
5-2
5-1
5-0
ALMACENAMIENTO DE CLAVE
107
SELECCIÓN DE CLAVE
106

Fig. 5A

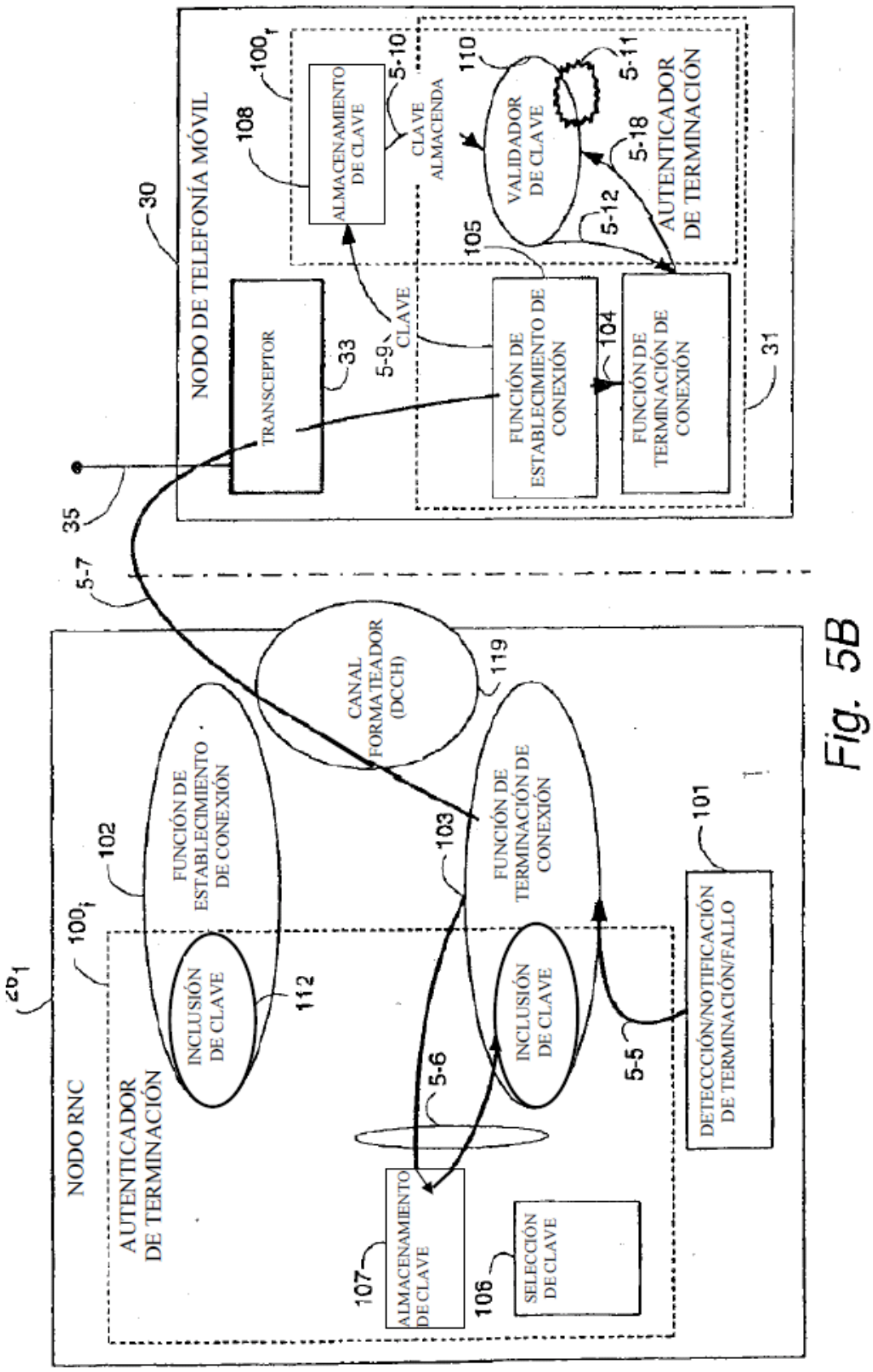

NODO DE TELEFONÍA MÓVIL
30
TRANSCEPTOR
33
ALMACENAMIENTO DE CLAVE
108
CLAVE ALMACENDA
5-10
VALIDADOR DE CLAVE
110
5-11
5-18
5-12
AUTENTICADOR DE TERMINACIÓN
105
CLAVE
5-9
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
104
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
31
35
5-7
NODO RNC
AUTENTICADOR DE TERMINACIÓN
INCLUSIÓN DE CLAVE
112
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
102
CANAL FORMATEADOR (DCCH)
119
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
103
INCLUSIÓN DE CLAVE
5-6
5-5
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
101
ALMACENAMIENTO DE CLAVE
107
SELECCIÓN DE CLAVE
106

Fig. 5B

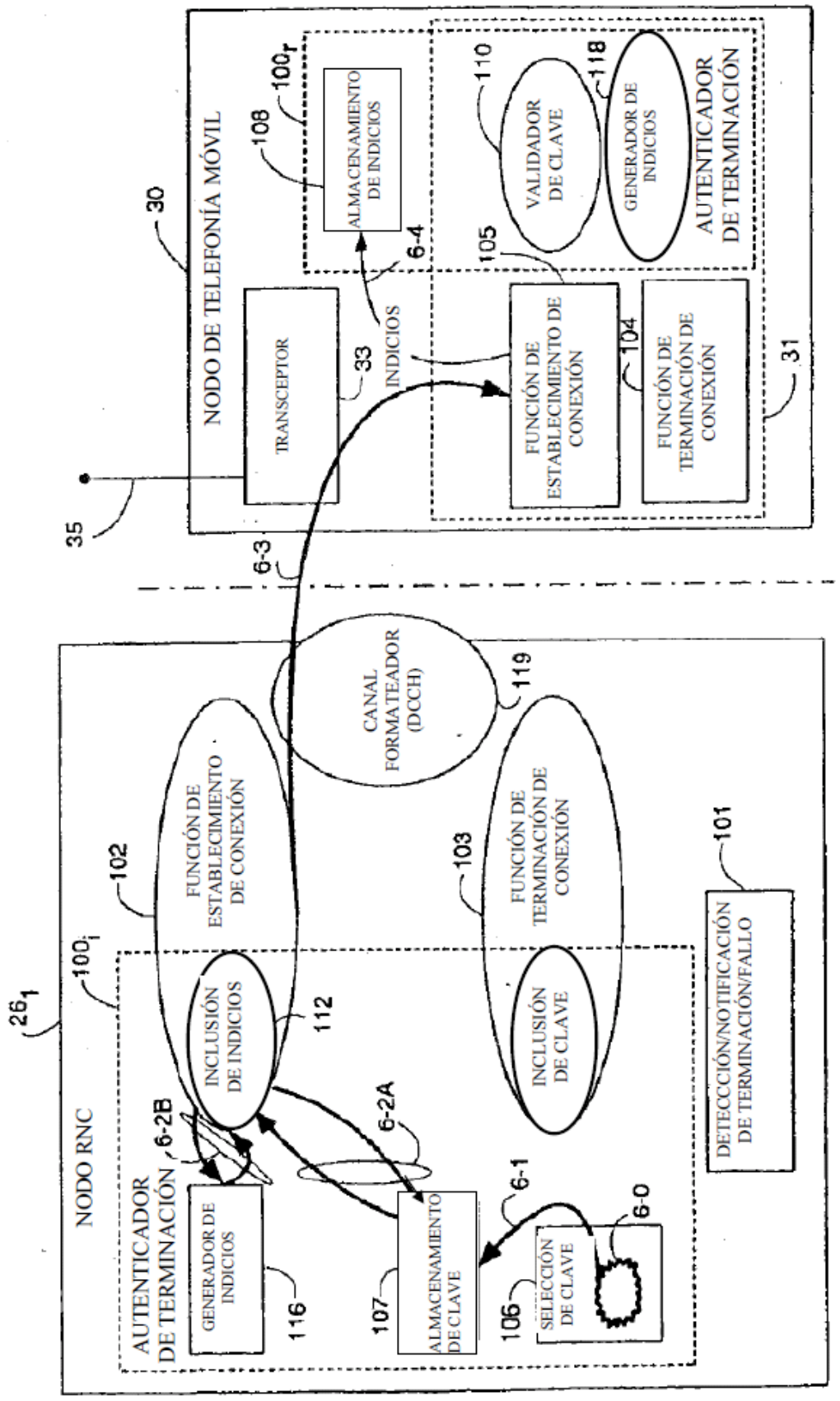

NODO DE TELEFONÍA MÓVIL
30
TRANSCEPTOR
33
ALMACENAMIENTO DE INDICIOS
108
100r
6-4
INDICIOS
AUTENTICADOR DE TERMINACIÓN
VALIDADOR DE CLAVE
110
GENERADOR DE INDICIOS
118
105
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
104
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
31
35
6-3
NODO RNC
261
100i
AUTENTICADOR DE TERMINACIÓN
GENERADOR DE INDICIOS
116
6-2B
INCLUSIÓN DE INDICIOS
112
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
102
CANAL FORMATEADOR (DCCH)
119
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
103
INCLUSIÓN DE CLAVE
6-2A
ALMACENAMIENTO DE CLAVE
107
6-1
SELECCIÓN DE CLAVE
106
6-0
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
101

Fig. 6A

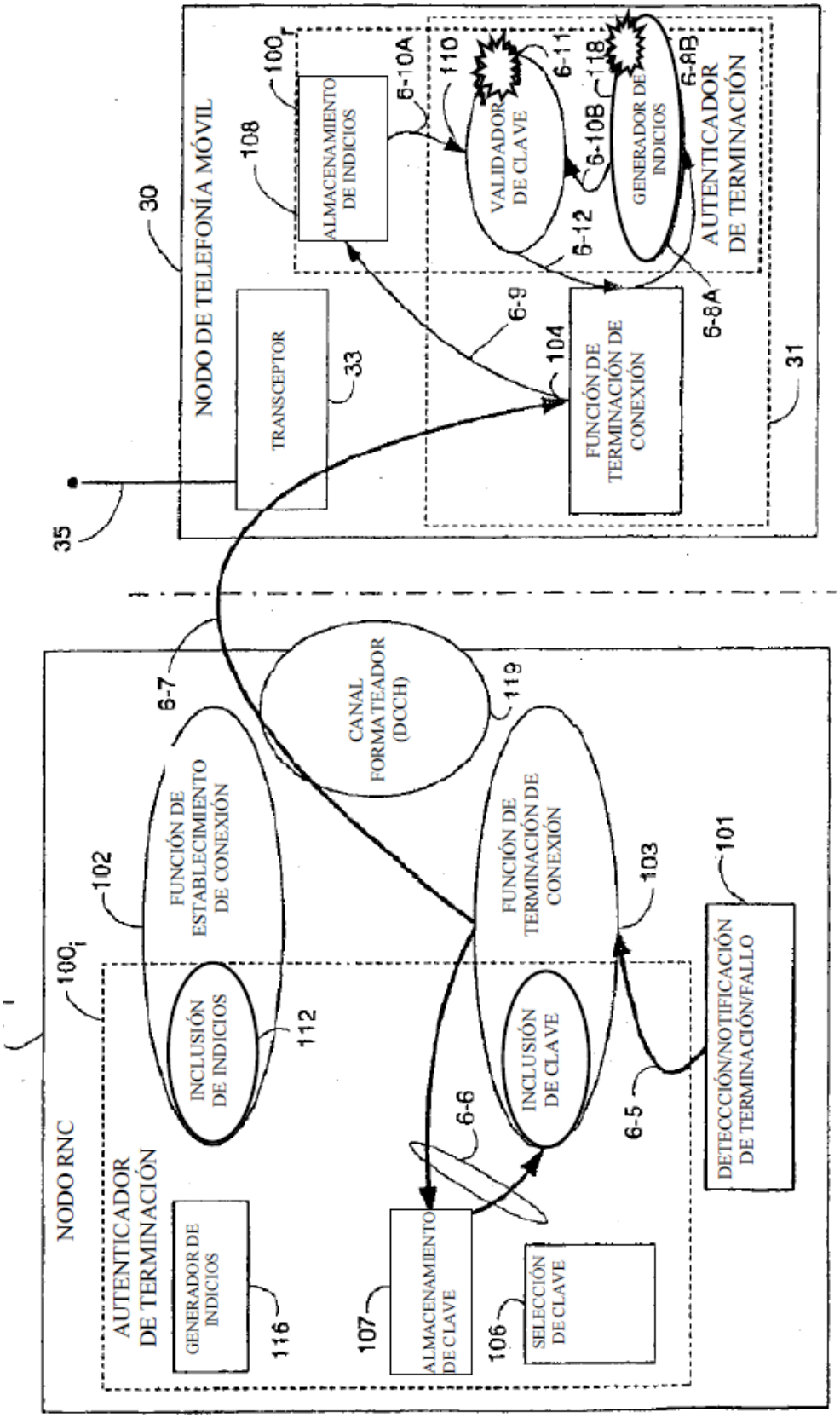
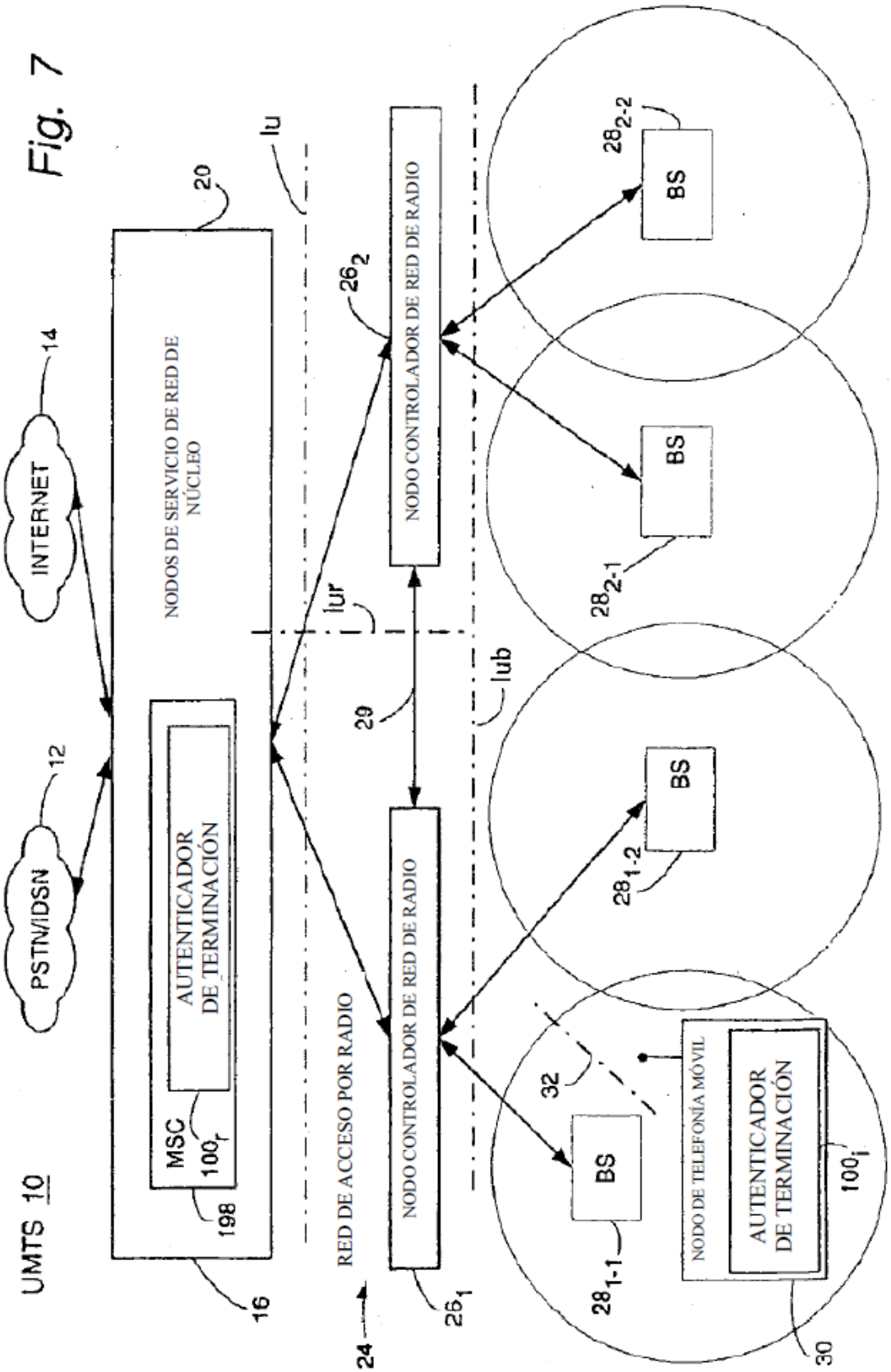

NODO DE TELEFONÍA MÓVIL
30
TRANSCEPTOR
33
35
ALMACENAMIENTO DE INDICIOS
108
100r
6-10A
110
VALIDADOR DE CLAVE
6-11
6-10B
118
GENERADOR DE INDICIOS
6-8B
AUTENTICADOR DE TERMINACIÓN
6-12
6-9
104
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
6-8A
31
6-7
CANAL FORMATEADOR (DCCH)
119
NODO RNC
100i
AUTENTICADOR DE TERMINACIÓN
102
FUNCIÓN DE ESTABLECIMIENTO DE CONEXIÓN
INCLUSIÓN DE INDICIOS
112
FUNCIÓN DE TERMINACIÓN DE CONEXIÓN
103
INCLUSIÓN DE CLAVE
6-6
6-5
101
DETECCCIÓN/NOTIFICACIÓN DE TERMINACIÓN/FALLO
GENERADOR DE INDICIOS
116
107
ALMACENAMIENTO DE CLAVE
106
SELECCIÓN DE CLAVE

Fig. 6B

Fig. 7


UMTS 10
INTERNET
14
PSTN/IDSN
12
NODOS DE SERVICIO DE RED DE NÚCLEO
20
MSC
100_r
AUTENTICADOR DE TERMINACIÓN
198
16
Iu
RED DE ACCESO POR RADIO
24
NODO CONTROLADOR DE RED DE RADIO
26_1
26_2
Iur
29
Iub
BS
28_{1-1}
28_{1-2}
28_{2-1}
28_{2-2}
32
NODO DE TELEFONÍA MÓVIL
AUTENTICADOR DE TERMINACIÓN
100_i
30

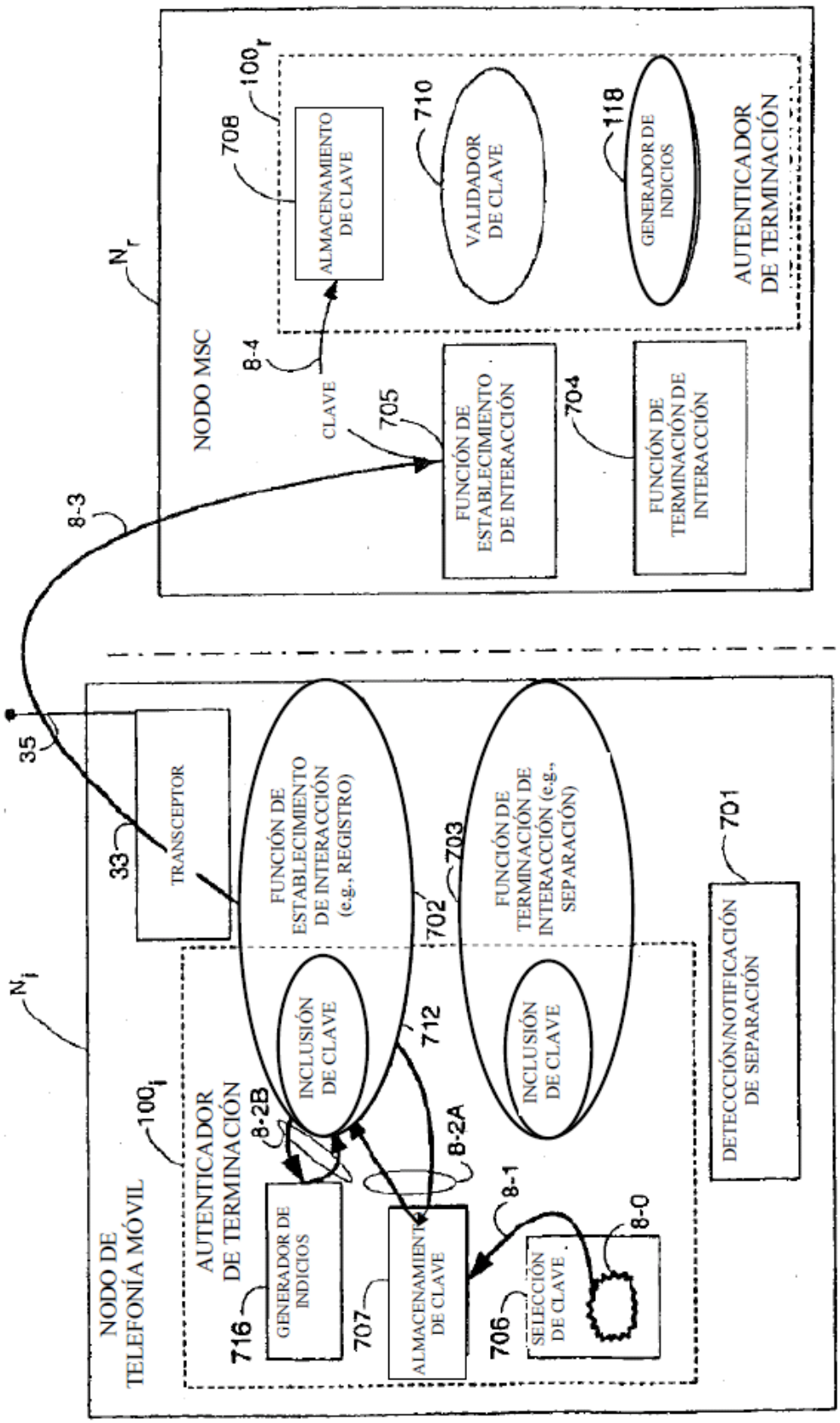

NODO DE TELEFONÍA MÓVIL
N_i
100_i
AUTENTICADOR DE TERMINACIÓN
TRANSCEPTOR
33
35
8-3
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN (e.g., REGISTRO)
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN (e.g., SEPARACIÓN)
INCLUSIÓN DE CLAVE
INCLUSIÓN DE CLAVE
712
702
703
701
DETECCCIÓN/NOTIFICACIÓN DE SEPARACIÓN
8-2B
8-2A
8-1
8-0
716
GENERADOR DE INDICIOS
707
ALMACENAMIENTO DE CLAVE
706
SELECCIÓN DE CLAVE
NODO MSC
N_r
100_r
708
ALMACENAMIENTO DE CLAVE
710
VALIDADOR DE CLAVE
118
GENERADOR DE INDICIOS
AUTENTICADOR DE TERMINACIÓN
8-4
CLAVE
705
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
704
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN

Fig. 8A

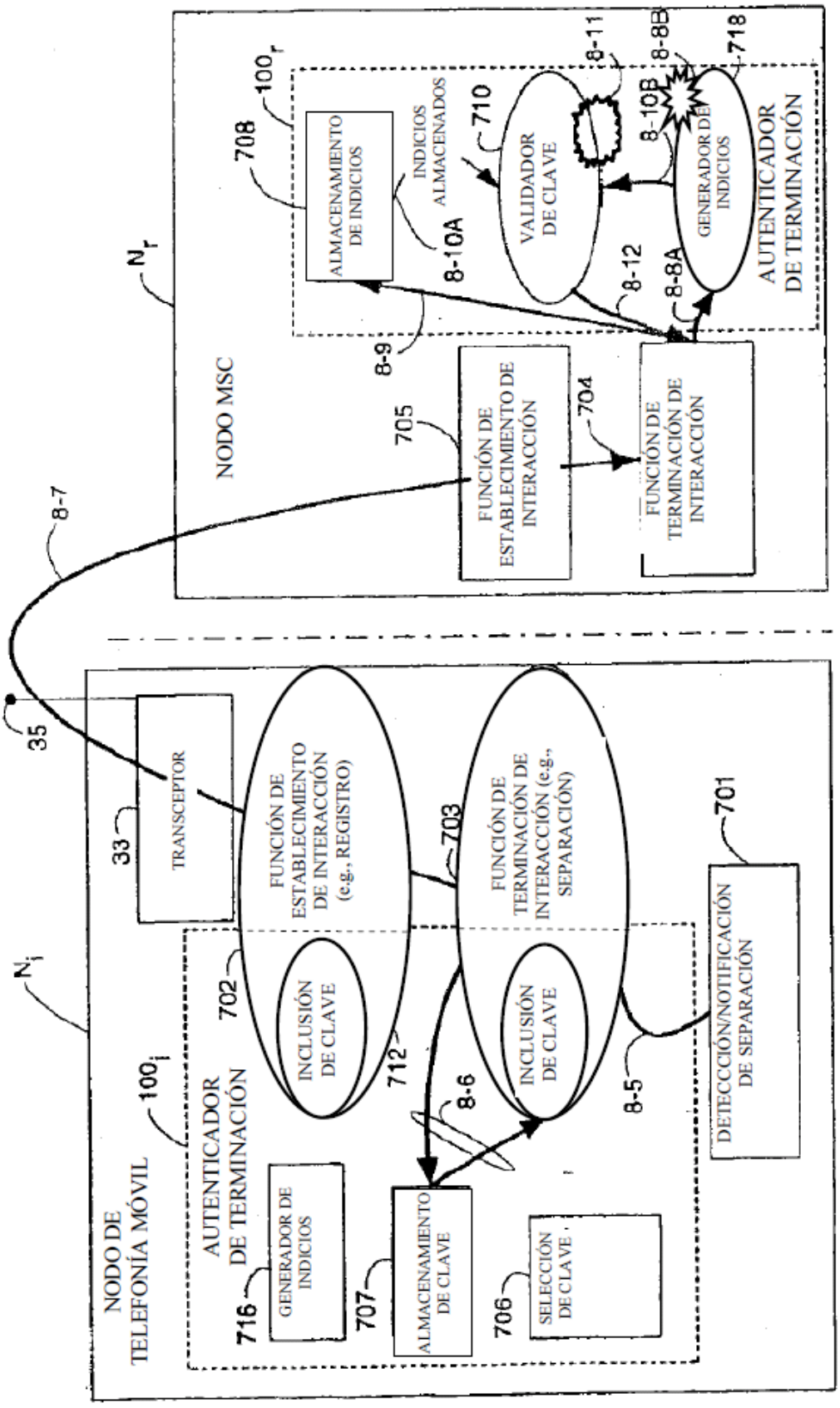

NODO DE TELEFONÍA MÓVIL
N_i
100_i
AUTENTICADOR DE TERMINACIÓN
TRANSCEPTOR
33
35
8-7
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN (e.g., REGISTRO)
INCLUSIÓN DE CLAVE
702
703
712
8-6
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN (e.g., SEPARACIÓN)
INCLUSIÓN DE CLAVE
8-5
701
DETECCCIÓN/NOTIFICACIÓN DE SEPARACIÓN
GENERADOR DE INDICIOS
716
ALMACENAMIENTO DE CLAVE
707
SELECCIÓN DE CLAVE
706
NODO MSC
N_r
100_r
708
ALMACENAMIENTO DE INDICIOS
INDICIOS ALMACENADOS
8-10A
8-9
710
VALIDADOR DE CLAVE
8-11
8-10B
8-8B
718
GENERADOR DE INDICIOS
AUTENTICADOR DE TERMINACIÓN
8-12
8-8A
705
FUNCIÓN DE ESTABLECIMIENTO DE INTERACCIÓN
704
FUNCIÓN DE TERMINACIÓN DE INTERACCIÓN

Fig. 8B

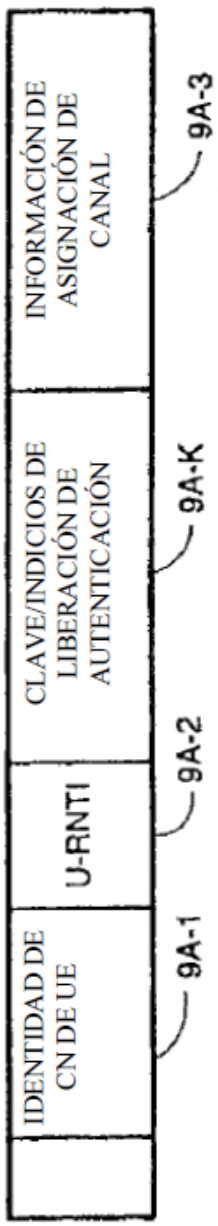


Fig. 9A

MENSAJE DE ESTABLECIMIENTO DE CONEXIÓN DEL RRC

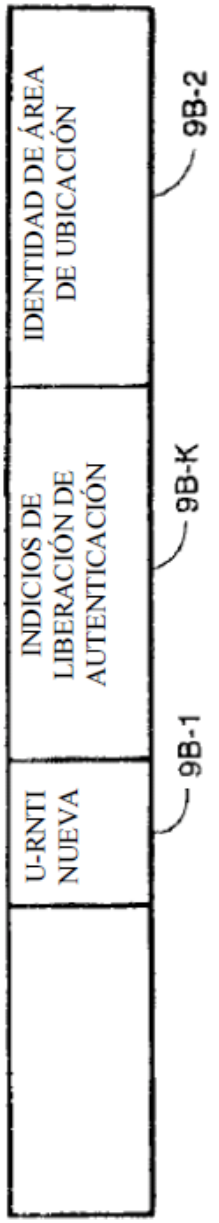


Fig. 9B

MENSAJE DE INFORMACIÓN DE MOVILIDAD EN UTRAN

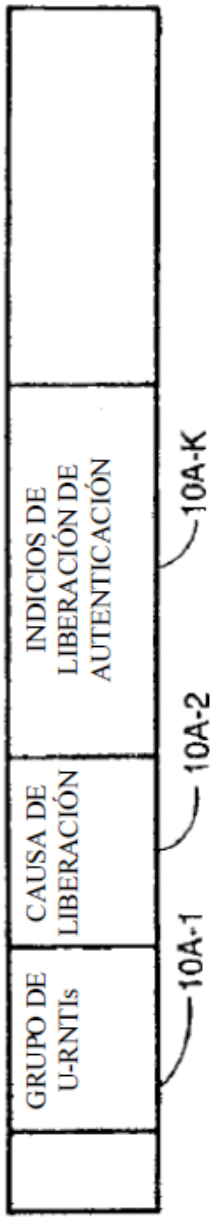


Fig. 10A

MENSAJE DE LIBERACIÓN DE CONEXIÓN DEL RRC (EN EL CCCH PARA GRUPO DE UES)

Fig. 10B

MENSAJE DE LIBERACIÓN DE CONEXIÓN DEL RRC (EN EL CCCH PARA UN SOLO UE)

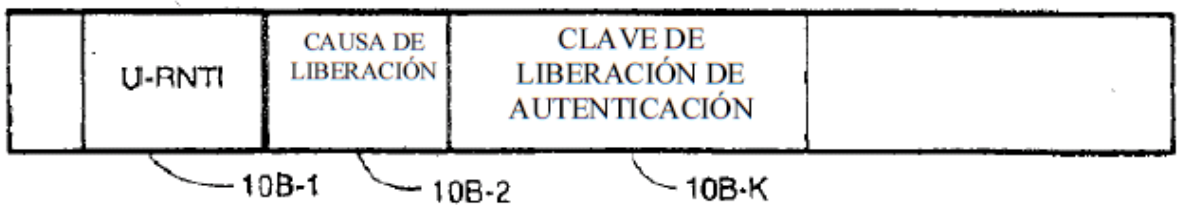


Fig. 10C

MENSAJE DE LIBERACIÓN DE CONEXIÓN DEL RRC (EN EL DCCH PARA UN SOLO UE)

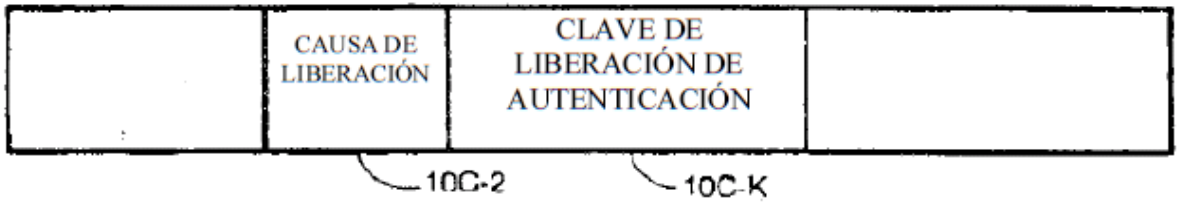


Fig. 10D

MENSAJE DE LIBERACIÓN DE TIPO 1 DE LOCALIZACIÓN (PARA LIBERAR UN SOLO UE)

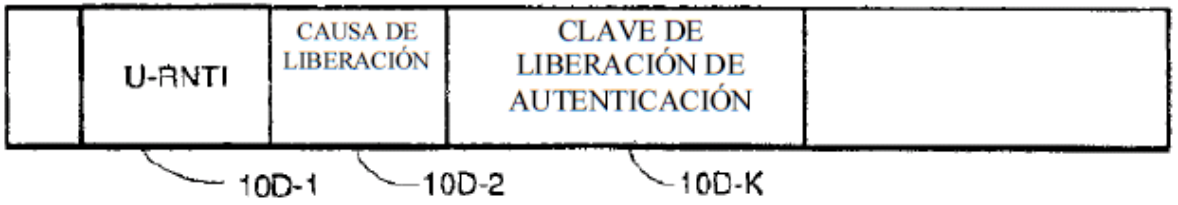
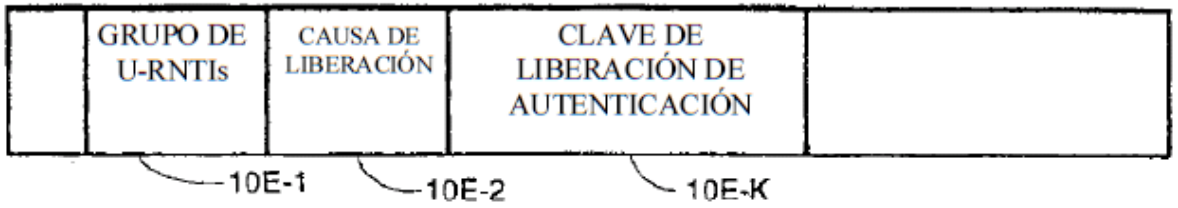


Fig. 10E

MENSAJE DE LIBERACIÓN DE TIPO 1 DE LOCALIZACIÓN (PARA LIBERAR UN GRUPO DE UES)



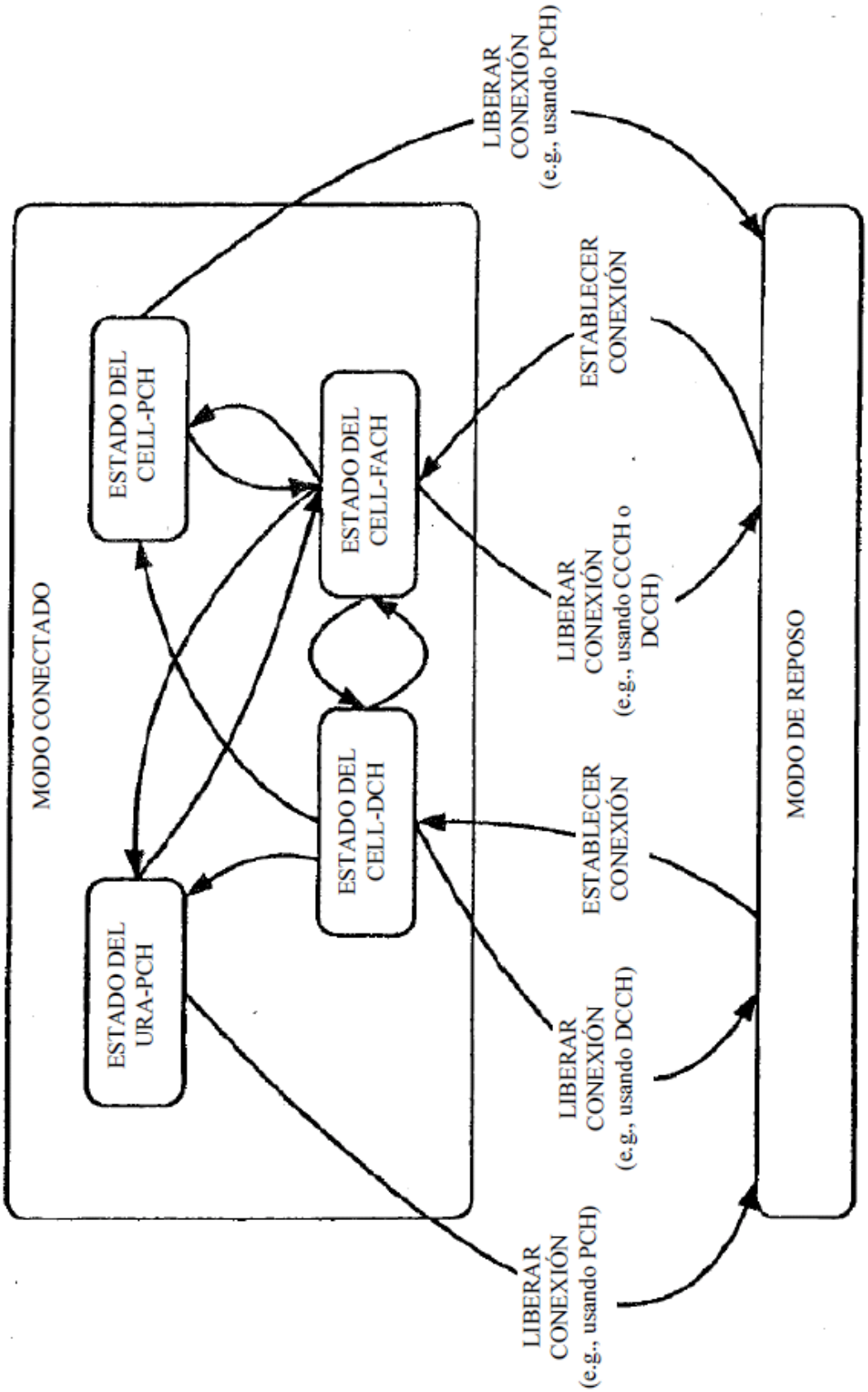

MODO CONECTADO
ESTADO DEL CELL-PCH
ESTADO DEL CELL-FACH
ESTADO DEL CELL-DCH
ESTADO DEL URA-PCH
LIBERAR CONEXIÓN (e.g., usando PCH)
ESTABLECER CONEXIÓN
LIBERAR CONEXIÓN (e.g., usando CCCH o DCCH)
ESTABLECER CONEXIÓN
LIBERAR CONEXIÓN (e.g., usando DCCH)
LIBERAR CONEXIÓN (e.g., usando PCH)
MODO DE REPOSO

Fig. 11

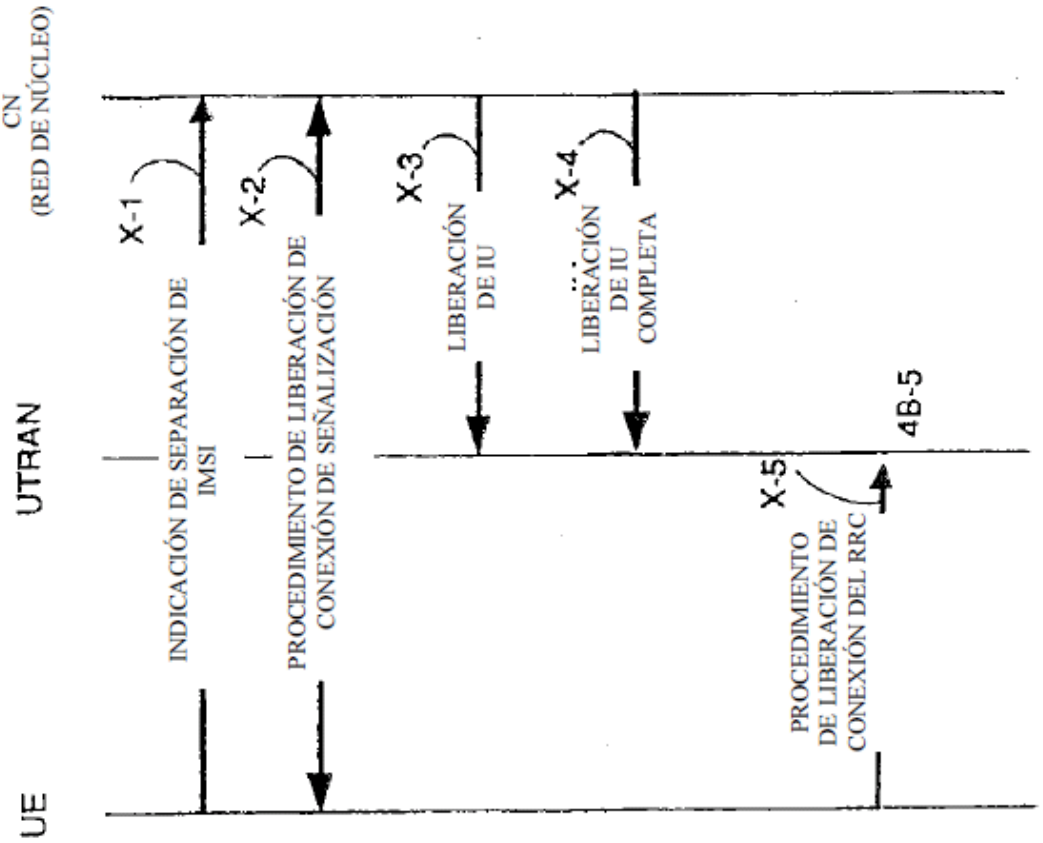

UE
UTRAN
CN
(RED DE NÚCLEO)
X-1
INDICACIÓN DE SEPARACIÓN DE IMSI
X-2
PROCEDIMIENTO DE LIBERACIÓN DE CONEXIÓN DE SEÑALIZACIÓN
X-3
LIBERACIÓN DE IU
X-4
LIBERACIÓN DE IU COMPLETA
4B-5
X-5
PROCEDIMIENTO DE LIBERACIÓN DE CONEXIÓN DEL RRC

Fig. 13

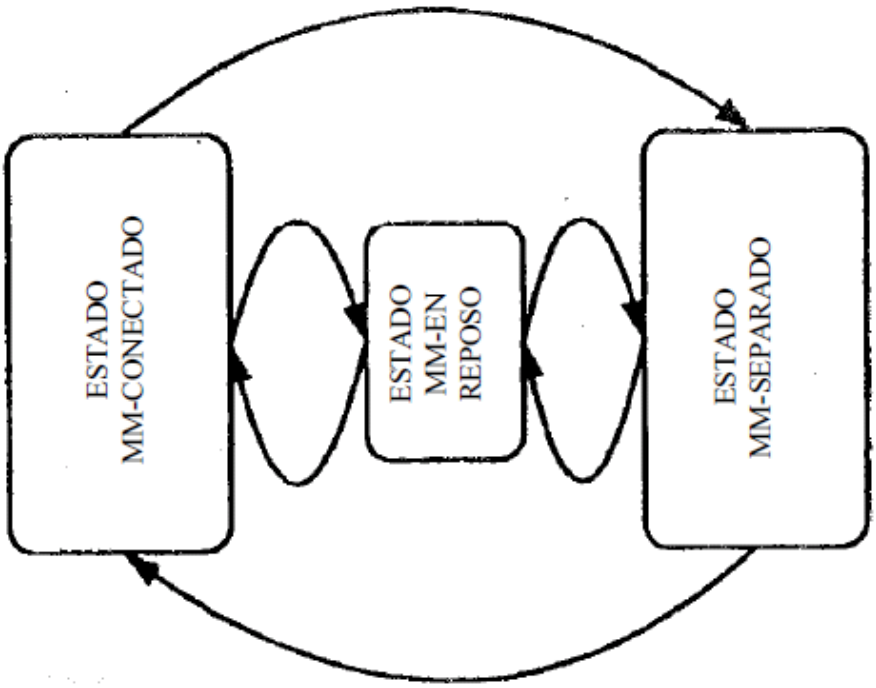

ESTADO MM-CONECTADO
ESTADO MM-EN REPOSO
ESTADO MM-SEPARADO

Fig. 12