(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 793 491**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 8/26 (2009.01)
H04W 12/00 (2009.01)
H04L 12/24 (2006.01)
H04W 4/50 (2008.01)
H04W 8/20 (2009.01)
H04W 4/00 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.07.2012 PCT/KR2012/005431**

(87) Fecha y número de publicación internacional: **17.01.2013 WO13009059**

(96) Fecha de presentación y número de la solicitud europea: **09.07.2012 E 12812078 (9)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 2731382**

(54) Título: **Procedimiento para configurar un terminal en un sistema de comunicación móvil**

(30) Prioridad:

08.07.2011 KR 20110067828

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.11.2020

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu
Suwon-si, Gyeonggi-do 443-742, KR

(72) Inventor/es:

SUH, KYUNG JOO;
BAEK, YOUNG KYO y
JEONG, SANG SOO

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Procedimiento para configurar un terminal en un sistema de comunicación móvil

Campo técnico

La presente invención se refiere a un procedimiento y a un aparato para configurar un terminal en un sistema de comunicación móvil. En particular, la presente invención se refiere a un procedimiento y a un aparato para configurar un terminal transmitiendo la información para su uso en el acceso a la red del terminal de manera eficiente.

Antecedentes de la técnica

El Proyecto de Asociación de 3a Generación (3GPP) es una de las organizaciones representativas de estandarización de tecnología de comunicación móvil. El 3GPP ha definido el Sistema de Paquetes Evolucionado (EPS) para la comunicación de la próxima generación. El 3GPP también ha introducido la entidad de gestión de movilidad (MME) como una entidad de movilidad de red.

Recientemente, los protocolos utilizados en el sistema 3G del 3GPP han sido mejorados por los investigadores en el campo. Los investigadores han propuesto esquemas de mejora para proporcionar un servicio de comunicación de alta velocidad en el sistema de comunicación móvil de próxima generación. En el procedimiento de comunicación convencional, los procedimientos de autenticación y seguridad se han realizado en la capa de acceso de radio. Los investigadores se están centrando en el esquema de gestión de seguridad reforzado con la introducción del concepto de protocolo de seguridad en la capa NAS además de dichos procedimientos de convención.

Sin embargo, en la arquitectura de sistema convencional, el terminal tiene que seleccionar un operador como proveedor de servicios. El terminal almacena la seguridad y otras informaciones asociadas con el operador correspondiente para conectarse al operador. En cualquier caso, el terminal correspondiente puede intentar recibir el servicio de otro operador. Para este fin, el terminal correspondiente debe usar el módulo de identidad de suscriptor universal (USIM) o la tarjeta de circuito integrado universal (UICC) correspondiente al operador. Es decir, dado que el módulo de identidad del suscriptor es específico del operador, no es fácil para el usuario cambiar entre operadores.

Por lo tanto, existe la necesidad de un procedimiento y un aparato para almacenar información para su uso en el acceso a la operación en el módulo de identidad del suscriptor. De esta manera, el usuario es capaz de configurar el operador en el uso inicial del terminal y cambiar entre operadores de manera eficiente.

El documento de la técnica anterior US2011136471A1 desvela que en un procedimiento de activación de una SIM o USIM de un dispositivo CDMA, el servidor UICC responde a un mensaje de solicitud de activación que incluye IMSI e IMEI con un mensaje de respuesta de activación que incluye MSISDN, MIN, CDMA A12 NAI, la PRL, el identificador PLMN y/o el acceso a la red CDMA NAI.

El documento de la técnica anterior WO2010090569A1 desvela un procedimiento para arranque seguro. El arranque seguro es un procedimiento de aprovisionamiento de una gestión de dispositivos, DM, cliente de un dispositivo móvil o inalámbrico, para mover el dispositivo de un estado vacío no aprovisionado a un estado en el que puede iniciar una sesión de administración a un servidor de DM y luego, por ejemplo, nuevos servidores de DM. El UE solo envía su IMSI, IMEI o número de serie electrónico y recibe información que puede conducir a la generación de la clave de seguridad.

Divulgación de la invención

Problema técnico

La presente invención ha sido concebida para resolver el problema anterior y tiene como objetivo proporcionar un procedimiento y un aparato de transmisión de información de dispositivo que sea capaz de configurar un operador en el uso inicial del terminal y cambiar entre operadores de manera eficiente.

Solución al problema

La invención se expone en el juego de reivindicaciones adjunto.

Se puede proporcionar un procedimiento para configurar un terminal de comunicación móvil que incluye transmitir, en el terminal de comunicación móvil, un mensaje de solicitud de provisión de información a una entidad de provisión de información y recibir, en el terminal de comunicación móvil, información para su uso en conexión del terminal de comunicación móvil desde la entidad de provisión de información.

Se puede proporcionar un procedimiento para configurar un terminal de comunicación móvil que incluye recibir, en una entidad de provisión de información, un mensaje de solicitud de información desde el terminal de comunicación móvil, generar, en la entidad de provisión de información, información para su uso en conexión del terminal de comunicación móvil, y transmitir, en la entidad de provisión de información, la información para su uso en conexión con el terminal de comunicación móvil.

Efectos ventajosos de la invención

El procedimiento y el aparato de acuerdo con una realización de la presente invención son ventajosos porque el usuario es capaz de configurar una operación en el uso inicial del terminal y cambiar entre operadores de manera eficiente.

Breve descripción de los dibujos

La figura 1 es un diagrama de flujo que ilustra un procedimiento de provisión de información de acuerdo con una realización de la presente invención.
La figura 2 es un diagrama que ilustra una arquitectura de red de acuerdo con una realización de la presente invención.
Las figuras 3 a 12b son diagramas de flujo que ilustran procedimientos de provisión de información de acuerdo con realizaciones de la presente invención.

Modo para la invención

Las realizaciones ejemplares de la presente invención se describen con referencia a los dibujos adjuntos en detalle.

Ventajas y características de la presente invención y procedimientos para lograr la misma pueden entenderse más fácilmente haciendo referencia a la siguiente descripción detallada de realizaciones ejemplares y los dibujos adjuntos. Sin embargo, la presente invención puede realizarse en muchas formas diferentes y no debe interpretarse como que está limitada a las realizaciones de ejemplo expuestas en el presente documento. Por el contrario, estas realizaciones ejemplares son proporcionados de modo que la presente divulgación sea exhaustiva y completa y para transmitir completamente el concepto de la invención a los expertos en la técnica, y la presente invención solamente se definirá mediante las reivindicaciones adjuntas. Números de referencia similares se refieren a elementos similares en toda la memoria descriptiva.

El procedimiento y aparato de transmisión de información de dispositivo de acuerdo con las realizaciones de la presente invención se describen a continuación con referencia a los dibujos adjuntos.

En la siguiente descripción, el terminal realiza la comunicación utilizando un protocolo NAS entre el terminal y MME y otros protocolos en un sistema de comunicación móvil. En este caso, la presente invención puede incluir la provisión de información inicial para que el terminal realice la comunicación en la red del operador correspondiente, proporcionando al terminal información del terminal y gestionando el identificador proporcionado. Aquí, la información del terminal incluye una clave de seguridad, un parámetro y un identificador para su uso en la comunicación. En lo sucesivo, la presente invención se describe con los ejemplos de sistema EPS, UTRAN y GERAN basados en 3GPP. Sin embargo, la presente invención es aplicable a otros sistemas de comunicación móvil. La presente invención se puede aplicar al procedimiento de aprovisionamiento inicial de la información inicial para su uso en el acceso a un determinado sistema de operador o al procedimiento de almacenamiento, cuando el terminal cambia el operador, la información relacionada con el mismo para acceder al operador conmutado.

Como se muestra en la figura 2, la realización de la figura 2 es uno de los objetos de la presente invención. Para lograr el objeto, el sistema de comunicación móvil proporciona al terminal parámetros de seguridad e identificador en el entorno EUTRAN. En el caso de que el terminal realice la autenticación y cuando el terminal se comunica con una entidad de red tal como MME, la seguridad puede estar soportada. Tal procedimiento es aplicable a otros sistemas de comunicación que tienen una formación técnica y un formato de canal y arquitectura de red similares. Tal procedimiento es aplicable a otro sistema de comunicación móvil que funciona con protocolos similares o con un protocolo diferente, pero que funciona de manera similar sin apartarse del ámbito de la presente invención. Esto es obvio para los expertos en la materia.

Una realización de la presente invención se puede aplicar al caso de soportar el protocolo NAS y otros protocolos de seguridad en el sistema de comunicación móvil evolucionado, tal como 3GPP EPS. En el procedimiento que el terminal se comunica con la red, el terminal configura la información del suscriptor apropiada para el operador específico y la clave de seguridad relacionada. Posteriormente, el terminal es capaz de realizar una comunicación segura con la red de manera eficiente utilizando la clave de seguridad. Según una realización de la presente invención, el terminal es capaz de seleccionar un operador que proporcione la clave de seguridad o la información necesaria al menos para su uso en el establecimiento de la comunicación. De acuerdo con una realización de la presente invención, el terminal puede configurar la información necesaria para su uso en la comunicación. La comunicación móvil puede soportar autenticación. El sistema de comunicación móvil también puede gestionar la seguridad entre el terminal y una entidad tal como MME y mantener la comunicación entre los mismos. La presente invención es aplicable a las tecnologías de acceso por radio anteriores a 3GPP, tales como UTRAN, GERAN y otras redes de acceso por radio, así como a 3GPP EPS y UTRAN.

Existe un problema al configurar la información del suscriptor y los parámetros de seguridad en una red de comunicación móvil. Según la presente invención, dicho problema puede resolverse y gestionarse utilizando el protocolo de estrato sin acceso (NAS) y los protocolos entre otras entidades de red.

De acuerdo con una realización de la presente invención, el terminal puede establecer los parámetros para seleccionar

un operador y seleccionar la información de seguridad. Es decir, el terminal puede establecer la información del suscriptor y realizar procedimientos de seguridad dinámicamente. A través de esto, el terminal puede realizar comunicaciones en el entorno de seguridad. Una realización de la presente invención se puede aplicar a la red de acceso de radio terrestre universal evolucionada (EUTRAN) y a la red de acceso de radio terrestre universal (UTRAN)/GSM/red de acceso de radio EDGE (GERAN).

La figura 1 es un diagrama de flujo que ilustra un procedimiento de provisión de información de acuerdo con una realización de la presente invención.

Con referencia a la figura 1, el terminal 10 recibe una solicitud de provisión de información ingresada por el usuario en la etapa 20. La entrada de solicitud de provisión de información es la entrada que recomienda solicitar a la red de comunicación móvil que proporcione la clave de acceso a la red de comunicación móvil y otra información de terminal de UE tal como un identificador. Tal entrada se describe con las realizaciones de las figuras 3 a 12b.

El terminal 10 transmite la solicitud de provisión de información en la etapa 22. El procedimiento de solicitud de provisión de información es el procedimiento en el que el terminal solicita la clave de seguridad y el identificador para su uso en la red de comunicación. El mensaje de solicitud de provisión de información incluye la identidad móvil (MID) para su uso en la solicitud de información y la información de seguridad para verificar si el terminal puede solicitar la información. La solicitud de provisión de información puede incluir otras informaciones que se describirán con las realizaciones de las figuras 3 a 12b.

La entidad 12 de provisión de información proporciona la clave de seguridad para el terminal 10 y otra información necesaria para su uso en la conexión de red, tal como el identificador de terminal en la etapa 24. La clave de seguridad es la clave maestra para su uso en la generación de la clave necesaria para que el terminal 10 se conecte al sistema de comunicación móvil. Se generan varias claves para su uso en la comunicación en función del maestro y se distribuyen. La clave de seguridad según una realización puede generarse mediante cualquiera de varias entidades. Se realiza una descripción del procedimiento para generar y distribuir la clave de seguridad y el identificador en detalle con referencia a las realizaciones de las figuras 3 a 12b.

La entidad de provisión de información envía al terminal 10 el identificador u otra información necesaria para su uso en el acceso, tal como la clave de seguridad a través de la red del operador o la red de comunicación de banda sin licencia, tal como el servidor OTA 14 y el servidor SMS 16 en las etapas 26, 28 y 30. De acuerdo con una realización alternativa, el identificador o clave y otra información necesaria para su uso en el acceso a la red de comunicación pueden transferirse a través de otras entidades que no sean el servidor OTA 14 y el servidor SMS 16.

El terminal 10 puede conectarse al sistema de comunicación móvil utilizando el identificador recibido y/o la clave de seguridad en la etapa 32.

Aunque la realización de la figura 1 se dirige al caso en el que el terminal 10 transmite la solicitud de provisión de información directamente, también es posible transmitir la solicitud de provisión de información a través de un dispositivo de procesamiento de información tal como un PC. Esto se describe posteriormente con referencia a las figuras 10a a 12b.

La figura 2 es un diagrama que ilustra una arquitectura de red de acuerdo con una realización de la presente invención. Se muestra la arquitectura del sistema 3GPP EPS. Aunque esta realización está dirigida a la E-UTRAN, la presente invención puede aplicarse a otro sistema de comunicación móvil.

Con referencia a la figura 2, la estación 112 base de nodo evolucionado (eNB)/controlador de red de radio (RNC) establece una conexión de radio para la comunicación con el equipo 110 de usuario (en adelante denominado terminal o UE) ubicado dentro del área de servicio del eNB. El área de servicio de cada eNB/RNC se denomina celda.

El UE 110 indica el terminal que se conecta a una red de paquetes de datos tal como Internet a través de una puerta 116 de enlace de servicio (en lo sucesivo, denominada GW de servicio o SGW). El UE 110 consiste en dos elementos. Es decir, el UE 110 consiste en un equipo 111 móvil (ME) y un USIM 170. El ME 111 es el componente responsable de la función de comunicación en interoperación con el usuario o la red. El USIM 170 es el componente responsable de almacenar y administrar la información del suscriptor y la información de seguridad.

Según una realización, el sistema de comunicación móvil incluye una pasarela de red de datos por paquetes (PDN GW) 118. La PDN GW 118 es una entidad de red clave de la red de paquetes de datos y funciona como agente local (HA).

El sistema de comunicación móvil incluye además la entidad 114 de gestión de movilidad (MME)/nodo 115 de soporte GPRS de servicio (SGSN). La MME/SGSN 114 y 115 es responsable de la gestión de movilidad de UE, la gestión de ubicación del UE y la gestión de registro.

El sistema de comunicación móvil incluía además el servidor de suscriptor doméstico (HSS)/registro de ubicación de inicio (HLR)/centro 121 de autenticación (AUC). El HSS/HLR 121 gestiona la información de autenticación de usuario y el UE y la información de servicio. El HSS/HLR/AUC 121 se conecta a la MME/SGSN 114 a través de una interfaz.

Hay una interfaz para proporcionar la ruta de datos y gestionar la movilidad del UE entre el eNB/RNC 112 y la GW 116 de servicio y entre la MME/SGSN 114 y la GW 116 de servicio.

En esta realización, el UE 110 y la MME/SGSN 114 se comunican a través de la pila de protocolos NAS para la gestión de la movilidad y la gestión de la sesión. Cada una de las redes domésticas y visitadas puede ser uno de varios tipos de RAT, tal como EUTRAN, UTRAN y GERAN y WLAN de banda sin licencia (Wi-Fi).

De acuerdo con esta realización, el sistema de comunicación móvil incluye un centro 191 USIM. El centro USIM participa en el procedimiento de almacenar la información del operador o del usuario en la UICC y transferir el parámetro de seguridad específico del operador del UE 110, la clave de seguridad y el identificador del UE al usuario.

De acuerdo con esta realización, el sistema de comunicación móvil incluye un centro 180 central de USIM. El usuario puede transferir la solicitud de almacenamiento de información del usuario al centro central de USIM a través de Internet utilizando el UE 110 u otro dispositivo 186 de información, tal como un PC. El centro 180 central de USIM recibe la solicitud de provisión de información del usuario.

El sistema de comunicación móvil incluye un centro 190 de autenticación USIM. El centro 190 de autenticación USIM participa en el procedimiento de autenticación de información de seguridad de USIM.

De acuerdo con esta realización, la tecnología en el aire (OTA) se usa para la transmisión y gestión segura de la información de autenticación del suscriptor, parámetros de seguridad e identificadores. Para este fin, el sistema de comunicación móvil incluye servidores 182 y 182-2 OTA. El sistema de comunicación móvil incluye el centro 184 y 184-2 de servicio de mensajes cortos (SMSC). El SMSC 184 y 184-2 realiza la transmisión de mensajes relacionados.

El sistema de comunicación móvil incluye un MSC 187 y 187-2 de puerta de enlace SMS (GMSC) para la transmisión de mensajes y un centro 188 y 188-2 de conmutación móvil (MSC).

En la figura 2, las entidades de red de la red local y visitada se indican con diferentes números de referencia. Además, el servidor 182 OTA incluido en la red doméstica y el servidor 182-2 OTA central incluido en una red de operador específica se indican con diferentes números de referencia.

Los procedimientos de operación de acuerdo con realizaciones de la presente invención se describen a continuación con referencia a las figuras 3 a 12b. Las siguientes descripciones en las realizaciones se hacen con referencia a la figura 2. En las siguientes realizaciones, se describen las operaciones del UE 110, MME 114, HSS 121 y 121-2, y otras entidades de red. Según dichas operaciones, la información de seguridad específica del operador y los identificadores del usuario se transmiten de manera eficiente.

Las figuras 3 a 5b son diagramas de flujo que ilustran procedimientos de provisión inicial o de provisión de información de acuerdo con una realización de la presente invención.

La provisión de información se activa en la etapa 201. El usuario puede manipular la interfaz del UE 110 para seleccionar un operador. El usuario puede seleccionar un operador primero después de comprar el UE o USIM o cambiar a un operador a través de un procedimiento de la presente invención. El usuario puede ingresar a una red del operador correspondiente para recibir un determinado servicio. Es decir, el usuario puede seleccionar si usar la red 3G o E-UTRAN. El UE 110 inicia el procedimiento de provisión de información para recibir el servicio del operador correspondiente. Este procedimiento puede realizarse de tal manera que el usuario seleccione la interfaz de usuario del UE 110. El usuario puede hacer una entrada de selección al UE 110, particularmente ME 111.

El USIM 170 envía al ME 111 una respuesta de activación de provisión en la etapa 203. La respuesta de activación de provisión se transmite en respuesta a la activación de provisión de información en la etapa 201.

Dicho procedimiento de iniciación de la provisión de información incluye transmitir la activación de la provisión de información del ME 111 al USIM 170 en la etapa 201 y transmitir la respuesta de activación de la provisión de información del USIM 170 al ME 111 en la etapa 203. En particular, la etapa 203 comprende una etapa de leer información del USIM 170 para adquirir la información que el UE 110 debe transmitir a través de la red. La etapa 203 también incluye la preparación para transmitir la información a la red.

El mensaje de solicitud de provisión de información se transmite desde el UE 110 a la MME 114 a través del eNB 112 en las etapas 205 y 207. El mensaje de solicitud de provisión de información se entrega al centro 180 central de USIM a través de la MME 114. Para que el UE 110 reciba a través de la red del operador correspondiente, se requiere la información de seguridad u otra información tal como un identificador. En las etapas 205 y 207, el UE 110 no tiene información necesaria para recibir el servicio del operador correspondiente. En consecuencia, si el UE 110 solicita la información inicial, esta es la situación capaz de acceder al centro 180 central del USIM en un modo limitado. Si el usuario 110 está cambiando el operador, puede estar en el modo de comunicación normal.

El mensaje de solicitud de provisión de información puede incluir Identidad Móvil (MID). Dependiendo de la realización, el mensaje de solicitud de provisión de información puede incluir al menos uno del valor de seguridad, credencial de seguridad, identidad de red móvil terrestre pública (ID de PLMN), tipo de red y ubicación de UE (loc.).

MID es el identificador del centro 180 central del USIM para identificar el UE 110 o USMI/SIM/UICC 170. El MID es asignado por el UE 110 o un fabricante (vendedor) del USIM/SIM/UICC 170 y se utiliza para el centro 180 central del USIM para identificar el UE 110 correspondiente. El MID puede expresarse en un tipo diferente de formato de identificador que puede transmitirse a través de la búsqueda o por un canal de radio. El USIM/ISM/UICC se proporciona en forma de un módulo o tarjeta que contiene la información de autenticación del suscriptor capaz de identificar al suscriptor.

El mensaje de solicitud de provisión de información puede incluir la información de seguridad junto con la información MID. El valor de seguridad y la credencial son información de seguridad representativa.

El valor de seguridad se utiliza cuando se recibe un mensaje en respuesta al mensaje de solicitud de provisión de información. El UE 110 compara el valor de seguridad que ha transmitido y el mensaje recibido. A través de la comparación, es posible probar si el mensaje recibido es el mensaje malicioso enviado por un atacante o un nodo no válido. Es decir, el valor de seguridad se usa para verificar que el mensaje transmitido en respuesta a la solicitud ha sido transmitido. Se pueden usar varios valores capaces de autenticar el UE, como el valor del algoritmo de seguridad soportado por el UE, como la capacidad de seguridad o el número aleatorio generado por el UE 110 como el valor de seguridad.

Normalmente, la credencial de seguridad se compone de un par de clave pública y clave secreta y un certificado en el procedimiento de seguridad de infraestructura de clave pública (PKI). Sin embargo, en la presente invención, la credencial de seguridad es una expresión general sobre la información que puede utilizarse para la verificación del terminal válido utilizado en el centro 190 de autenticación del USIM, así como dicha información.

Si se usa el procedimiento PKI, el centro 190 de autenticación del USIM puede usar la credencial de seguridad para autenticar el UE 110 o el USIM 170 que ha transmitido el valor de autenticación como un procedimiento usado en general. Se puede utilizar para autenticar nodos pares transmitidos el valor a través del protocolo de autenticación y acuerdo de clave (AKA) mutuamente. En este caso, el valor del vector utilizado en AKA puede ser la credencial de seguridad. En el caso de utilizar el procedimiento de autenticación con un número aleatorio y un valor clave, el valor aleatorio puede usarse como credencial de seguridad. Se pueden usar otras diversas tecnologías candidatas. En la siguiente realización, si hay alguna información de seguridad que el centro 190 de autenticación USIM puede usar para verificar el usuario válido, esto puede denominarse credencial de seguridad.

La ID de PLMN también se conoce como ID de red de servicio. Para que el suscriptor proporcione la información del país de la red del operador para la suscripción y la información de la red del operador al centro 191 USIM, el UE 110 puede enviar la información en la red que proporciona el servicio utilizando la ID de PLMN. El tipo de red es la información sobre el tipo de red que proporciona el servicio. El tipo de red puede ser la información sobre el tipo de red de los enlaces alámbricos/inalámbricos de la red del operador, como la red del sistema de paquetes evolucionado (EPS) como la red de acceso de radio terrestre UMTS evolucionada (EUTRAN), la red de acceso de radio terrestre UMTS (UTRAN), y red de acceso de radio GSM/EDGE (GERAN). Si el tipo de red se incluye en el mensaje de solicitud de provisión de información, el UE 110 puede usar uno de los diversos tipos de red proporcionados por el operador correspondiente de forma selectiva. Es decir, el UE 110 puede seleccionar el enlace alámbrico/inalámbrico para su uso al recibir el servicio. La información de ubicación del UE 110 puede usarse para determinar la MME 114 o el MSC 188 que proporciona al usuario el servicio o determinar el área de seguimiento que proporciona al usuario el servicio.

La MME 114 envía al centro 180 central de USIM un mensaje de solicitud de verificación de provisión de información en la etapa 209. Al recibir el mensaje de solicitud de provisión de información del UE 110, la MME 114 envía al centro 180 central de USIM el mensaje de solicitud de verificación de provisión de información. El mensaje de solicitud de verificación de provisión de información puede incluir la identidad móvil (MID). Según una realización, el mensaje de solicitud de verificación de provisión de información puede incluir al menos uno de valor de seguridad, credencial de seguridad, ID de PLMN, tipo de red e información de ubicación de UE (loc.).

La realización anterior ha ejemplificado el caso en el que el UE 110 determina el tipo de la red de servicio en el momento de seleccionar el operador y transmitir el mensaje de solicitud de provisión de información. Sin embargo, si el operador conectado es el operador al que el UE 110 pretende suscribirse, se puede aplicar una realización alternativa. Según una realización alternativa, la MME 1140 proporciona la información del tipo de red en la red a la que pertenece la MME en el momento en que envía al centro 180 central de USIM el mensaje de solicitud de verificación de provisión de información en la etapa 209, ya que el UE 110 ha transmitido el mensaje de solicitud de provisión de información. El tipo de red puede ser cualquiera de las redes cableadas/inalámbricas del operador, incluyendo la red de sistema de paquetes evolucionado (EPS) como red de acceso de radio terrestre UMTS evolucionada (EUTRAN), red de acceso de radio terrestre UMTS (UTRAN) y red de acceso de radio GSM/EDGE (GERAN). Según la realización alternativa, la MME 114 envía al centro 180 central de USIM el tipo de red junto con el MID, el valor de seguridad, la credencial de seguridad y la ID de PLMN transmitida por el UE 110.

Posteriormente, el centro 180 central de USIM envía al centro 190 de autenticación USIM el mensaje de solicitud de verificación de provisión de información en la etapa 211. El mensaje de solicitud de verificación de provisión de información puede incluir MID. Según una realización, el mensaje de solicitud de verificación de provisión de información puede incluir al menos una de credencial de seguridad, ID de PLMN y tipo de red. El centro 180 central

de USIM solicita verificar que el MID identifica al usuario válido accesible para el operador utilizando el mensaje de solicitud de verificación de provisión de información. En la verificación de solicitud de provisión de información, se pueden usar varias credenciales de seguridad.

Si el centro 190 de autenticación USIM y el UE 110 usan el sistema PKI, la clave pública y la clave de seguridad de PKI se usan como credenciales de seguridad. Es decir, el centro 190 de autenticación USIM verifica el UE 110 o USIM 170 que ha transmitido el valor de autenticación con las claves públicas y de seguridad. Se puede utilizar para autenticar nodos pares transmitidos el valor a través del protocolo de autenticación y acuerdo de clave (AKA) mutuamente. En este caso, el valor del vector utilizado en AKA puede ser la credencial de seguridad. En el caso de utilizar el procedimiento de autenticación con un número aleatorio y un valor clave, el valor aleatorio puede usarse como credencial de seguridad. Se pueden usar otras diversas tecnologías candidatas. En esta realización, si hay alguna información de seguridad que el centro 190 de autenticación USIM puede usar para verificar el usuario válido, esto puede denominarse credencial de seguridad. No se menciona un procedimiento detallado para usar la credencial de seguridad. Sin embargo, el centro 180 central de USIM envía al centro 190 de autenticación USIM el mensaje de solicitud de verificación de provisión de información y recibe el mensaje de respuesta de verificación de provisión de información en repetición en las etapas 211 y 213 como el procedimiento correspondiente. En este caso, el parámetro de seguridad denominado credencial de seguridad utilizado en las etapas 211 y 213 puede determinarse dependiendo de si se utiliza el esquema PKI o AKA. En cualquier caso, sin embargo, es posible verificar el acceso válido del UE 110 basado en la información proporcionada por el UE 110 tal como el parámetro de seguridad y la identidad llamada credencial de seguridad en las etapas 211 y 213. Los expertos en la materia pueden modificar este procedimiento de verificación de varias maneras. El centro 190 de autenticación USIM envía al centro central de USIM el mensaje de respuesta de autenticación de provisión de información en la etapa 213. El mensaje de respuesta de autenticación de provisión de información puede incluir MID para indicar la solicitud de autenticación de provisión de información correspondiente verificada con éxito.

A continuación, el procedimiento de las etapas 213-2 a 213-16 o el proceso de las etapas 227-2 a 227-7 se realizan de forma selectiva.

Se realiza una descripción de la realización de ejecutar las etapas 213-2 a 213-16 con referencia a las figuras 4a y 4b.

Como se describió anteriormente, el centro 180 central de USIM recibe un mensaje de respuesta del centro 190 de autenticación de USIM en respuesta a la solicitud de verificación de provisión de información en la etapa 213. Luego, el centro 180 central de USIM envía a la MME 114 el mensaje de respuesta de provisión de información en la etapa 213-2. El mensaje de respuesta de provisión de información puede incluir MID.

Después del procedimiento de verificación, la MME 114 envía al MSC 188 un mensaje de solicitud de registro de ubicación en la etapa 213-11. El mensaje de solicitud de registro de ubicación puede incluir un identificador MID y/o MME. Después, el MSC 188 almacena un mapeo entre el identificador MID y MME en la etapa 213-12. El MSC 188 envía al HSS 121 el MID en la etapa 213-13. Dependiendo de la realización, el MSC 188 puede enviar además la información de dirección (MSCA) del MSC. El HSS 121 almacena el mapeo entre MID y MSCA en la etapa 213-14. El HSS 121 puede generar MSISDN en la etapa 213-15. El MSISDN se utiliza como un identificador para la comunicación en una red de conmutación de circuitos. El HSS 121 puede enviar al MSC 188 el MID en la etapa 213-16. Dependiendo de la realización, el HSS 121 puede transmitir además al menos uno de MSISDN y MSCA. Las etapas 213-11,213-12, 213-13, 213-14 y 213-16 descritas anteriormente son idénticas a las etapas 227-2, 227-3, 227-4, 227-5 y 227-7 que se describirán a continuación. Si se ejecutan las etapas 213-11,213-12, 213-13, 213-14 y 213-16 (caso 1), se omiten las etapas 227-2, 227-3, 227-4, 227-5 y 227-7. Por el contrario, si se ejecutan 227-2, 227-3, 227-4, 227-5 y 227-7 (caso 2), las etapas 213-11, 213-12, 213-13, 213-14 y 213 -16 se omiten.

Posteriormente, el centro 180 central de USIM puede enviar al centro 191 de USIM el MID en la etapa 215. Dependiendo de la realización, el centro 180 central de USIM puede enviar además al centro 191 USIM al menos uno de valor de seguridad, ID de PLMN, tipo de red, valor de verificación del centro central de seguridad (centro de Seg-Central) e información de ubicación de UE (loc.). El valor de verificación del centro central de seguridad se utiliza para verificar el centro 180 central de USIM. El valor de verificación del centro de Seg-central puede ser el valor que incluye la clave pública/clave de seguridad en el caso de utilizar el sistema PKI para la verificación. El valor de verificación del centro de Seg-central también puede ser un número aleatorio que se cifra o descifra utilizando una clave compartida. Se pueden usar varios valores como el valor de verificación del centro de Seg-central, y en el presente documento se omite la descripción detallada del procedimiento de autenticación mutua.

Al recibir el parámetro, el centro 191 USIM verifica el valor de verificación del centro de Seg-central en la etapa 217.

El centro 191 USIM puede generar una clave de seguridad en la etapa 219. Esto corresponde a una realización (caso 1) en la que el centro 191 de USIM genera y distribuye la clave de seguridad. Según otra realización (caso 2), el centro 191 de USIM no tiene función de generación de seguridad. En esta realización, el AUC/HSS/HLR 121 es responsable de la función correspondiente. Es decir, el AUC/HSS/HLR 121 genera la clave de seguridad que puede usarse como la clave maestra (clave raíz) asignada al operador correspondiente en sí mismo. Según otra realización (caso 3), el centro 191 de USIM genera la clave de seguridad para el operador y el operador usa esta clave como semilla para generar la clave maestra de seguridad como clave reforzada específica del operador. Es decir, el centro 191 de USIM

genera la clave de seguridad. El AUC/HSS/HLR 121 de la red del operador genera otra clave maestra derivada (Kdm) que funciona como el papel del maestro utilizado en la red del operador utilizando la clave de seguridad como semilla. La clave maestra puede ser la clave raíz como clave de seguridad o la clave maestra derivada (Kdm). Sobre la base de dicha clave maestra, la red del operador genera la clave de autenticación (KASME). La red del operador genera una clave de integridad NAS (KNASint) y una clave de cifrado NAS (KNASenc).

El centro 191 de USIM determina la MME al que se ha conectado el UE o el MSC conectado a la MME al que se ha conectado el UE u otra MME o MSC para proporcionar al UE el servicio de provisión de información inicial en la etapa 219-2. El centro 191 de USIM puede usar al menos una ID de PLMN, información de ubicación de UE e información de red conectada al UE para hacer tal determinación. En esta realización, la MME al que se ha conectado el UE 110 y el MSC conectado a la MME correspondiente proporciona al UE 110 el servicio de provisión de información inicial. Sin embargo, este procedimiento puede modificarse de varias maneras. Es decir, dicho procedimiento de selección se puede modificar de varias maneras dependiendo de si el operador proporciona el servicio al operador de red al que se ha conectado el UE.

El centro 191 de USIM puede determinar una lista de identidad (ID) de áreas de seguimiento (área de registro de ubicación de UE) en la etapa 219-3. La MME puede utilizar el área de seguimiento para seleccionar el eNB para la entrega del servicio de provisión de información inicial. La lista de ID de TA se envía en el procedimiento después de la etapa 237 o 239. La MME puede seleccionarse por el centro 191 de USIM. Sin embargo, en cierto caso, el servidor 182 OTA puede ser responsable de la función que se describe con referencia a las etapas 237-2 y 237-3.

En una realización (caso 1), si el centro 191 de USIM genera y almacena la clave de seguridad en la etapa 219, envía la MME 114 de la red del operador al que el UE 110 tiene la intención de suscribir al menos uno de MID como UE o USIM/Identificador UICC/SIM, valor de seguridad, ID PLMN y tipo de red. Después, la MME 114 envía al HSS/HLR 121 el valor MID y de seguridad en la etapa 223. Si el centro 191 de USIM genera la clave de seguridad, la MME también puede enviar al HSS/HLR 121 la clave de seguridad. El AUC/HSS/HLR 121 genera y almacena el IMSI como el identificador del UE 110 en la etapa 225. Si el centro 191 de USIM no ha generado la clave de seguridad, el AUC/HSS/HLR 121 genera y almacena la clave de seguridad de acuerdo con otra realización (caso 2). El AUC/HSS/HLR 121 puede generar y almacenar el número de red digital de servicios integrados internacionales de estación móvil (MSISDN) necesario para la comunicación en una red CS en la etapa 225. Si la red a la que se ha conectado inicialmente el UE es idéntica a la red para proporcionar servicio después, el MSISDN puede generarse en la etapa 213-15. Según otra realización, el MSISDN puede generarse después en la etapa 225. Sin embargo, si la red que el UE 110 ha conectado inicialmente difiere de la red que proporcionará el servicio después, el MSISDN generado en la etapa 213-15 se usa para proporcionar información al UE 110 mientras se usa el MSISDN asignado en la etapa 225 como el identificador para su uso en la red después. A diferencia del ejemplo anterior (caso 1), el AUC/HSS/HLR 121 genera la seguridad en otra realización (caso 2). En otra realización más (caso 3), se genera una clave maestra (clave maestra derivada) utilizando la clave de seguridad enviada por el centro 191 de USIM como una semilla, utilizándose la clave maestra derivada (Kdm) como clave maestra de seguridad. En el caso 1, la clave de seguridad transmitida almacenada en las etapas 227, 229 y 236 es la clave de seguridad generada por el centro 191 de USIM. En el caso 2, la clave de seguridad transmitida y almacenada en las etapas 227, 229 y 236 es la clave generada por el AUC/HSS/HLR 121. En el caso 3, la clave de seguridad transmitida y almacenada en las etapas 227, 229 y 236 es la clave maestra de seguridad derivada usando la clave recibida del centro 191 de USIM como semilla.

El AUC/HSS/HLR 121 envía a la MME 114 el MID en la etapa 227. Dependiendo de la realización, el AUC/HSS/HLR 121 puede enviar a la MME 114 al menos uno de IMSI, clave de seguridad (caso 2)/clave maestra de seguridad (caso 3) y perfil. El perfil es la información necesaria para configurar el UE 110 o USIM/UICC/SIM para que se ajuste a la red del operador correspondiente. El perfil puede incluir al menos un algoritmo de kilometraje que representa la función de seguridad en AKA, algoritmo de seguridad de cifrado SNOW (cifrado de corriente: un nuevo cifrado de corriente de palabra)/integridad, algoritmo de seguridad de protección de cifrado estándar de cifrado avanzado/integridad. El perfil también puede incluir al menos uno de la clase de control de acceso, códigos de llamadas de emergencia, lista PLMN y dominio de la red doméstica.

El MME 114, MSC 188 y HSS 121 pueden participar en el registro de ubicación de UE con una red CS para SMS posteriormente. En el caso de que no se realicen las etapas 213-11, 213-12, 213-13, 213-14 y 213-16 (caso 2), las etapas 227-2, 227-3, 227-4, 227-5 y 227-7 se puede realizar. Las etapas 227-2 a 227-7 pueden ejecutarse selectivamente. El MME 114 envía al MSC 188 un mensaje de solicitud de registro de ubicación. El mensaje de registro de ubicación puede incluir el MID. Dependiendo de la realización, el mensaje de solicitud de registro de ubicación puede incluir además un identificador MME. El MSC 188 puede almacenar la correspondencia entre el identificador MID y MME en la etapa 227-3. El MSC 188 envía al HSS 121 el MID y la información de dirección (MSCA) del MSC en la etapa 227-4. El HSS 121 almacena el mapeo entre mediados y MSCA 227-5. El HSS 121 envía al MSC 188 el MID en la etapa 227-7. Dependiendo de la realización, el HSS 121 envía al MSC 188 al menos uno de MSISDN y MSCA. Las etapas 227-2, 227-3, 227-4, 227-5, 227-7 son idénticas a las etapas 213-11, 213-12, 213-13, 213-14 y 213-16. En lugar de las etapas 213-11, 213-12, 213-13, 213-14 y 213-16, se pueden realizar las etapas 227-2, 227-3, 227-4, 227-5 y 227-7.

El MME 114 puede enviar al centro 191 de USIM el MID en la etapa 229. Dependiendo de la realización, la MME 114 puede transmitir al menos uno de IMSI, seguridad (caso 2)/clave maestra de seguridad (caso 3), perfil y valor de

seguridad.

Después, el centro 191 de USIM puede enviar al centro 180 central de USIM el MID en la etapa 231. Dependiendo de la realización, el centro 191 de USIM puede enviar al centro 180 central de USIM el valor de verificación del centro de USIM (valor de verificación del centro Sec-USIM). El valor de verificación del centro Sec-USIM se utiliza para la autenticación mutua y la seguridad entre el centro 180 central de USIM y el centro 191 de USIM. Es decir, el centro 180 de USIM utiliza el valor de verificación del centro Sec-USIM para verificar el centro 191 de USIM. De esta manera, es posible notificar que el centro 191 de USIM ha procesado la solicitud para el UE 110 representado por MID transmitido desde el centro 180 central de USIM al centro 191 de USIM. El centro 180 central de USIM y el centro 191 de USIM pueden realizar la autenticación mutua.

Al recibir el parámetro, el centro 180 central de USIM verifica el valor de verificación del centro Sec-USIM en la etapa 233. En la etapa 233, si el sistema PKI se usa para verificar el valor de verificación del centro Sec-USIM, el valor puede incluir la clave pública/clave de seguridad. El valor de verificación del centro Sec USIM puede ser un valor aleatorio que se cifra y descifra con una clave compartida cuando se aplica la autenticación mutua. En el caso de utilizar el esquema AKA, el valor de verificación del centro Sec-USIM puede ser un valor de señal de autenticación. Se pueden usar varios valores como el valor de verificación del centro de Seg-central, y en el presente documento se omite la descripción detallada del procedimiento de autenticación mutua.

El centro 180 central de USIM envía al centro 191 de USIM un mensaje de confirmación en la etapa 235. El mensaje de confirmación se utiliza para notificar que el centro 191 de USIM ha procesado la solicitud del centro 180 central de USIM con éxito. El mensaje de confirmación también puede notificar el éxito de la autenticación mutua. En el caso 2 o 3, dado que la clave de seguridad o el valor de la clave maestra de seguridad se genera o modifica en el AUC/HSS/HLR 121 en la etapa 236, el centro 191 de USIM puede almacenar el valor de la clave de seguridad/clave maestra de seguridad. Si el centro 191 de USIM es responsable de almacenar la información de seguridad asignada por el operador en asociación con MID, el centro 191 de USIM puede almacenar el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil.

Después, el centro 191 de USIM puede enviar al servidor 182 OTA el MID en la etapa 237. Dependiendo de la realización, el centro 191 de USIM puede enviar además al servidor 182 OTA al menos uno de los valores de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil. En el caso de que la información de la lista de ID de TA se determine en la etapa 219-3, el centro 191 de USIM envía al servidor 182 de OTA la lista de ID de TA.

Si el centro 191 de USIM no ha seleccionado ninguna MME para proporcionar información inicial en las etapas 219-2 y 219-3 o si el servidor OTA 182 es capaz de seleccionar la MME, el servidor OTA 182 puede seleccionar una MME en las etapas 237-2 y 237-3. Es decir, el servidor 182 OTA puede seleccionar la MME a la que se ha conectado el UE o el MSC conectado a la MME a la que se ha conectado el UE utilizando al menos una ID de PLMN, información de ubicación de UE e información de red conectada a UE en la etapa 237-2. El servidor 182 OTA puede determinar la MME o el MSC para proporcionar el UE dentro del servicio de provisión de información inicial utilizando la información descrita anteriormente. Esta realización ha ejemplificado el caso en el que la MME al que se ha conectado el UE y el MCS conectado a la MME correspondiente entrega el servicio de provisión de información inicial al UE. Sin embargo, este procedimiento puede modificarse de varias maneras. Es decir, el procedimiento de selección puede modificarse de varias maneras dependiendo de si el UE es servido por el operador de red conectado u otro operador. El servidor 182 OTA puede determinar la información tal como la lista de identidad del área de seguimiento (lista de ID de TA) en la etapa 237-3. El área de seguimiento se utiliza para que la MME determine el eNB para la entrega del servicio de provisión de información inicial. Dicha información puede transmitirse a través del procedimiento que sigue a la etapa 239.

El servidor OTA puede enviar al centro de servicio de mensajes cortos (SMSC) el MID en la etapa 239. Dependiendo de la realización, el servidor 182 OTA puede enviar además el SMSC 184 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil. En cualquier caso, el servidor 182 OTA puede enviar además la lista de ID de TA al SMSC 184.

En el procedimiento de las etapas 239-2 a 241-2, el SMSC 184 puede enviar al UE 110 el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA. El procedimiento de las etapas 239-2 a 241-2 se divide en varios procedimientos. De acuerdo con los procedimientos, el SMSC 184 envía al MSC 188 el MID, el valor de seguridad, el IMSI, la clave de seguridad, el perfil y otros parámetros. Si la red como objetivo del UE 110 es una red de servicio de datos de circuito conmutado (CS), la información y los parámetros relacionados se entregan al UE 110 a través del MSC 188. De lo contrario, si la red como objetivo del UE 110 es una red de servicio de datos con conmutación de paquetes (PS), la información y los parámetros relacionados se entregan al UE 110 a través de SMSC 184, MSC 188 y MME 114.

Las etapas 239-2 a 239-5 pueden realizarse selectivamente.

El SMSC 184 envía al GMSC 187 el MID en la etapa 239-2. Según una realización, el SMSC 184 puede enviar además el GMSC 187 al menos uno de los valores de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA. Después, el GMSC 187 envía al HSS 121 el MSISDN en la etapa 239-3. El GMSC 187 recibe la

dirección MSC (MSCA) desde el HSS 121. Después, el GSMC 187 envía al MCS 188 el MID en la etapa 239-5. Dependiendo de la realización, el GSMC 187 puede enviar además el MSC 188 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA. Luego, el MSC 188 envía a la MME 114 al MID. Dependiendo de la realización, el MSC 188 transmite al menos uno de los valores de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA.

La MME 114 determina un eNB al que se reenvía la información recibida en la etapa 239-7. La MME 114 puede usar la lista de ID de TA recibida para hacer la determinación. En el caso de que se usen el eNB 112 y la MME 114 cuando el UE 110 se ha conectado a la red como en esta realización, la MME 114 selecciona el eNB 112 usado para la conexión con prioridad. La MME 114 envía al eNB 112 el valor MID y de seguridad en la etapa 241-1. El eNB 112 puede enviar al UE 110 el valor MID y de seguridad en la etapa 241-2.

El UE 110 es capaz de verificar si la información se recibe en respuesta a la solicitud que ha transmitido basándose en el valor de seguridad en la etapa 243. El UE 110 puede notificar al eNB 112 que el valor de seguridad se verifica con éxito en la etapa 243-2. El mensaje de notificación puede incluir MID. El eNB 112 puede notificar a la MME 114 que el UE 110 ha verificado con éxito el valor de seguridad en la etapa 243-3. Las etapas 243-2 y 243-3 pueden ejecutarse selectivamente.

La MME 114 puede actualizar la clave de búsqueda primaria de la base de datos del HSS 121 para la comunicación y buscar posteriormente en la etapa 243-4. La etapa 243-4 se realiza para recuperar la información en el UE 110 del HSS 121 de manera eficiente y adquirir la sincronización de la base de datos del HSS. Este procedimiento es opcional dependiendo de la implementación de la base de datos del HSS. Posteriormente, la MME 114 puede enviar el eNB 112 al MID. Dependiendo de la realización, la MME 114 puede enviar el eNB 112 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, lista de ID de TA de perfil y MSISDN. Después, el eNB 112 puede enviar al UE 110 el MID en la etapa 243-6. Dependiendo de la realización, el eNB transmite al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y MSISDN. En este momento, se puede utilizar un procedimiento similar a la paginación.

Posteriormente, si se recibe la información anterior, el UE 110 almacena al menos uno de los perfiles, IMSI, clave de seguridad/clave maestra de seguridad y MSISDN. El USIM 170 activa el procedimiento de conexión del UE a la ME 111. El UE 110 envía a la MME 114 el mensaje ATTAHC a través del eNB 112 en las etapas 249 y 251. El mensaje ADJUNTO puede incluir el IMSI como el identificador de UE. Después, la MME 114 envía al UE 110 un mensaje ACEPTACIÓN DE ADJUNTO a través del eNB 112 en las etapas 259 y 261. Dado que el procedimiento ADJUNTO es bien conocido, la descripción se dirige a una parte modificada en la presente invención en el presente documento.

Las figuras 6a y 6b son un diagrama de flujo que ilustra el procedimiento de provisión de información de acuerdo con una realización de la presente invención. Las figuras 6a y 6b se refieren integralmente a la figura 6. Dado que el proceso antes del procedimiento de la figura 6 es idéntico a la primera mitad del procedimiento de las figuras 3 a 5b, es decir, una parte de la figura 3, 4a o 4b, y la figura 6 es similar a las figuras 5a y 5b, la descripción se dirige a la parte diferente de las etapas 339-7 a 342-6.

La MME 114 determina un eNB al que reenvía la información recibida en la etapa 339-7. Para tomar esta determinación, la MME puede usar la lista de ID de TA recibida. Si existe el eNB y la MME al que se ha conectado el UE en esta realización, la MME 114 puede seleccionar el eNB correspondiente con prioridad para reenviar la información recibida. La MME envía el eNB 112 el MID en la etapa 342-1. Dependiendo de la realización, la MME 114 puede enviar además al eNB 112 la indicación de notificación de transmisión de información para la provisión de información inicial, MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil, lista de ID de TA y MSISDN. La indicación utilizada en la etapa 342-1 es un parámetro que indica el significado de transmitir la información para la provisión de información inicial. Si la MME 114 envía el mensaje que lleva la información inicial al eNB 112 conectado a la MME como en la etapa 342-1 o un eNB específico basado en la lista de TA depende de la realización. El eNB 112 busca el UE 110 en el modo inactivo para recibir el mensaje de provisión de información inicial en la etapa 342-2. El eNB 112 puede enviar al UE 110 el MID en la etapa 342-3. Dependiendo de la realización, el eNB 1120 puede enviar además el UE 110 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y MSISDN. El eNB 112 puede enviar al UE 110 dicha información de tal manera que se difunda en el mensaje de información del sistema. El UE 110 verifica, basándose en el valor de seguridad, que la información se recibe en respuesta a la solicitud que el UE 110 como un UE válido tiene como transmitida.

El procedimiento de las etapas 342-4 y 342-5 puede realizarse selectivamente.

El UE 110 notifica al eNB 112 el éxito de la verificación del valor de seguridad en la etapa 342-4. El mensaje de notificación puede incluir MID. El eNB 112 notifica a la MME 114 que el UE 110 ha verificado con éxito el valor de seguridad en la etapa 342-5. El mensaje de notificación puede incluir MID. La MME 114 puede actualizar la clave de búsqueda primaria de la base de datos del HSS para la comunicación y buscar posteriormente en la etapa 342-6. La etapa 342-6 se realiza para que el HSS 121 busque información en el UE 110 de manera eficiente. La etapa 342 se realiza para adquirir la sincronización de la base de datos entre el UE 110 y el HSS 121 correspondiente al UE 110 y facilitar la búsqueda y puede saltarse dependiendo de la implementación de la base de datos del HSS 121.

Las figuras 7a y 8b son un diagrama de flujo que ilustra el procedimiento de provisión de información de acuerdo con una realización de la presente invención.

La provisión de información se activa en la etapa 601. El usuario puede realizar la manipulación para seleccionar un operador a través de la interfaz del UE 110. El usuario puede seleccionar un operador primero después de comprar el UE o USIM o cambiar el operador a través de un procedimiento de la presente invención. El usuario también puede ingresar a una red del operador correspondiente para recibir el servicio. Es decir, el usuario puede seleccionar si usar la red 3G o EUTRAN del mismo operador. El UE 110 inicia el procedimiento de provisión de información para recibir el servicio del operador correspondiente. Este procedimiento puede realizarse de tal manera que el usuario seleccione una interfaz de usuario del UE 110. La entrada de selección del usuario puede hacerse a la ME 111 del UE 110.

El USIM 170 envía a la ME 111 la provisión de información que desencadena la respuesta en la etapa 603. La respuesta de activación de provisión de información es una respuesta a la activación de provisión de información realizada en la etapa 601.

El procedimiento de iniciación de la provisión de información incluye transmitir la activación de la provisión de información del ME 111 al USIM 170 en la etapa 601 y transmitir la respuesta de activación del suministro del USIM 170 al ME 111 en la etapa 603. En particular, la etapa 603 incluye leer, en el UE 110, la información a transmitir a través de la red desde el USIM 170. La etapa 603 incluye transmitir la información correspondiente a la red.

En las etapas 605 y 607, el mensaje de solicitud de provisión de información se transmite desde el UE 110 a la MME (aquí, MME-VNO 115 en la red visitada) a través del eNB (aquí, eNB-VNO 113 en la red visitada). El mensaje de solicitud de provisión de información se transmite al centro 180 central de USIM a través del eNB-VNO 113 y la MME-VNO 115. Para que el UE 110 reciba el servicio de la red del operador correspondiente, existe la necesidad de información complementaria tal como la información de seguridad o el identificador. En las etapas 605 y 607, el UE está en el estado que no tiene información para recibir el servicio en la red del operador correspondiente. Si el UE solicita la información inicial, este es el estado capaz de acceder al centro 180 central de USIM en un modo limitado. Si es la situación de cambiar el operador, esto significa que puede ser posible operar en el modo de comunicación normal.

La presente realización está dirigida al caso ejemplar en el que el UE 110 transmite la señal a través del eNB 113 y la MME 115 de la otra red de operadores que el operador al que el UE 110 pretende suscribirse. En este caso, dado que el UE 110 no tiene información tal como una clave de seguridad o un identificador para su uso en la red del operador, el servicio para la conexión al centro 180 central de USIM de la red visitada solo se permite en un estado significativamente limitado.

El mensaje de solicitud de provisión de información puede incluir la identidad móvil (MID). Dependiendo de la realización, el mensaje de solicitud de provisión de información puede incluir al menos un valor de seguridad, credencial de seguridad, ID de PLMN, tipo de red y ubicación de UE (loc.).

El MID es el identificador para su uso para identificar el UE 110 o USIM/SIM/UICC 170. El MID es asignado por el fabricante (proveedor) del UE 110, el USIM/SIM/UICC 170, y se utiliza para identificar el UE 110 en el centro 180 central del USIM. En la descripción anterior, USIM, SIM y UICC son los módulos o tarjetas que contienen la información de autenticación del suscriptor para identificar el UE.

El mensaje de solicitud de provisión de información puede incluir la información de seguridad junto con la información MID. La información de seguridad representativa incluye el valor de seguridad y la credencial.

El valor de seguridad se utiliza cuando se transmite el mensaje de solicitud de provisión de información y se recibe el mensaje relacionado. El UE 110 compara el valor de seguridad que ha transmitido y el mensaje recibido. A través de esta comparación, es posible verificar si el mensaje recibido es un mensaje malicioso transmitido por un atacante u otro nodo no válido. Es decir, el valor de seguridad se utiliza para verificar el mensaje transmitido en respuesta a un mensaje de solicitud transmitido. Se pueden utilizar varios valores de los algoritmos de seguridad, tal como la capacidad de seguridad o el número aleatorio generado por el UE como valor de seguridad.

Por lo general, la credencial de seguridad indica la información que incluye un par de claves de seguridad y secretas y un certificado para su uso en el esquema de seguridad de infraestructura de clave pública (PKI). En la presente invención, sin embargo, la credencial de seguridad indica la información para su uso en la verificación del UE válido en el centro 190 de autenticación de USIM.

Si se usa el esquema PKI, el centro 190 de autenticación de USIM puede usar la credencial de seguridad para autenticar el UE 110 o el USIM 170 que ha transmitido el valor relacionado con la autenticación en un procedimiento normal. En el Protocolo de Autenticación y Acuerdo de Clave (AKA), el procedimiento de autenticación mutua se puede utilizar para autenticar los nodos pares mutuamente. En este caso, el valor del vector relacionado con el AKA puede ser la credencial de seguridad. En el caso del procedimiento de autenticación que utiliza el número aleatorio del valor clave, el valor aleatorio puede ser la credencial de seguridad. Se pueden usar otras diversas tecnologías. En la siguiente realización, si se puede usar cierta información de seguridad para verificar el usuario válido, esto se puede llamar credencial de seguridad.

La ID de PLMN también se conoce como ID de red de servicio. Para que el suscriptor proporcione la información del país de la red del operador para la suscripción y la información de la red del operador al centro 191 USIM, el UE 110 puede enviar la información en la red que proporciona el servicio utilizando la ID de PLMN. El tipo de red es la información sobre el tipo de red que proporciona el servicio. El tipo de red puede ser la información sobre el tipo de red de los enlaces alámbricos/inalámbricos de la red del operador, como la red del sistema de paquetes evolucionado (EPS) como la red de acceso de radio terrestre UMTS evolucionada (EUTRAN), la red de acceso de radio terrestre UMTS (UTRAN), y red de acceso de radio GSM/EDGE (GERAN). Si el tipo de red se incluye en el mensaje de solicitud de provisión de información, el UE 110 puede usar uno de los diversos tipos de red proporcionados por el operador correspondiente de forma selectiva. Es decir, el UE 110 puede seleccionar el enlace alámbrico/inalámbrico para su uso al recibir el servicio. La información de ubicación del UE 110 puede usarse para determinar la MME 114 o el MSC 188 que proporciona al usuario el servicio o determinar el área de seguimiento que proporciona al usuario el servicio.

La MME-VNO 115 envía al centro 180 central de USIM un mensaje de solicitud de verificación de provisión de información en la etapa 609. Al recibir el mensaje de solicitud de provisión de información desde el UE 110, la MME-VNO 115 envía al centro 180 central de USIM el mensaje de solicitud de verificación de provisión de información. El mensaje de solicitud de verificación de provisión de información puede incluir la Identidad Móvil (MID). Dependiendo de la realización, el mensaje de solicitud de verificación de provisión de información puede incluir al menos uno de valor de seguridad, credencial de seguridad, ID de PLMN, tipo de red e información de ubicación de red (loc.).

La realización anterior se dirige a un caso ejemplar en el que el UE 110 selecciona un operador al que pretende suscribirse y envía el tipo de red que proporciona el servicio en el momento en que transmite el mensaje de solicitud de provisión de información. Sin embargo, si el operador al que se ha conectado el UE 110 es el operador al que pretende suscribirse, se puede aplicar una realización alternativa. De acuerdo con una realización alternativa, cuando la MME envía al centro central de USIM el mensaje de solicitud de verificación de provisión de información en la etapa 609 después de que el UE 110 ha transmitido el mensaje de solicitud de provisión de información, el procedimiento puede modificarse de modo que la información tal como el tipo de red de la red a la que pertenece la MME se proporciona conjuntamente. Incluso cuando la red a la que el UE 110 pretende suscribirse y la red a la que se ha conectado el UE 110 en el momento en que envía el mensaje de solicitud de provisión de información pertenecía a diferentes operadores, la información del tipo de red puede proporcionarse a la MME-VNO 115 de la red visitada a la que se ha conectado el UE. Sin embargo, este procedimiento es aplicable solo cuando la red visitada conoce el tipo de red de la red doméstica del par a través del intercambio de información sobre la red y el servicio al que el UE pretende suscribirse. El tipo de red puede ser cualquiera de los tiempos de red de los enlaces alámbricos/inalámbricos de la red del operador, como la red del Sistema de paquetes evolucionado (EPS) como la Red de acceso de radio terrestre UMTS evolucionada (EUTRAN), la Red de acceso de radio terrestre UMTS (UTRAN) y red de acceso de radio GSM/EDGE (GERAN). Es decir, según una realización alternativa, la MME envía al centro 180 central de USIM el tipo de red, así como el MID, el valor de seguridad, la credencial de seguridad y la ID de PLMN transmitida por el UE.

El centro 180 central de USIM envía al centro 190 de autenticación de USIM el mensaje de solicitud de verificación de provisión de información en la etapa 611. El mensaje de solicitud de verificación de provisión de información incluye MID. Dependiendo de la realización, el mensaje de solicitud de verificación de provisión de información puede incluir además al menos una credencial de seguridad, ID de PLMN y tipo de red. El centro central de USIM solicita verificar si el MID identifica al usuario válido accesible para la red del operador utilizando el mensaje de solicitud de verificación de provisión de información. Para verificar la solicitud de provisión de información, se pueden utilizar varias credenciales de seguridad.

Si el centro 190 de autenticación de USIM y el UE 110 usan el sistema PKI, la clave pública y la clave secreta del sistema PKI se usan como credencial de seguridad. Es decir, el centro 190 de autenticación de USIM autentica el UE 110 o USIM 170 que ha enviado el valor relacionado con la autenticación utilizando las claves públicas y secretas. Se puede utilizar para autenticar nodos pares transmitidos el valor a través del protocolo de autenticación y acuerdo de clave (AKA) mutuamente. En este caso, el valor del vector utilizado en AKA puede ser la credencial de seguridad. En el caso de utilizar el procedimiento de autenticación basado en el número aleatorio del valor clave, el valor aleatorio se puede utilizar como credencial de seguridad. Se pueden usar otras diversas tecnologías candidatas. En esta realización, si hay alguna información de seguridad que el centro 190 de autenticación USIM puede usar para verificar el usuario válido, esto puede denominarse credencial de seguridad. No se menciona un procedimiento detallado para usar la credencial de seguridad. Sin embargo, el centro 180 central de USIM envía al centro 190 de autenticación USIM el mensaje de solicitud de verificación de provisión de información y recibe el mensaje de respuesta de verificación de provisión de información en repetición en las etapas 611 y 613 como el procedimiento correspondiente. En este caso, el parámetro de seguridad denominado credencial de seguridad utilizado en las etapas 611 y 613 puede determinarse dependiendo de si se utiliza el esquema PKI o AKA. En cualquier caso, sin embargo, es posible verificar el acceso válido del UE 110 basado en la información proporcionada por el UE 110 tal como el parámetro de seguridad y la identidad llamada credencial de seguridad en las etapas 611 y 613. Los expertos en la materia pueden modificar este procedimiento de verificación de varias maneras. El centro 190 de autenticación USIM envía al centro central de USIM el mensaje de respuesta de autenticación de provisión de información en la etapa 613. El mensaje de respuesta de autenticación de provisión de información puede incluir MID para indicar la solicitud de autenticación de provisión de información correspondiente verificada con éxito.

Las etapas 613-2 a 613-16 descritas a continuación pueden ejecutarse selectivamente.

Como se describió anteriormente, el centro 180 central de USIM recibe un mensaje de respuesta del centro 190 de autenticación de USIM en respuesta a la solicitud de verificación de provisión de información. Luego, el centro 180 central de USIM envía al MME 115 el mensaje de respuesta de provisión de información. El mensaje de respuesta de provisión de información puede incluir MID.

Después de la etapa de autenticación, la MME-VNO 115 de la red visitada envía al MSC-VNO 188-2 el mensaje de solicitud de registro de ubicación en la etapa 613-11. El mensaje de registro de ubicación puede incluir un identificador MID y/o MME. Posteriormente, el MSC-VNO 188-2 almacena el mapeo entre el identificador MID y MME en la etapa 613-12. Dependiendo de la realización, el MSC-VNO 121-2 puede generar MSISDN. Aquí, el MSISDN generado puede usarse como el identificador para usar en la comunicación de red CS. El MSISDN se utiliza para transmitir la información inicial. El HSS-VNO 121-2 envía el MSC-VNO 188-2 al MID. Dependiendo de la realización, el HSS-VNO 121-2 puede enviar además el MSC 188-2 a al menos uno de MSISDN y MSCA.

El centro 180 central de USIM envía al centro 191 de USIM el MID en la etapa 615. Dependiendo de la realización, el centro 180 central de USIM puede transmitir además al menos uno de los valores de seguridad, ID de PLMN, tipo de red, valor de verificación del centro central de seguridad (centro Sec-Central) e información de ubicación de UE (loc.). El valor de verificación del centro Sec-Central se utiliza para la autenticación mutua y la seguridad entre el centro 180 central de USIM y el centro 191 de USIM. Es decir, el valor de verificación del centro central de seguridad se utiliza para verificar el centro 180 central de USIM en el centro 191 de USIM. En el caso de utilizar el sistema PKI para la verificación, el valor de verificación del centro central secundario puede ser un valor que incluye la clave pública/clave secreta. En el caso de utilizar un procedimiento para la autenticación mutua, el valor de verificación del centro Sec-central puede ser un número aleatorio cifrado y descifrado con una clave compartida para la transmisión. En el caso de utilizar el procedimiento AKA, el valor de verificación del centro central secundario puede ser el valor de la señal de autenticación. Se pueden usar varios valores como el valor de verificación del centro de Seg-central, y en el presente documento se omite la descripción detallada del procedimiento de autenticación mutua.

Al recibir el parámetro, el centro 191 USIM verifica el valor de verificación del centro de Seg-central en la etapa 617.

El centro 191 USIM puede generar una clave de seguridad en la etapa 619. Esto corresponde a una realización (caso 1) en la que el centro 191 de USIM genera y distribuye la clave de seguridad. Según otra realización (caso 2), el centro 191 de USIM no tiene función de generación de seguridad. En esta realización, el AUC/HSS/HLR 121 es responsable de la función correspondiente. Es decir, el AUC/HSS/HLR 121 genera la clave de seguridad que puede usarse como la clave maestra (clave raíz) asignada al operador correspondiente en sí mismo. Según otra realización (caso 3), el centro 191 de USIM genera la clave de seguridad para el operador y el operador usa esta clave como semilla para generar la clave maestra de seguridad como clave reforzada específica del operador. Es decir, el centro 191 de USIM genera la clave de seguridad. El AUC/HSS/HLR 121 de la red del operador genera otra clave maestra derivada (Kdm) que funciona como el papel del maestro utilizado en la red del operador utilizando la clave de seguridad como semilla. La clave maestra puede ser la clave raíz como clave de seguridad o la clave maestra derivada (Kdm). Sobre la base de dicha clave maestra, la red del operador genera la clave de autenticación (KASME). La red del operador genera una clave de integridad NAS (KNASint) y una clave de cifrado NAS (KNASenc).

El centro 191 de USIM determina la MME al que se ha conectado el UE o el MSC conectado a la MME al que se ha conectado el UE u otra MME o MSC para proporcionar al UE el servicio de provisión de información inicial en la etapa 619-2. El centro 191 de USIM puede usar al menos una ID de PLMN, información de ubicación de UE e información de red conectada al UE para hacer tal determinación. En esta realización, la MME al que se ha conectado el UE 110 y el MSC conectado a la MME correspondiente proporciona al UE 110 el servicio de provisión de información inicial. Sin embargo, este procedimiento puede modificarse de varias maneras. Es decir, dicho procedimiento de selección se puede modificar de varias maneras dependiendo de si el operador proporciona el servicio al operador de red al que se ha conectado el UE.

A continuación, el centro 191 de USIM puede determinar una lista de identidad (ID) de áreas de seguimiento (área de registro de ubicación de UE) en la etapa 619-3. La MME puede utilizar el área de seguimiento para seleccionar el eNB para la entrega del servicio de provisión de información inicial. La lista de ID de TA se envía en el procedimiento después de la etapa 637 o 639. La MME puede seleccionarse por el centro 191 de USIM. En cierto caso, sin embargo, el servidor 182-2 central OTA puede ser responsable de la función que se describe con referencia a las etapas 637-2 y 637-3 que se describen a continuación.

En una realización (caso 1), si el centro 191 de USIM genera y almacena la clave de seguridad en la etapa 619, envía la MME 114 de la red del operador al que el UE 110 tiene la intención de suscribir al menos uno de MID como UE o USIM/Identificador UICC/SIM, valor de seguridad, ID PLMN y tipo de red. Después, la MME 114 envía al HSS/HLR 121 el valor MID y de seguridad en la etapa 623. Si el centro 191 de USIM genera la clave de seguridad, la MME también puede enviar al HSS/HLR 121 la clave de seguridad. El AUC/HSS/HLR 121 genera y almacena el IMSI como el identificador del UE 110 en la etapa 625. Si el centro 191 de USIM no ha generado la clave de seguridad en la etapa 619, el AUC/HSS/HLR 121 genera y almacena la clave de seguridad de acuerdo con otra realización (caso 2). El AUC/HSS/HLR 121 puede generar y almacenar el número de red digital de servicios integrados internacionales de

estación móvil (MSI SDN) necesario para la comunicación en una red CS en la etapa 625. En este caso, dado que el MSISDN generado en la etapa 613-15 se usa para transmitir información para la provisión de información al UE 110 y el MSISDN asignado en la etapa 625 se usa como el identificador para su uso en la nueva red del UE, son diferentes entre sí en la propiedad. Según otra realización, aunque en una red de operador diferente, el MSISDN para su uso en la transmisión de información para la provisión de información al UE 110 y el MSISDN para su uso en la nueva red pueden establecerse en el mismo valor. A diferencia del ejemplo anterior (caso 1), el AUC/HSS/HLR 121 genera la seguridad en otra realización (caso 2). En otra realización más (caso 3), se genera una clave maestra (clave maestra derivada) utilizando la clave de seguridad enviada por el centro 191 de USIM como una semilla, utilizándose la clave maestra derivada (Kdm) como clave maestra de seguridad. En el caso 1, la clave de seguridad transmitida almacenada en las etapas 627, 629 y 636 es la clave de seguridad generada por el centro 191 de USIM. En el caso 2, la clave de seguridad transmitida y almacenada en las etapas 627, 629 y 636 es la clave generada por el AUC/HSS/HLR 121. En el caso 3, la clave de seguridad transmitida y almacenada en las etapas 627, 629 y 636 es la clave maestra de seguridad derivada usando la clave recibida del centro 191 de USIM como semilla.

El AUC/HSS/HLR 121 envía al MME 114 el MID en la etapa 627. Dependiendo de la realización, el AUC/HSS/HLR 121 puede enviar además a la MME 114 el IMSI, la clave de seguridad (caso 2)/clave maestra de seguridad (caso 3) e información de perfil. El perfil es la información necesaria para configurar el UE 110 o USIM/UICC/SIM para que se ajuste a la red del operador correspondiente. El perfil puede incluir al menos un algoritmo de kilometraje que representa la función de seguridad en AKA, algoritmo de seguridad de cifrado SNOW (cifrado de corriente: un nuevo cifrado de corriente de palabra)/integridad, algoritmo de seguridad de protección de cifrado estándar de cifrado avanzado/integridad. El perfil también puede incluir al menos uno de la clase de control de acceso, códigos de llamadas de emergencia, lista PLMN y dominio de la red doméstica.

El MME 114 envía al centro 191 de USIM el MID en la etapa 629. Dependiendo de la realización, la MME 114 envía al centro 191 de USIM al menos uno de IMSI, información de perfil de clave de seguridad (caso 2)/clave maestra de seguridad (caso 3) y valor de seguridad.

El centro 191 de USIM envía al centro 180 central de USIM el MID en la etapa 631. Dependiendo de la realización, el centro 191 de USIM puede enviar al centro 180 central de USIM el valor de verificación del centro de USIM (valor de verificación del centro Sec-USIM). El valor de verificación del centro Sec-USIM se utiliza para la autenticación mutua y la seguridad entre el centro 180 central de USIM y el centro 191 de USIM. Es decir, el valor de verificación del centro Sec-USIM se utiliza para verificar el centro 191 de USIM en el centro 180 central de USIM. A través de esto, es posible notificar que la solicitud al UE 110 correspondiente al MID transmitido desde el centro 180 central de USIM al centro de USIM se ha procesado con éxito. Además, la autenticación mutua se puede realizar entre el centro central de USIM y el centro 191 de USIM.

Al recibir el parámetro, el centro 180 central de USIM verifica el valor de verificación del centro Sec-USIM en la etapa 633. En el caso de utilizar el sistema PKI para verificar el valor de verificación del centro Sec-USIM en la etapa 633, el valor puede incluir la clave pública/clave secreta. En el caso de utilizar el procedimiento para la autenticación mutua, el valor de verificación del centro de claves Sec-USIM puede ser un valor aleatorio que se cifra y descifra con una clave compartida. En el caso de utilizar el esquema AKA, el valor de verificación del centro Sec-USIM puede ser un valor de señal de autenticación. Se pueden usar varios valores como el valor de verificación del centro de Seg-central, y en el presente documento se omite la descripción detallada del procedimiento de autenticación mutua.

El centro 180 central de USIM envía al centro 191 de USIM un mensaje de confirmación en la etapa 635. El mensaje de confirmación se utiliza para notificar que el centro 191 de USIM ha procesado la solicitud del centro 180 central de USIM con éxito. El mensaje de confirmación también puede notificar el éxito de la autenticación mutua. En el caso 2 o 3, dado que la clave de seguridad o el valor de la clave maestra de seguridad se genera o modifica en el AUC/HSS/HLR 121 en la etapa 636, el centro 191 de USIM puede almacenar el valor de la clave de seguridad/clave maestra de seguridad. Si el centro 191 de USIM es responsable de almacenar la información de seguridad asignada por el operador en asociación con MID, el centro 191 de USIM puede almacenar el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil.

Posteriormente, el centro 191 de USIM puede enviar el servidor 182-2 central OTA al MID en la etapa 637. Dependiendo de la realización, el centro 191 de USIM puede enviar además al servidor 182-2 central OTA al menos uno de los valores de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil. En el caso de que la información de la lista de ID de TA se determine en la etapa 619-3, el centro 191 de USIM envía al servidor 182-2 central OTA la lista de ID de TA.

Si el centro 191 de USIM no ha seleccionado ningún MME para proporcionar información inicial en las etapas 619-2 y 619-3 o si el servidor 182-2 central OTA es capaz de seleccionar MME, el servidor 182-2 central OTA puede seleccionar un MME en las etapas 637-2 y 637-3. Es decir, el servidor 182 OTA puede seleccionar la MME a la que se ha conectado el UE o el MSC conectado a la MME a la que se ha conectado el UE utilizando al menos una ID de PLMN, información de ubicación de UE e información de red conectada a UE. El servidor 182-2 OTA central puede determinar la MME o el MSC para proporcionar el UE dentro del servicio de provisión de información inicial utilizando la información descrita anteriormente. Esta realización ha ejemplificado el caso en el que la MME al que se ha conectado el UE y el MCS conectado a la MME correspondiente entrega el servicio de provisión de información inicial

al UE. Sin embargo, este procedimiento puede modificarse de varias maneras. Es decir, el procedimiento de selección realizado modificado de varias maneras dependiendo de si el UE es servido por el operador de red conectado u otro operador. El servidor 182-2 OTA central puede determinar la información tal como la lista de identidad del área de seguimiento (lista de ID de TA) en la etapa 637-3. El área de seguimiento se utiliza para que la MME determine el eNB para la entrega del servicio de provisión de información inicial. Dicha información puede transmitirse a través del procedimiento que sigue a la etapa 639.

El servidor 182-2 OTA central puede enviar el centro 184-2 de servicio de mensajes cortos (SMSC-VNO) al MID en la etapa 639. Dependiendo de la realización, el servidor 182-2 OTA central puede enviar además el SMSC-VNO 184-2 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil. En cualquier caso, el servidor 182-2 OTA central puede enviar la lista de ID de TA al SMSC-VNO 184-2.

En el procedimiento de las etapas 639-2 a 641-2, el SMSC-VNO 184-2 puede enviar al UE 110 el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA. El procedimiento de las etapas 639-2 a 641-2 se divide en varios procedimientos. De acuerdo con los procedimientos, el SMSC-VNO 184-2 envía al MSC-VNO 188-2 el MID, el valor de seguridad, el IMSI, la clave de seguridad, el perfil y otros parámetros. Si la red como objetivo del UE 110 es una red de servicio de datos de circuito conmutado (CS), la información y los parámetros relacionados se entregan al UE 110 a través del MSC-VNO 188-2. De lo contrario, si la red como objetivo del UE 110 es una red de servicio de datos con conmutación de paquetes (PS), la información y los parámetros relacionados se entregan al UE 110 a través de SMSC-VNO 184-2, MSC-VNO 188-2 y MME-VNO 115.

El procedimiento detallado es el siguiente.

Las etapas 239-2 a 239-5 pueden realizarse selectivamente.

El SMSC-VNO 184-2 envía el GMSC-VNO 187-2 el MID en la etapa 639-2. Según una realización, el SMSC-VNO 184-2 puede enviar además el GM-SC-VNO 187-2 al menos uno de los valores de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA. Posteriormente, el GMSC-VNO 187 envía el HSS-VNO 121-2 al MSISDN en la etapa 639-3. El GMSC-VNO 187-2 recibe la dirección MSC (MSCA) desde el HSS-VNO 121-2. Posteriormente, el GSMC-VNO 187-2 envía el MCS-VNO 188-2 al MID en la etapa 639-5. Dependiendo de la realización, el GSMC-VNO 187-2 puede enviar además el MSC-VNO 188-2 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA. A continuación, el MSC-VNO 188-2 envía la MME-VNO 115 al MID. Dependiendo de la realización, el MSC-VNO 188-2 transmite al menos uno de los valores de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA.

La MME-VNO 115 determina un eNB al que se reenvía la información recibida en la etapa 639-7. La MME-VNO 115 puede usar la lista de ID de TA recibida para hacer la determinación. En el caso de que se usen el eNB-VNO 113 y la MME-VNO 115 cuando el UE 110 se ha conectado a la red como en esta realización, la MME-VNO 115 selecciona el eNB-VNO 113 utilizado para la conexión con prioridad. La MME-VNO 115 envía al eNB-VNO 113 el valor MID y de seguridad en la etapa 641-1. El eNB-VNO 113 puede enviar al UE 110 el valor MID y de seguridad en la etapa 641-2.

El UE 110 es capaz de verificar si la información se recibe en respuesta a la solicitud que ha transmitido basándose en el valor de seguridad en la etapa 643.

Las etapas 643-2 y 643-3 pueden ejecutarse selectivamente.

El UE 110 puede notificar al eNB-VNO 113 que la verificación del valor de seguridad es exitosa en la etapa 643-2. El eNB-VNO 113 puede notificar a la MME-VNO 115 que la verificación del valor de seguridad es exitosa en el UE 110 en la etapa 643-3. El mensaje de notificación puede incluir MID. Después, la MME-VNO 115 puede enviar la MME-VNO 115 al MID en la etapa 643-5. Dependiendo de la realización, la MME-VNO 115 puede enviar el eNB-VNO 113 al menos uno de valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil, lista de ID de TA y MSISDN. Después, el eNB-VNO 113 envía al UE 110 al menos uno de los valores medios, IMSI, clave de seguridad/clave maestra de seguridad, perfil y MSISDN en la etapa 643-6. En este momento, se puede utilizar un procedimiento similar a la paginación.

Posteriormente, si se recibe la información anterior, el UE 110 almacena al menos uno de los perfiles, IMSI, clave de seguridad/clave maestra de seguridad y MSISDN en la etapa 645. El USIM 170 activa el procedimiento de conexión del UE a la ME 111. El UE 110 envía a la MME 114 el mensaje ATTAHC a través del eNB 112 en las etapas 649 y 651. El mensaje ADJUNTO puede incluir el IMSI como el identificador de UE. Después, la MME 114 envía al UE 110 un mensaje ACEPTACIÓN DE ADJUNTO a través del eNB 112 en las etapas 659 y 661. Dado que el procedimiento ADJUNTO es bien conocido, la descripción se dirige a una parte modificada en la presente invención en el presente documento.

Las figuras 9a y 9b son un diagrama de flujo que ilustra el procedimiento de provisión de información de acuerdo con una realización de la presente invención. Como la primera parte del procedimiento de las figuras 9a y 9b es similar a la parte correspondiente de las figuras 7a a 8b, la descripción se dirige principalmente a las diferentes partes de las etapas 739 a 742-6.

La MME-VNO 115 determina el eNB al que se reenvía la información recibida en la etapa 739-7. La MME-VNO 115 puede usar la lista de ID de TA recibida para esta determinación. Como en esta realización, si hay el eNB y la MME utilizados cuando se conecta a la red, la MME-VNO 115 determina el eNB correspondiente para reenviar la información recibida con prioridad. La MME-VNO 115 envía al eNB-VNO 113 el MID en la etapa 742-1. Dependiendo de la realización, la MME-VNO 115 puede enviar además al eNB-VNO 113 la indicación que notifica la transmisión de la información para el aprovisionamiento de información inicial, MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil, lista de ID de TA, y MSISDN. La indicación de la etapa 742-1 es un parámetro que puede usarse para indicar que se transmite la información de aprovisionamiento inicial, y puede modificarse dependiendo de si la MME-VNO 115 envía el mensaje que contiene información de aprovisionamiento inicial a los eNB conectados a la MME como la etapa 742-1 o eNB específico basado en la lista de TA.

El eNB-VNO 113 busca el UE 110 en el modo inactivo para recibir el mensaje de aprovisionamiento inicial en la etapa 742-2. El eNB-VNO 1130 puede enviar al UE 110 el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y MSISDN en el mensaje de información del sistema transmitido en la etapa 742-3. El UE 110 verifica si la información se recibe en respuesta a la solicitud que ha transmitido utilizando el valor de seguridad en la etapa 742-3-2.

El procedimiento de las etapas 742-4 y 742-5 puede realizarse selectivamente.

El UE 110 notifica al eNB-VNO 113 el éxito de la verificación del valor de seguridad en la etapa 742-4, y el eNB-VNO 113 notifica a la MME-VNO 115 que el éxito de la verificación del valor de seguridad en el UE 110 en la etapa 742-5. Cada mensaje de notificación puede incluir MID.

Las figuras 10a y 11b son diagramas de flujo que ilustra el procedimiento de provisión de información de acuerdo con una realización de la presente invención.

El UE 110 se enciende para solicitar información inicial. El UE 110 tiene que estar en el estado de encendido para el progreso del procedimiento incluso cuando no solicita la provisión de información directamente.

El usuario selecciona un operador a través de la interfaz de usuario del UE 110 en la etapa 800-1. Esto incluye las etapas de seleccionar un operador inicialmente después de comprar un UE o un USIM, notificar al operador correspondiente de una red de destino para su uso en la recepción del servicio e iniciar el procedimiento de provisión de información para recibir el servicio del operador. En este procedimiento, el usuario selecciona el operador a través de la interfaz de usuario del UE. En particular, esto se realiza a través de la ME 111 del UE, y el inicio de la provisión de información se realiza de tal manera que la ME 111, el USIM 170, la provisión de información que se activa en la etapa 800-1 y el USIM 170 envía una provisión a la ME 111 una respuesta de activación en la etapa 800-2. Particularmente en la etapa 800-2, el UE 110 lee la información a transmitir a través de la red desde el USIM 170 y se prepara para transmitir la información a la red. El UE 110 envía a la MME (aquí, MME-VNO de la red visitada) 115 el mensaje de solicitud de provisión de información a través del eNB (aquí, eNB-VNO de la red visitada) en las etapas 800-3 y 800-4. Aunque las figuras 10a a 12b de esta realización ejemplifican la facilidad cuando el UE 110 inicia el acceso a la red visitada, es posible intentar el acceso a través de la red doméstica de acuerdo con una combinación de las figuras 3 a 6b. En las etapas 800-3 y 800-4, el mensaje de solicitud de provisión de información se transmite al centro central de USIM a través del eNB-VNO 113 y la MME-VNO 115. Dado que el UE 110 aún no tiene información complementaria, como información de seguridad e identificador para recibir un servicio en la red de servicio correspondiente, puede acceder al centro central de USIM en un modo limitado. Por consiguiente, esta realización ejemplifica un caso en el que el UE 110 envía la información usando el eNB-VNO 113 y la MME-VNO 115 de una red de operador diferente de la red de operador a la que el UE 110 pretende suscribirse, es decir, la red visitada. En este caso, la red visitada ayuda al acceso a la red del UE de tal manera que la conexión al centro 180 central de USIM está en un estado muy limitado. Mientras tanto, el mensaje de solicitud de provisión de información puede incluir al menos una identidad móvil (MID), valor de seguridad, credencial de seguridad, identidad de red móvil terrestre pública (ID PLMN), tipo de red e información de ubicación de UE (loc.). El MID es el identificador para identificar el UE o USIM/SIM/UICC correspondiente en el centro central de USIM y asignado por el fabricante (proveedor) de USIM/SIM/UICC. El USIM/ISM/UICC se proporciona en forma de un módulo o tarjeta que contiene la información de autenticación del suscriptor capaz de identificar al suscriptor. La información de seguridad proporcionada junto con la información MID incluye el valor de seguridad y la credencial de seguridad. El valor de seguridad se usa para verificar si se comprueba si el mensaje recibido es un mensaje malicioso transmitido por un atacante u otro nodo no válido al comparar el valor de provisión de información recibido en respuesta al mensaje de solicitud de provisión de información con el valor transmitido, y verificar si es el valor válido como respuesta a la solicitud que ha transmitido. En consecuencia, varios valores de los algoritmos de seguridad, tales como la capacidad de seguridad o el número aleatorio generado por el UE, pueden usarse como el valor de seguridad.

Normalmente, la credencial de seguridad se compone de un par de clave pública y clave secreta y un certificado en el procedimiento de seguridad de infraestructura de clave pública (PKI). Sin embargo, en la presente invención, la credencial de seguridad es una expresión general sobre la información que puede utilizarse para la verificación del terminal válido utilizado en el centro 190 de autenticación del USIM, así como dicha información.

Si se usa el procedimiento PKI, el centro 190 de autenticación del USIM puede usar la credencial de seguridad para

autenticar el UE 110 o el USIM 170 que ha transmitido el valor de autenticación como un procedimiento usado en general. Se puede utilizar para autenticar nodos pares transmitidos el valor a través del protocolo de autenticación y acuerdo de clave (AKA) mutuamente. En este caso, el valor del vector utilizado en AKA puede ser la credencial de seguridad. En el caso de utilizar el procedimiento de autenticación con un número aleatorio y un valor clave, el valor aleatorio puede usarse como credencial de seguridad. Se pueden usar otras diversas tecnologías candidatas. En la siguiente realización, si hay alguna información de seguridad que el centro 190 de autenticación USIM puede usar para verificar el usuario válido, esto puede denominarse credencial de seguridad.

La ID de PLMN también se conoce como ID de red de servicio. Para que el suscriptor proporcione la información del país de la red del operador para la suscripción y la información de la red del operador al centro 191 USIM, el UE 110 puede enviar la información en la red que proporciona el servicio utilizando la ID de PLMN. El tipo de red es la información sobre el tipo de red que proporciona el servicio. El tipo de red puede ser la información sobre el tipo de red de los enlaces alámbricos/inalámbricos de la red del operador, como la red del sistema de paquetes evolucionado (EPS) como la red de acceso de radio terrestre UMTS evolucionada (EUTRAN), la red de acceso de radio terrestre UMTS (UTRAN), y red de acceso de radio GSM/EDGE (GERAN). Si el tipo de red se incluye en el mensaje de solicitud de provisión de información, el UE 110 puede usar uno de los diversos tipos de red proporcionados por el operador correspondiente de forma selectiva. Es decir, el UE 110 puede seleccionar el enlace alámbrico/inalámbrico para su uso al recibir el servicio. La información de ubicación del UE 110 puede usarse para determinar la MME 115 o el MSC 188-2 que proporciona al usuario el servicio o determinar el área de seguimiento que proporciona al usuario el servicio.

Posteriormente, al recibir el mensaje de solicitud de provisión del UE 110, la MME-VNO 115 envía al centro 180 central de USIM el mensaje de solicitud de verificación de provisión de información que incluye el MID, el valor de seguridad, la credencial de seguridad, el ID de PLMN, el tipo de red y la ubicación del UE información (loc.). Aunque la presente realización ejemplifica el caso en el que el UE 110 selecciona un operador al que tiene la intención de suscribirse y envía el mensaje de solicitud de provisión de información junto con el tipo de red para su uso en la recepción del servicio, si el operador al que el UE 110 tiene conectado es el operador al que el UE 110 pretende suscribirse, puede ser posible que la MME proporcione la información del tipo de red en la red a la que pertenece la MME en el mensaje de solicitud de verificación de provisión de información transmitido al centro central de USIM en la etapa 800-5 después de que el UE haya transmitido el mensaje de solicitud de provisión de información que no sea el momento en que el UE transmite el mensaje de solicitud de provisión de información como las etapas 800-3 y 800-4 en una realización alternativa. Aunque la MME puede proporcionar la información del tipo de red de la red visitada a la que se ha conectado el UE, incluso cuando la red a la que el UE 110 pretende suscribirse y la red a la que se ha conectado el UE al enviar el mensaje de solicitud de provisión de información pertenecen para diferentes operadores, esto puede estar restringido al caso en el que la red visitada del UE tiene la capacidad de verificar el tipo de tipo de red de la red doméstica del par mediante un acuerdo sobre el servicio con la red a la que el UE tiene la intención de suscribirse. El tipo de red puede ser la información sobre el tipo de red de los enlaces alámbricos/inalámbricos de la red del operador, como la red del sistema de paquetes evolucionado (EPS) como la red de acceso de radio terrestre UMTS evolucionada (EUTRAN), la red de acceso de radio terrestre UMTS (UTRAN), y red de acceso de radio GSM/EDGE (GERAN). Es decir, en la realización alternativa, el tipo de red se envía al centro 180 central de USIM junto con el MID, el valor de seguridad, la credencial de seguridad y el ID de PLMN.

La etapa 801 es un proceso para transmitir un mensaje de solicitud de provisión de información o iniciar la provisión de información utilizando un dispositivo de procesamiento de información capaz de conectarse a Internet, tal como un ordenador y una red, para ejecutar el procedimiento de provisión de información para el UE 110. La solicitud de provisión de información incluye el MID, el valor de seguridad, la credencial de seguridad, el ID de PLMN, el tipo de red y la información de ubicación del UE (loc.) para proporcionar al UE la información necesaria para que el UE conecte una red de operador.

Según otra realización, para la conexión inicial basada en PC, el MID puede reemplazarse con un ID de provisión. El fabricante (proveedor) del UE 110 o USIM/SIM/UICC 170 asigna la identificación de la provisión. Dado que el MID es información de seguridad importante, se transmite desde el UE a la red y, cuando es necesario ingresar la información relacionada con el UE al PC, se usa el ID de provisión en lugar del MID para evitar que se ingrese el MID al PC 186. El ID de provisión se puede usar en las etapas 810 a 801-4 en lugar del MID. Es decir, el usuario ingresa el ID de provisión del UE 110 al PC 186, y el sistema identifica el UE 110 y la entrada basado en el ID de provisión. El ID de provisión del UE 110 puede transmitirse independientemente del MID en las etapas 800-3 a 800-5. El centro 180 central de USIM es capaz de integrar la solicitud de verificación de provisión de información de la etapa 800-5 y la solicitud de provisión de información de la etapa 800-4 para sincronizar la información en la etapa 811 y continuar los procedimientos posteriores.

En particular, los parámetros antes mencionados son los valores únicos del UE o las informaciones necesarias para que el UE opere en la red del operador y, por lo tanto, se requiere ingresar los valores correspondientes con precisión utilizando el procedimiento capaz de leer los valores establecidos inicialmente en el UE 110. En una realización, para leer los valores establecidos en el UE 110, el fabricante del UE o USIM proporciona una interfaz o aplicación capaz de manejar los parámetros correspondientes en el dispositivo de información. Es decir, el programa de aplicación correspondiente es capaz de leer la información del USIM y preparar la transmisión de la información a través de la red. La información de ubicación del UE puede usarse para determinar la MME 114 y el MSC 188 que proporcionan el servicio y el área de seguimiento para recibir el servicio. En el caso de la información de ubicación del UE, dado que

la ubicación de provisión de información inicial es la ubicación en la que se enciende el UE debido a la ejecución de la aplicación, el UE proporciona la información de ubicación en el lugar en el que se enciende el UE de tal manera que es posible si el UE funciona. Es decir, puede ser una forma de solicitar la información inicial para su uso en el UE después de que el UE se enciende.

Esta etapa corresponde al estado en el que el UE 110 no tiene información complementaria, como información de seguridad e identificador para su uso en la recepción del servicio en la red del operador correspondiente y, dado que la solicitud hace que otro dispositivo de información lea la información básica del UE 110 para conectarse al centro central de USIM a través de una red como Internet, el centro central de USIM también se encuentra en el estado permitiendo el acceso en modo limitado.

En una realización de la presente invención, la información se proporciona a través del procedimiento de activación de las etapas 800-1, 800-2, 800-3, 800-4 y 800-5 (en adelante, referido integralmente como 800-x) desde el UE y a través de Internet mediante el dispositivo de información representado por el PC. El procedimiento 800-x incluye un proceso en el que el UE se prepara para recibir información, y el UE transmite al menos uno de los MID del UE, valor de seguridad, credencial de seguridad, ID de PLMN, tipo de red e información de ubicación del UE (loc.) selectivamente como la información importante.

Al menos uno de los parámetros, incluida la identificación de PLMN, el tipo de red y la información de ubicación, puede transmitirse selectivamente por medio del PC 186 en las etapas 801-1, 801-2, 801-3 y 801-4 (en adelante, referido integralmente como 801-x). Además, la información se puede ingresar por medio del PC 186 con otro identificador que no sea MID en la etapa 801- x, la etapa 801-x para ingresar información por medio del PC se puede reemplazar por el procedimiento de asignación de un número o identificador único, es decir, el ID del dispositivo, para facilitar el acceso del usuario o del comprador del dispositivo y usar un número PIN para autenticar el dispositivo.

En una realización, en lugar de transmitir el mensaje de solicitud de provisión de información en la etapa 801, es posible enviar al centro 180 central de USIM el mensaje de solicitud de provisión de información a través del servidor 180-2 de control de admisión del centro central de USIM (servidor Adm del centro central de USIM) a través de tres etapas divididas de 801-2, 801-3 y 801-4. Sin embargo, hay un procedimiento para que el servidor Adm del centro 180-2 central de USIM verifique el UE válido. Esta es una realización del procedimiento de recibir solo la solicitud de aprovisionamiento inicial y verificar la solicitud realizada con un derecho válido asignado por el fabricante, tal como un MID válido para permitir el acceso al centro 180 central de USIM, sin aceptar la conexión directa al centro 180 central de USIM para proteger el servidor 180-2 de administración central de USIM de la denegación de distribución de adjunto de servicio (DDoS) como un ataque de piratería a un sitio específico mediante el control de una pluralidad de ordenadores para funcionar simultáneamente.

El mensaje de solicitud de provisión de información incluye al menos uno de identidad móvil (MID), valor de seguridad, credencial de seguridad, identificación de identidad de red móvil terrestre pública (PLMN) y tipo de red.

El MID es el identificador para su uso para identificar el UE 110 correspondiente o USIM/SIM/UICC 170 en el centro 180 central de USIM. El MID es asignado por el fabricante (proveedor) del UE 110, es decir, USIM/SIM/UICC 170, y el centro 180 central del USIM lo utiliza para identificar el UE 110. El USIM/SIM/UICC se proporciona en forma de un módulo o tarjeta que contiene la información de autenticación del suscriptor capaz de identificar al suscriptor.

El mensaje de solicitud de provisión de información puede incluir información de seguridad, así como el MID. Las informaciones de seguridad representativas son valores de seguridad y credenciales de seguridad.

El valor de seguridad se utiliza cuando se recibe un mensaje en respuesta al mensaje de solicitud de provisión de información. El UE 110 compara el valor de seguridad que ha transmitido y el mensaje recibido. A través de la comparación, es posible probar si el mensaje recibido es el mensaje malicioso enviado por un atacante o un nodo no válido. Es decir, el valor de seguridad se usa para verificar que el mensaje transmitido en respuesta a la solicitud ha sido transmitido. Se pueden usar varios valores capaces de autenticar el UE, como el valor del algoritmo de seguridad soportado por el UE, como la capacidad de seguridad o el número aleatorio generado por el UE 110 como el valor de seguridad.

Normalmente, la credencial de seguridad se compone de un par de clave pública y clave secreta y un certificado en el procedimiento de seguridad de infraestructura de clave pública (PKI). Sin embargo, en la presente invención, la credencial de seguridad es una expresión general sobre la información que puede utilizarse para la verificación del terminal válido utilizado en el centro 190 de autenticación del USIM, así como dicha información.

Si se usa el procedimiento PKI, el centro 190 de autenticación del USIM puede usar la credencial de seguridad para autenticar el UE 110 o el USIM 170 que ha transmitido el valor de autenticación como un procedimiento usado en general. Se puede utilizar para autenticar nodos pares transmitidos el valor a través del protocolo de autenticación y acuerdo de clave (AKA) mutuamente. En este caso, el valor del vector utilizado en AKA puede ser la credencial de seguridad. En el caso de utilizar el procedimiento de autenticación con un número aleatorio y un valor clave, el valor aleatorio puede usarse como credencial de seguridad. Se pueden usar otras diversas tecnologías candidatas. En la siguiente realización, si hay alguna información de seguridad que el centro 190 de autenticación USIM puede usar para verificar el usuario válido, esto puede denominarse credencial de seguridad.

La ID de PLMN también se conoce como ID de red de servicio. Para que el suscriptor proporcione la información del país de la red del operador para la suscripción y la información de la red del operador al centro 191 USIM, el UE 110 puede enviar la información en la red que proporciona el servicio utilizando la ID de PLMN. El tipo de red es la información sobre el tipo de red que proporciona el servicio. El tipo de red puede ser la información sobre el tipo de red de los enlaces alámbricos/inalámbricos de la red del operador, como la red del sistema de paquetes evolucionado (EPS) como la red de acceso de radio terrestre UMTS evolucionada (EUTRAN), la red de acceso de radio terrestre UMTS (UTRAN), y red de acceso de radio GSM/EDGE (GERAN). Si el tipo de red se incluye en el mensaje de solicitud de provisión de información, el UE 110 puede usar uno de los diversos tipos de red proporcionados por el operador correspondiente de forma selectiva. Es decir, el UE 110 puede seleccionar el enlace alámbrico/inalámbrico para su uso al recibir el servicio. La información de ubicación del UE 110 puede usarse para determinar la MME 114 o el MSC 188 que proporciona al usuario el servicio o determinar el área de seguimiento que proporciona al usuario el servicio.

El centro 180 central de USIM envía al centro 190 de autenticación de USIM el mensaje de solicitud de verificación de provisión de información en la etapa 811. Este mensaje puede incluir al menos uno de los MID, credenciales de seguridad, ID de PLMN y tipo de red. De esta manera, el centro 180 central de USIM solicita verificar si el MID correspondiente es de un usuario válido accesible para la red del operador utilizando la identidad y la credencial de seguridad. Se pueden usar varias credenciales de seguridad para verificar la solicitud de provisión de información.

Si el centro 190 de autenticación USIM y el UE 110 usan el sistema PKI, la clave pública y la clave de seguridad de PKI se usan como credenciales de seguridad. Es decir, el centro 190 de autenticación USIM verifica el UE 110 o USIM 170 que ha transmitido el valor de autenticación con las claves públicas y de seguridad. Se puede utilizar para autenticar nodos pares transmitidos el valor a través del protocolo de autenticación y acuerdo de clave (AKA) mutuamente. En este caso, el valor del vector utilizado en AKA puede ser la credencial de seguridad. En el caso de utilizar el procedimiento de autenticación con un número aleatorio y un valor clave, el valor aleatorio puede usarse como credencial de seguridad. Se pueden usar otras diversas tecnologías candidatas. En esta realización, si hay alguna información de seguridad que el centro 190 de autenticación USIM puede usar para verificar el usuario válido, esto puede denominarse credencial de seguridad. No se menciona un procedimiento detallado para usar la credencial de seguridad. Sin embargo, el centro 180 central de USIM envía al centro 190 de autenticación USIM el mensaje de solicitud de verificación de provisión de información y recibe el mensaje de respuesta de verificación de provisión de información en repetición en las etapas 811 y 813 como el procedimiento correspondiente. En este caso, el parámetro de seguridad denominado credencial de seguridad utilizado en las etapas 811 y 813 puede determinarse dependiendo de si se utiliza el esquema PKI o AKA. En cualquier caso, sin embargo, es posible verificar el acceso válido del UE 110 basado en la información proporcionada por el UE 110 tal como el parámetro de seguridad y la identidad llamada credencial de seguridad en las etapas 811 y 813. Los expertos en la materia pueden modificar este procedimiento de verificación de varias maneras. El centro 190 de autenticación USIM envía al centro central de USIM el mensaje de respuesta de autenticación de provisión de información en la etapa 813. El mensaje de respuesta de autenticación de provisión de información puede incluir MID para indicar la solicitud de autenticación de provisión de información correspondiente verificada con éxito. El procedimiento de las etapas 813-2 a 813-16 se realiza de forma selectiva.

Si el centro 190 de autenticación de USIM envía al centro 180 central de USIM un mensaje de respuesta en respuesta a la solicitud de verificación de provisión de información en la etapa 813, el centro 180 central de USIM envía a la MME-VNO 115 el mensaje de respuesta de provisión de información que incluye MID en la etapa 813-2. La MME-VNO 115 de la red visitada envía al MSC-VNO 188-2 un mensaje de solicitud de registro de ubicación en la etapa 813 después del procedimiento de verificación. Este mensaje incluye el identificador MID y/o MME. Después, el MSC 188-2 almacena el mapeo entre el MID y el identificador de MME en la etapa 813-12, y el MSC-VNO 188-2 envía al HSS-VNO 121-2 la dirección MID y MSC (MSCA) en la etapa 813-13. El HSS-VNO 121-2 almacena el mapeo del MID y el MSCA en la etapa 813-14 y genera MSISDN en la etapa 813-15. Aquí, el MSISDN generado para su uso para transmitir la información inicial como el identificador para usar en la comunicación a través de la red CS. MID, MSISDN y MSCA se transmiten al MSC-VNO 188-2 en la etapa 813-16.

Posteriormente, el centro 180 central de USIM envía al centro 191 de USIM al menos uno de los valores MID, valor de seguridad, ID de PLMN, tipo de red, valor de verificación del centro central de seguridad (en adelante, centro Sec-Central) para su uso en la verificación del centro central de USIM en el centro USIM para autenticación y seguridad mutua entre el centro 180 central de USIM y el centro 191 de USIM, y la información de ubicación de UE (loc.). El valor de verificación del centro central secundario puede ser un valor que incluye la clave pública/clave secreta en la verificación usando el sistema PKI, un número aleatorio cifrado y descifrado con una clave compartida al usar el procedimiento de autenticación mutua y un valor de señal de autenticación al usar el procedimiento AKA y el procedimiento detallado de la autenticación mutua se omite en el presente documento. Al recibir el parámetro, el centro 191 de USIM verifica el valor de verificación del centro de Seg-central en la etapa 817. El centro 191 de USIM genera la clave de seguridad en una realización (caso 1) en la que el centro USIM es responsable de generar y distribuir la clave de seguridad. En otra realización (caso 2) en la que el centro de USIM no tiene la función de generación de clave de seguridad, el Centro de Autenticación (AUC) puede ser responsable de la función correspondiente. Es decir, el AUC/HSS/HLR 121 es responsable de la función de generación de la clave de seguridad de modo que la clave de seguridad se pueda usar como la clave maestra (clave raíz) asignada al operador correspondiente en sí mismo. En otra realización más (caso 3), el centro de USIM genera la clave de seguridad que se utiliza como semilla para generar la clave maestra de seguridad que está reforzada por seguridad por operador. Es decir, la clave maestra derivada (Kdm) que funciona como la clave maestra en la red del operador se deriva de la clave de seguridad generada en el

centro de USIM en el AUC/HSS/HLR 121 de la red del operador. La clave maestra puede ser la clave raíz o la clave maestra derivada (Kdm) de la cual se deriva la clave de autenticación (KASME) para su uso en la red del operador después, la clave de autenticación se usa para generar la clave de cifrado NAS (KNASenc) de la clave de integridad NAS (KNASint).

El centro 191 de USIM determina la MME al que se ha conectado el UE o el MSC conectado a la MME al que se ha conectado el UE u otra MME o MSC para proporcionar al UE el servicio de provisión de información inicial utilizando el ID de PLMN, la información de ubicación del UE, e información sobre la red a la que se ha conectado el UE, en la etapa 819-2. Aunque esta realización ejemplifica el caso en el que la MME al que se ha conectado el UE y el MSC conectado a la MME correspondiente proporciona al UE el servicio de provisión de información inicial, esto puede modificarse de varias maneras. Es decir, dicho procedimiento de selección puede modificarse de varias maneras dependiendo de si el UE recibe el servicio de la red de operador conectada u otra red de operador. Posteriormente, el centro 191 de USIM puede determinar la lista de identidad del área de seguimiento (lista de ID de TA) para que la MME seleccione un eNB para proporcionar el servicio de provisión de información inicial en la etapa 819-3, y esta información se transmite en la etapa 837 u 839. La MME puede seleccionarse por el centro 191 de USIM o el servidor 182-2 OTA central y su descripción se hace con referencia a las etapas 837-2 y 837-3.

En una realización (caso 1), el centro de USIM genera y almacena la clave de seguridad en la etapa 819 y transmite el MID como el identificador del UE o USIM/UICC/SIM, valor de seguridad, ID de PLMN y tipo de red a la MME 114 de la red del operador a la que el UE pretende suscribirse en la etapa 821. Después, la MME 114 envía al HSS/HLR 121 el MID, el valor de seguridad y, si el centro de USIM ha generado la clave de seguridad, la clave de seguridad en la etapa 823. El AUC/HSS/HLR 121 genera y almacena el IMSI como el identificador de UE y, si el centro 191 de USIM no ha generado la clave de seguridad, la clave de seguridad según otra realización (caso 2) en la etapa 825. En la etapa 825, el AUC/HSS/HLR 121 también puede generar y almacenar el número de red digital de servicio integrado internacional de estación móvil (MSISDN) necesario para la comunicación en la red CS. Si la red a la que se ha conectado inicialmente el UE difiere de la red que proporcionará al UE el servicio son redes de operador diferentes, el MSISDN generado en la etapa 813-15 se usa para transmitir información sobre la provisión de información al UE mientras el MSISDN asignado en la etapa 825 es el identificador del UE para su uso en una nueva red, es decir, los dos MSISDN son de naturaleza diferente entre sí. En otra realización, aunque las dos redes son redes de operador diferentes, el MSISDN para su uso en la transmisión de información sobre la transmisión de información y el MSISDN que se utilizará en la red posteriormente pueden ser idénticos entre sí.

A diferencia del ejemplo anterior (caso 1), el AUC/HSS/HLR 121 genera la seguridad en otra realización (caso 2). En otra realización más (caso 3), se genera una clave maestra (clave maestra derivada) utilizando la clave de seguridad enviada por el centro 191 de USIM como una semilla, utilizándose la clave maestra derivada (Kdm) como clave maestra de seguridad. En el caso 1, la clave de seguridad transmitida almacenada en las etapas 827, 829 y 836 es la clave de seguridad generada por el centro 191 de USIM. En el caso 2, la clave de seguridad transmitida y almacenada en las etapas 827, 829 y 836 es la clave generada por el AUC/HSS/HLR 121. En el caso 3, la clave de seguridad transmitida y almacenada en las etapas 827, 829 y 836 es la clave maestra de seguridad derivada usando la clave recibida del centro 191 de USIM como semilla. El AUC/HSS/HLR 121 envía al MME 114 el MID en la etapa 827. Dependiendo de la realización, el AUC/HSS/HLR 121 puede enviar además a la MME 114 el IMSI, la clave de seguridad (caso 2)/clave maestra de seguridad (caso 3) e información de perfil. El perfil es la información necesaria para configurar el UE 110 o USIM/UICC/SIM para que se ajuste a la red del operador correspondiente. El perfil puede incluir al menos un algoritmo de kilometraje que representa la función de seguridad en AKA, algoritmo de seguridad de cifrado SNOW (cifrado de corriente: un nuevo cifrado de corriente de palabra)/integridad, algoritmo de seguridad de protección de cifrado estándar de cifrado avanzado/integridad. El perfil también puede incluir al menos uno de la clase de control de acceso, códigos de llamadas de emergencia, lista PLMN y dominio de la red doméstica.

El MME 114 envía al centro 191 de USIM la clave MID, IMSI y de seguridad (caso 2)/clave maestra de seguridad (caso 3), información de perfil y valor de seguridad en la etapa 629.

El centro 191 de USIM envía al centro 180 central de USIM el valor de verificación del centro de USIM y de seguridad (centro Sec-USIM) utilizado para verificar el centro USIM en el centro central de USIM para la autenticación y seguridad mutuas entre el centro 180 central de USIM y el centro 191 de USIM. Esta es la etapa de notificar que el centro de USIM ha procesado la solicitud del centro central de USIM para la solicitud de procesamiento para el UE que tiene el MID con éxito. El valor de verificación del centro central secundario puede ser un valor que incluye la clave pública/clave secreta en la verificación usando el sistema PKI, un número aleatorio cifrado y descifrado con una clave compartida al usar el procedimiento de autenticación mutua y un valor de señal de autenticación al usar el procedimiento AKA y el procedimiento detallado de la autenticación mutua se omite en el presente documento. Al recibir los parámetros, el centro 1809 central de USIM verifica el valor del centro Sec-USIM, el centro 180 central de USIM envía al centro 191 de USIM el mensaje de confirmación en la etapa 835, y este es el mensaje que notifica que el centro de USIM ha procesado la solicitud del centro central de USIM para que el UE tenga el MID con éxito. En el caso 2 o 3, dado que la clave de seguridad o el valor de la clave maestra de seguridad se genera o modifica en el AUC/HSS/HLR 121 en la etapa 836, el centro 191 de USIM puede almacenar el valor de la clave de seguridad/clave maestra de seguridad. Si el centro 191 de USIM es responsable de almacenar la información de seguridad asignada por el operador en asociación con MID, el centro 191 de USIM puede almacenar el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad y perfil. Mientras tanto, el centro 191 de USIM puede enviar a la MME

114 un mensaje de confirmación en la etapa 836-2, y la MME 1140 almacena el MID para verificar y controlar, cuando hay una solicitud de conexión para el UE correspondiente, el acceso del UE antes de verificar el HSS, la información almacenada se usa para que la MME 1140 verifique el MID para bloquear el acceso del UE 110 no válido antes de transmitir la solicitud de conexión del UE 110 al HSS para la verificación de IMSI como en la etapa 852.

Posteriormente, el centro 191 de USIM envía al servidor 182-2 OTA central el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y (cuando la información de la lista de ID de TA se determina en la etapa 819-3) la lista de ID de TA en la etapa 837.

Si el centro 191 de USIM no ha seleccionado ningún MME para proporcionar información inicial en las etapas 819-2 y 819-3 o si el servidor OTA central es capaz de seleccionar MME, el servidor OTA central puede seleccionar una MME en las etapas 837-2 y 837-3. Es decir, el servidor 182-2 OTA central puede seleccionar la MME a la que se ha conectado el UE o el MSC conectado a la MME a la que se ha conectado el UE utilizando al menos una ID de PLMN, información de ubicación de UE e información de red conectada a UE en la etapa 837-2. Aunque esta realización ejemplifica el caso en el que la MME a la que se ha conectado el UE y el MSC conectado a la MME al que se ha conectado el UE transmite el servicio de provisión de información inicial al UE, este procedimiento puede modificarse de varias maneras. Es decir, el procedimiento de selección puede modificarse de varias maneras dependiendo de si el UE es servido por el operador de red conectado u otro operador. El servidor 182-2 OTA central puede determinar la información tal como la lista de identidad del área de seguimiento (lista de ID de TA) en la etapa 837-3, y esta información se transmite en la etapa 839 y las etapas posteriores. El servidor 182-2 OTA central envía al centro 184-2 de servicio de mensajes cortos (SMSC) el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y, si es necesario, la lista de ID de TA en la etapa 839. El SMSC 184 envía al UE 110 el MID, el valor de seguridad, IMSI, la clave de seguridad/clave maestra de seguridad, el perfil y la lista de ID de TA en las etapas 839-2 a 841-2. El procedimiento de las etapas 839-2 a 841-2 se realiza de tal manera que el SMSC 184-2 transmite al MSC 188-2 la información y los parámetros (tal como MID, valor de seguridad, IMSI, clave de seguridad y perfil) y, si la red que proporciona el servicio al UE es una red de servicio de datos con conmutación de circuitos (CS), el MSC 188-2 entrega la información y los parámetros al UE 110 o, si la red que proporciona el servicio al UE es una red de servicio de datos de paquetes conmutados (PS), el MSC 188-2 reenvía la información y los parámetros a la MME 115 de modo que la MME 115 entrega la información y los parámetros al UE 110.

A continuación se realiza una descripción detallada de dicho procedimiento.

Las etapas 839-2 a 839-5 pueden realizarse selectivamente.

El SMSC 184-2 envía el GMSC 187-2 al menos uno de MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y lista de ID de TA en la etapa 639-2. Luego, el GMSC 187-2 solicita al HSS 121-2 la dirección MSC (MSCA) con MSISDN en la etapa 839-3 y recibe el MSCA en la etapa 839-4. Luego, si se encuentra el MSC basado en el MSCA en la etapa 839-4, el GSMC 187-2 envía al MSC 188-2 el MID, el valor de seguridad, el IMSI, la clave de seguridad/clave maestra de seguridad, el perfil y la lista de ID de TA. Posteriormente, el MSC 188-2 envía a la MME 115 el MID, el valor de seguridad, el IMSI, la clave de seguridad/clave maestra de seguridad, el perfil y la lista de ID de TA.

La MME 115 determina un eNB al que reenvía la información recibida utilizando la lista de ID de TA o tomando nota del eNB 113 y la MME 115 a la que se ha conectado el UE como en una realización de la presente invención en la etapa 839-7 y envía el eNB 113, el MID y el valor de seguridad en la etapa 841-1, y el eNB entrega la información al UE 110 en la etapa 841-2.

El UE 110 verifica la validez de la información recibida, es decir, si la información se recibe en respuesta a la solicitud que ha transmitido, utilizando el MID y el valor de seguridad en la etapa 843.

El procedimiento de las etapas 843-2 y 843-3 puede realizarse opcionalmente.

El UE 110 notifica al eNB 113 que el valor de seguridad se ha verificado con éxito en la etapa 843-2, y el eNB 112 notifica a la MME 115 que el UE 112 ha verificado el valor de seguridad con éxito en la etapa 843-3. Posteriormente, la MME 114 envía al eNB 112 el MID, el valor de seguridad, el IMSI, la clave de seguridad/clave maestra de seguridad, el perfil, la lista de ID de TA y el MSISDN en la etapa 843-5. El eNB 112 envía al UE 110 al menos uno de MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil, lista de ID de TA y MSISDN en la etapa 843-6, de manera similar a la paginación.

Al recibir la información, el UE 110 almacena al menos uno de MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil, lista de ID de TA y MSISDN en la etapa 845. El USIM 170 activa la ME 111 para realizar el procedimiento ADJUNTAR del UE en la etapa 847. El UE 110 envía a la MME 114 el mensaje ADJUNTAR que incluye el IMSI como el identificador del UE a través del eNB 112 en las etapas 849 y 851. La MME 114 envía al UE 110 un mensaje ACEPTACIÓN DE ADJUNTO a través del eNB 112 en las etapas 859 y 861. Dado que el procedimiento ADJUNTO es bien conocido, la descripción se dirige a una parte modificada en la presente invención en el presente documento.

Las figuras 12a y 12b son un diagrama de flujo que ilustra el procedimiento de provisión de información de acuerdo

con una realización de la presente invención.

Como la primera parte del procedimiento de las figuras 12a y 12b es idéntico o similar a la parte correspondiente de las figuras 10a a 11b, la descripción se dirige a una parte diferente de las etapas 939-7 a 942-6.

La MME 115 selecciona un eNB al que reenvía la información recibida utilizando la lista de ID de TA o tomando nota del eNB y la MME a la que se ha conectado el UE en la etapa 937-7.

La MME-VNO 115 envía al eNB-VNO 113 el MID, indicador de transmisión de información de aprovisionamiento inicial, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil, lista de ID de TA y MSISDN en la etapa 942-1. El indicador de la etapa 942-1 puede usarse como un parámetro que indica la transmisión de la información de aprovisionamiento inicial, y el procedimiento puede modificarse dependiendo de si la MME-VNO 115 envía el mensaje de indicación de información de aprovisionamiento inicial a los eNB conectados a la MME o un eNB específico basado en la lista de TA.

El eNB-VNO 113 busca el UE 110 en el modo inactivo para recibir el mensaje de aprovisionamiento inicial en la etapa 942-2. El eNB-VNO 113 transmite el MID, valor de seguridad, IMSI, clave de seguridad/clave maestra de seguridad, perfil y MSISDN al UE 110 en el mensaje de información del sistema transmitido en la etapa 942-3. El UE 110 verifica la validez de la información recibida, es decir, si la información se recibe en respuesta a la solicitud que ha transmitido utilizando el valor de seguridad en la etapa 942-3-2.

El procedimiento de las etapas 942-4 y 942-5 se realiza de forma selectiva.

El UE 110 notifica al eNB-VNO 113 la verificación exitosa del valor de seguridad en la etapa 942-4, y el eNB-VNO 113 notifica a la MME 115 que el UE 110 ha verificado el valor de seguridad con éxito en la etapa 942-5.

Los efectos logrados por la parte representativa de la invención desvelada que funciona como se describe anteriormente son los siguientes.

La presente invención se refiere al procedimiento y al sistema para aprovisionar el identificador de UE y los parámetros de seguridad utilizando estrato sin acceso (NAS) y otros protocolos en EUTRAN u otro entorno RAT (GERAN, UTRAN, etc.) de tal manera que el UE seleccione un operador y comunique la seguridad y otras informaciones en la red de comunicación móvil, configurando, en el UE, la operación usando el protocolo de acuerdo con la presente invención, asignando el identificador relacionado y los parámetros relacionados con la seguridad para la comunicación con el operador correspondiente para facilitar la autenticación de UE, la ejecución del comando del modo de seguridad y la comunicación, lo que resulta en una mejora de la eficiencia de la gestión de seguridad.

Aunque la descripción se ha hecho con referencia a realizaciones particulares, la presente invención se puede implementar con diversas modificaciones sin apartarse del ámbito de la presente invención. Por lo tanto, la presente invención no se limita a las realizaciones particulares desveladas, sino que se define por el conjunto de reivindicaciones adjuntas.

Se ha de apreciar que los expertos en la materia pueden cambiar o modificar las realizaciones sin alejarse del concepto técnico de la presente invención. Por consiguiente, debería entenderse que las realizaciones anteriormente descritas son esencialmente para el fin ilustrativo únicamente pero de ninguna manera para restricción a la misma. Por lo tanto el alcance de la invención debería determinarse por las reivindicaciones adjuntas en lugar de la memoria descriptiva, y diversas alteraciones y modificaciones dentro de la definición y ámbito de las reivindicaciones se incluyen en las reivindicaciones.

Aunque las realizaciones preferidas de la invención se han descrito utilizando términos específicos, la memoria descriptiva y los dibujos deben ser considerados a título ilustrativo en lugar de un sentido restrictivo con el fin de ayudar a comprender la presente invención.

REIVINDICACIONES

1. Un procedimiento para configurar un terminal de comunicación móvil realizado por el terminal de comunicación móvil, comprendiendo el procedimiento:

transmitir, por el terminal (10) de comunicación móvil, un mensaje de solicitud de provisión de información a una entidad de provisión de información, en el que el mensaje de solicitud de provisión de información comprende una identidad móvil del terminal (10) de comunicación móvil, un tipo de red, información de ubicación del terminal (10) de comunicación móvil, un valor de seguridad y una credencial de seguridad; y
recibir, por el terminal de comunicación móvil, información para su uso en conexión del terminal de comunicación móvil desde la entidad de provisión de información, en el que la información para la conexión del terminal (10) de comunicación móvil comprende un identificador único del terminal de comunicación móvil que comprende al menos uno de una identidad de suscriptor móvil internacional, IMSI, y un número de directorio de suscriptor internacional de estación móvil, MSISDN, y una primera clave de seguridad como clave maestra para su uso en la generación de una segunda clave de seguridad necesaria para que el terminal de comunicación móvil se conecte a un sistema de comunicación móvil, caracterizado porque
la información de ubicación incluida en el mensaje de solicitud de provisión de información se utiliza para determinar una entidad de gestión de movilidad, MME, un centro de conmutación móvil, MSC o un área de seguimiento que proporciona servicio al terminal de comunicación móvil,
en el que el valor de seguridad incluido en el mensaje de solicitud de provisión de información se utiliza por el terminal (10) de comunicación móvil para verificar que un mensaje recibido como respuesta al mensaje de solicitud de provisión de información transmitida se origina en un nodo fiable, y
en el que la credencial de seguridad incluida en el mensaje de solicitud de provisión de información se usa para verificar una validez del terminal (10) de comunicación móvil en un centro de autenticación de módulo de identidad de suscriptor universal, USIM.

2. El procedimiento de la reivindicación 1, en el que el mensaje de solicitud de provisión de información comprende además una identidad de red móvil terrestre pública, ID de PLMN, de la red del operador.

3. El procedimiento de la reivindicación 1, en el que la entidad de provisión de información se implementa en al menos uno de un centro central de USIM y un servidor de suscriptor doméstico, HSS.

4. El procedimiento de la reivindicación 1, en el que la entidad de provisión de información genera el identificador único del terminal de comunicación móvil y la primera clave de seguridad del terminal de comunicación móvil.

5. Un procedimiento para configurar un terminal de comunicación móvil realizado por una entidad de provisión de información, comprendiendo el procedimiento:

recibir, por la entidad de provisión de información desde el terminal (10) de comunicación móvil, un mensaje de solicitud de provisión de información, en el que el mensaje de solicitud de provisión de información comprende una identidad móvil del terminal (10) de comunicación móvil, un tipo de red, información de ubicación del terminal de comunicación móvil, un valor de seguridad y una credencial de seguridad;
generar, en la entidad de provisión de información, información para su uso en conexión con el terminal (10) de comunicación móvil; y
transmitir, por la entidad de provisión de información al terminal (10) de comunicación móvil, la información para su uso en conexión con el terminal (10) de comunicación móvil, en el que la información para su uso en conexión del terminal (10) de comunicación móvil comprende un identificador único del terminal de comunicación móvil que comprende al menos uno de una identidad de suscriptor móvil internacional, IMSI, y un número de directorio de suscriptor internacional de estación móvil, MSISDN, y una primera clave de seguridad como clave maestra para su uso en la generación de una segunda clave de seguridad necesaria para el terminal (10) de comunicación móvil para conectarse a un sistema de comunicación móvil, caracterizado porque
la información de ubicación incluida en el mensaje de solicitud de provisión de información se utiliza para determinar una entidad de gestión de movilidad, MME, un centro de conmutación móvil, MSC o un área de seguimiento que proporciona servicio al terminal de comunicación móvil,
en el que el valor de seguridad incluido en el mensaje de solicitud de provisión de información se utiliza por el terminal (10) de comunicación móvil para verificar que un mensaje recibido en respuesta al mensaje de solicitud de provisión de información transmitida se origina en un nodo fiable, y
en el que la credencial de seguridad incluida en el mensaje de solicitud de provisión de información se usa para verificar una validez del terminal (10) de comunicación móvil en un centro de autenticación de módulo de identidad de suscriptor universal, USIM.

6. El procedimiento de la reivindicación 5, en el que el mensaje de solicitud de provisión de información comprende además una identidad de red móvil terrestre pública, ID de PLMN.

7. El procedimiento de la reivindicación 5, en el que la entidad de provisión de información se implementa en al menos uno de un centro central de USIM y un servidor de suscriptor doméstico, HSS.

8. El procedimiento de la reivindicación 5, en el que la entidad de provisión de información genera el identificador único

del terminal de comunicación móvil y la primera clave de seguridad del terminal de comunicación móvil.

9. Un terminal de comunicación móvil, comprendiendo el terminal de comunicación móvil:

un transceptor; y
un controlador configurado para:

transmitir, a una entidad de provisión de información a través del transceptor, un mensaje de solicitud de provisión de información a una entidad de provisión de información, en el que el mensaje de solicitud de provisión de información comprende una identidad móvil del terminal (10) de comunicación móvil, un tipo de red, información de ubicación del terminal (10) de comunicación móvil, un valor de seguridad y una credencial de seguridad, y
recibir, desde la entidad de provisión de información a través del transceptor, información para su uso en conexión con el terminal (10) de comunicación móvil, en el que la información para la conexión del terminal (10) de comunicación móvil comprende un identificador único del terminal de comunicación móvil que comprende al menos uno de una identidad internacional de suscriptor móvil, IMSI, y un número de directorio internacional de suscriptor de estación móvil, MSISDN, y una primera clave de seguridad como clave maestra para su uso en la generación de una segunda clave de seguridad necesaria para que el terminal (10) de comunicación móvil se conecte a un sistema de comunicación móvil, caracterizado porque
la información de ubicación incluida en el mensaje de solicitud de provisión de información se utiliza para determinar una entidad de gestión de movilidad, MME, un centro de conmutación móvil, MSC o un área de seguimiento que proporciona servicio al terminal de comunicación móvil,
en el que el valor de seguridad incluido en el mensaje de solicitud de provisión de información se utiliza por el terminal (10) de comunicación móvil para verificar que un mensaje recibido en respuesta al mensaje de solicitud de provisión de información transmitida se origina en un nodo fiable, y
en el que la credencial de seguridad incluida en el mensaje de solicitud de provisión de información se usa para verificar una validez del terminal (10) de comunicación móvil en un centro de autenticación de módulo de identidad de suscriptor universal, USIM.

10. El terminal de comunicación móvil de la reivindicación 9, en el que el mensaje de solicitud de provisión de información comprende además una Identidad de red móvil terrestre pública, ID de PLMN, de la red del operador.

11. Una entidad de provisión de información para configurar un terminal de comunicación móvil, comprendiendo la entidad:

un transceptor; y
un controlador configurado para:

recibir, desde el terminal (10) de comunicación móvil a través del transceptor, un mensaje de solicitud de provisión de información, en el que el mensaje de solicitud de provisión de información comprende una identidad móvil del terminal (10) de comunicación móvil, un tipo de red, información de ubicación del terminal (10) de comunicación móvil, un valor de seguridad y una credencial de seguridad;
generar información para su uso en conexión con el terminal (10) de comunicación móvil, y
transmitir, al terminal (10) de comunicación móvil a través del transceptor, la información para usar en conexión con el terminal (10) de comunicación móvil, en el que la información para su uso en conexión del terminal (10) de comunicación móvil comprende un identificador único del terminal de comunicación móvil que comprende al menos uno de una identidad de suscriptor móvil internacional, IMSI, y un número de directorio de suscriptor internacional de estación móvil, MSISDN, y una primera clave de seguridad como clave maestra para su uso en la generación de una segunda clave de seguridad necesaria para el terminal de comunicación móvil se conecte a un sistema (10) de comunicación móvil, caracterizado porque
la información de ubicación incluida en el mensaje de solicitud de provisión de información se utiliza para determinar una entidad de gestión de movilidad, MME, un centro de conmutación móvil, MSC o un área de seguimiento que proporciona servicio al terminal de comunicación móvil,
en el que el valor de seguridad incluido en el mensaje de solicitud de provisión de información se utiliza por el terminal (10) de comunicación móvil para verificar que un mensaje recibido en respuesta al mensaje de solicitud de provisión de información transmitida se origina en un nodo fiable, y
en el que la credencial de seguridad incluida en el mensaje de solicitud de provisión de información se usa para verificar una validez del terminal (10) de comunicación móvil en un centro de autenticación de módulo de identidad de suscriptor universal, USIM.

FIG. 1

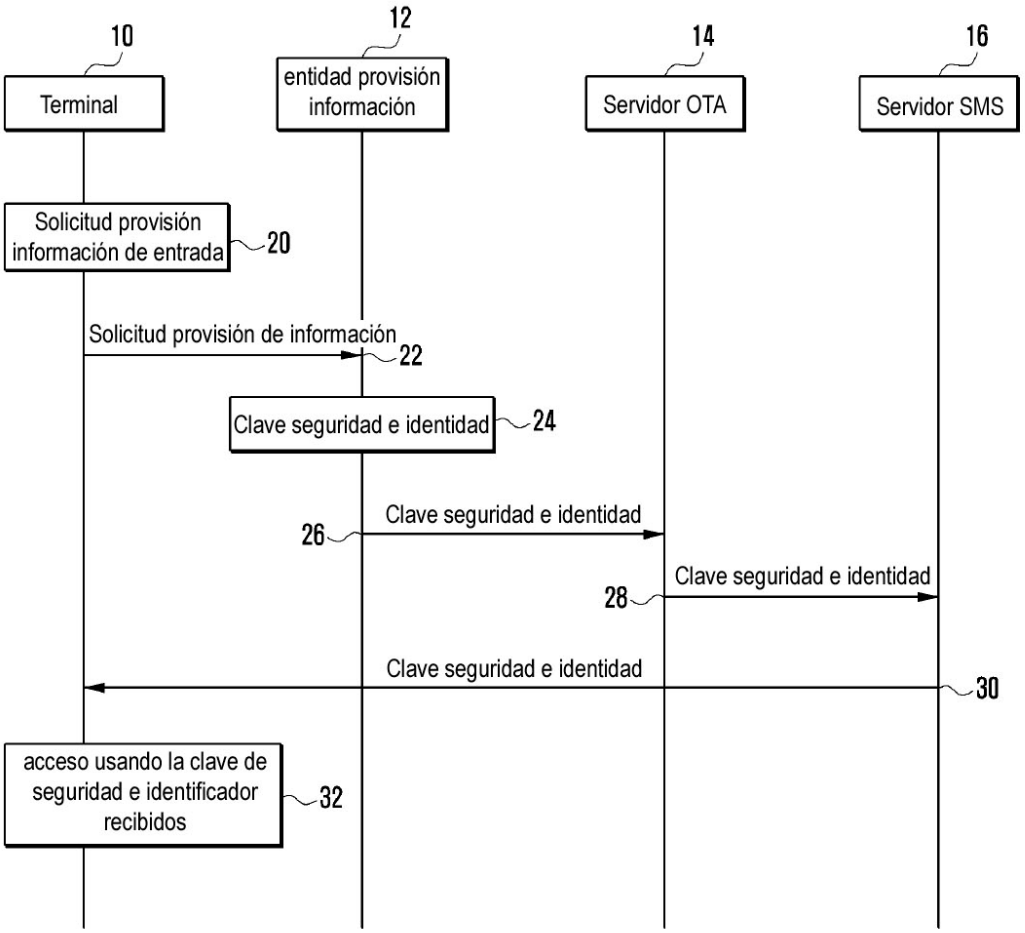

10
Terminal
12
entidad provisión información
14
Servidor OTA
16
Servidor SMS
Solicitud provisión información de entrada
20
Solicitud provisión de información
22
Clave seguridad e identidad
24
Clave seguridad e identidad
26
Clave seguridad e identidad
28
Clave seguridad e identidad
30
acceso usando la clave de seguridad e identificador recibidos
32

FIG. 2

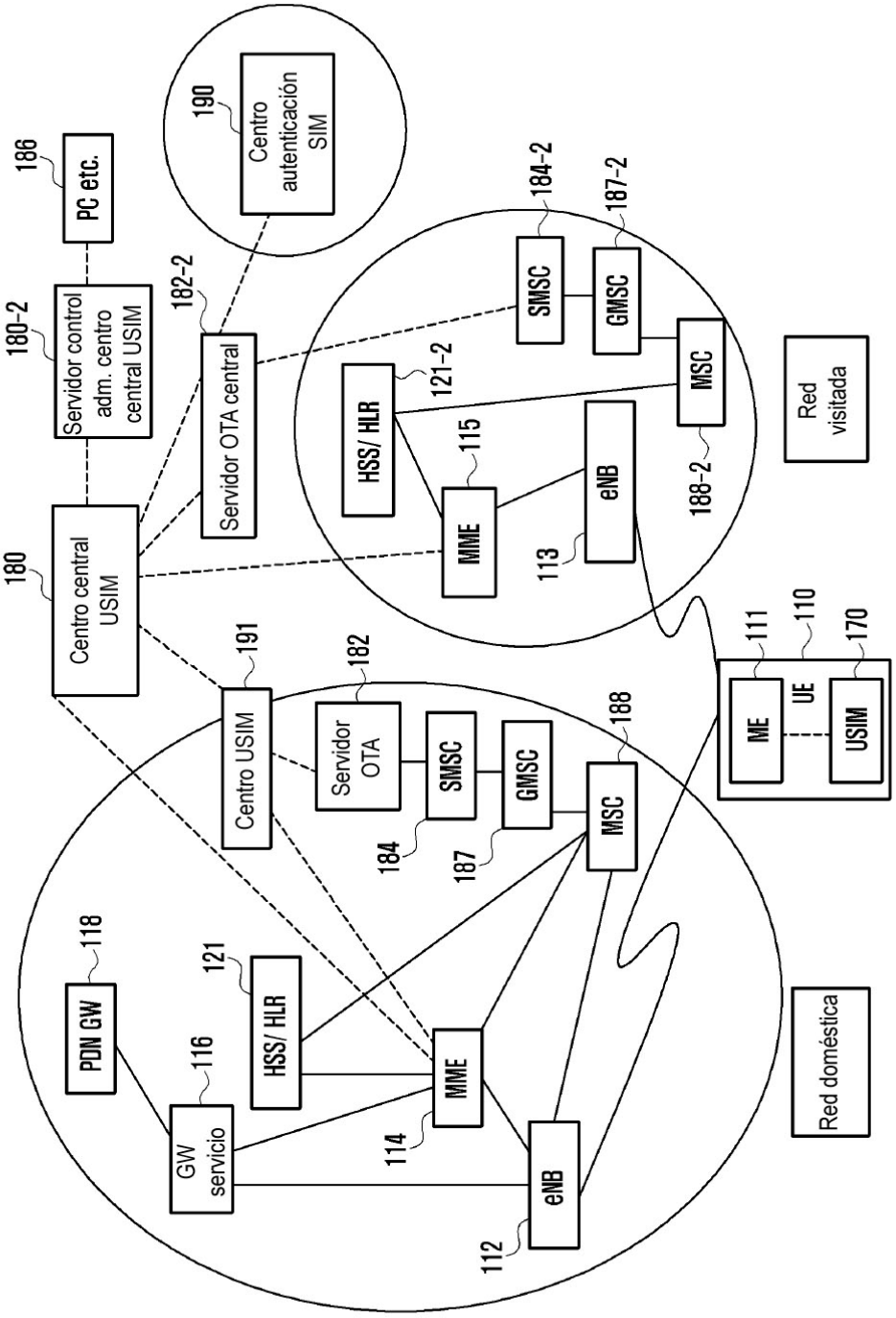

190
Centro autenticación SIM
186
PC etc.
180-2
Servidor control adm. centro central USIM
182-2
Servidor OTA central
180
Centro central USIM
184-2
SMSC
187-2
GMSC
MSC
188-2
121-2
HSS/ HLR
115
MME
113
eNB
Red visitada
191
Centro USIM
182
Servidor OTA
SMSC
GMSC
MSC
184
187
188
111
ME
110
UE
170
USIM
118
PDN GW
121
HSS/ HLR
116
GW servicio
MME
114
eNB
112
Red doméstica

FIG. 3

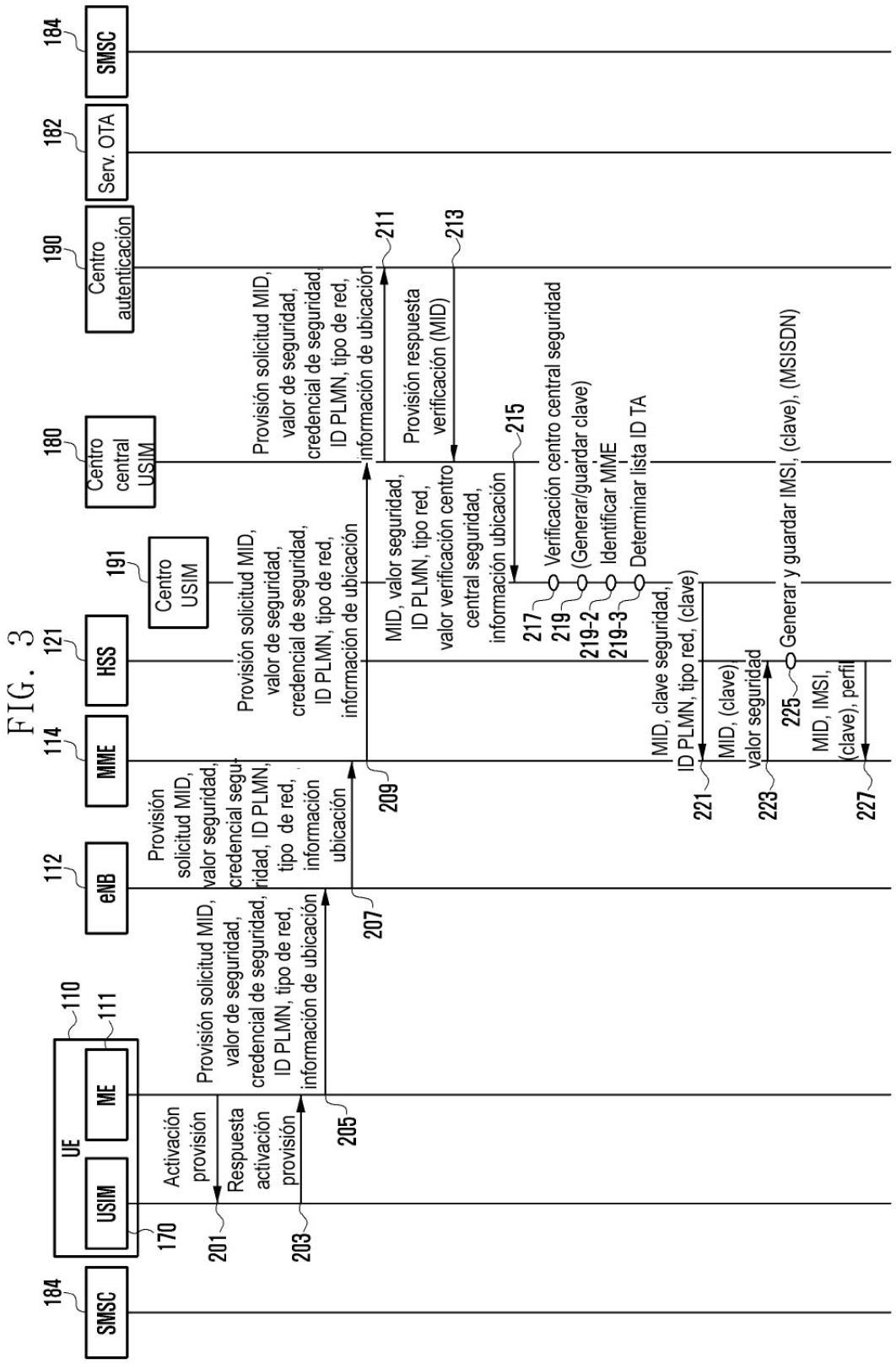

UE
USIM
ME
110
111
170
eNB
112
MME
114
HSS
121
Centro USIM
191
Centro central USIM
180
Centro autenticación
190
Serv. OTA
182
SMSC
184
Activación provisión
201
Respuesta activación provisión
203
Provisión solicitud MID, valor de seguridad, credencial de seguridad, ID PLMN, tipo de red, información de ubicación
205
Provisión solicitud MID, valor seguridad, credencial seguridad, ID PLMN, tipo de red, información ubicación
207
Provisión solicitud MID, valor de seguridad, credencial de seguridad, ID PLMN, tipo de red, información de ubicación
209
Provisión solicitud MID, valor de seguridad, credencial de seguridad, ID PLMN, tipo de red, información de ubicación
211
Provisión respuesta verificación (MID)
213
MID, valor seguridad, ID PLMN, tipo red, valor verificación centro central seguridad, información ubicación
215
217 Verificación centro central seguridad
219 (Generar/guardar clave)
219-2 Identificar MME
219-3 Determinar lista ID TA
MID, clave seguridad, ID PLMN, tipo red, (clave)
221
MID, (clave), valor seguridad
223
225 Generar y guardar IMSI, (clave), (MSISDN)
MID, IMSI, (clave), perfil
227

FIG. 4A

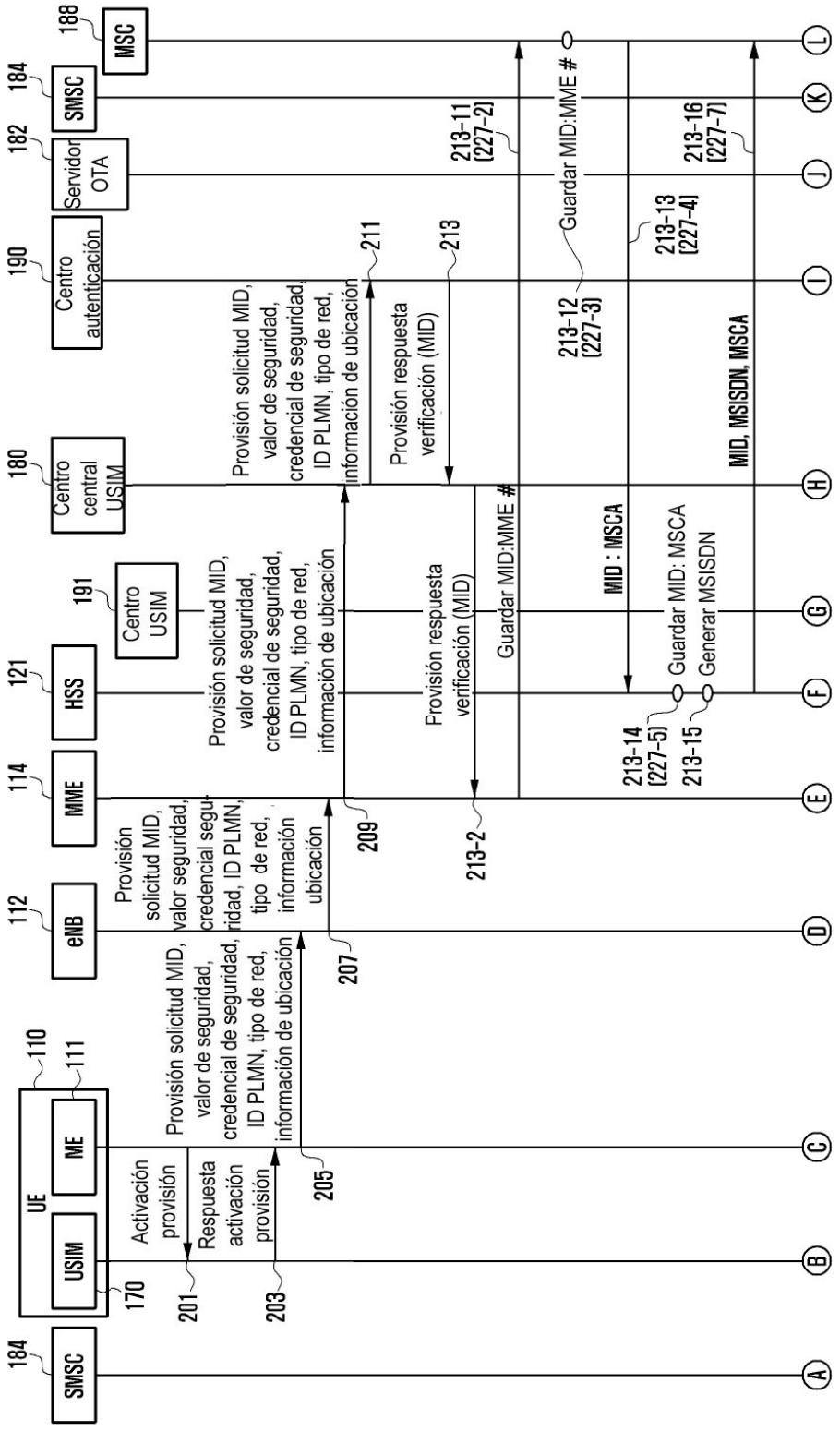

UE
USIM
ME
110
111
170
184
SMSC
112
eNB
114
MME
121
HSS
191
Centro USIM
180
Centro central USIM
190
Centro autenticación
182
Servidor OTA
184
SMSC
188
MSC
Activación provisión
Respuesta activación provisión
Provisión solicitud MID, valor de seguridad, credencial de seguridad, ID PLMN, tipo de red, información de ubicación
Provisión solicitud MID, valor seguridad, credencial seguridad, ID PLMN, tipo de red, información ubicación
Provisión solicitud MID, valor de seguridad, credencial de seguridad, ID PLMN, tipo de red, información de ubicación
Provisión respuesta verificación (MID)
Guardar MID:MME #
MID : MSCA
Guardar MID: MSCA
Generar MSISDN
MID, MSISDN, MSCA
201
203
205
207
209
211
213
213-2
213-11 [227-2]
213-12 [227-3]
213-13 [227-4]
213-14 [227-5]
213-15
213-16 [227-7]
A
B
C
D
E
F
G
H
I
J
K
L

FIG. 4B

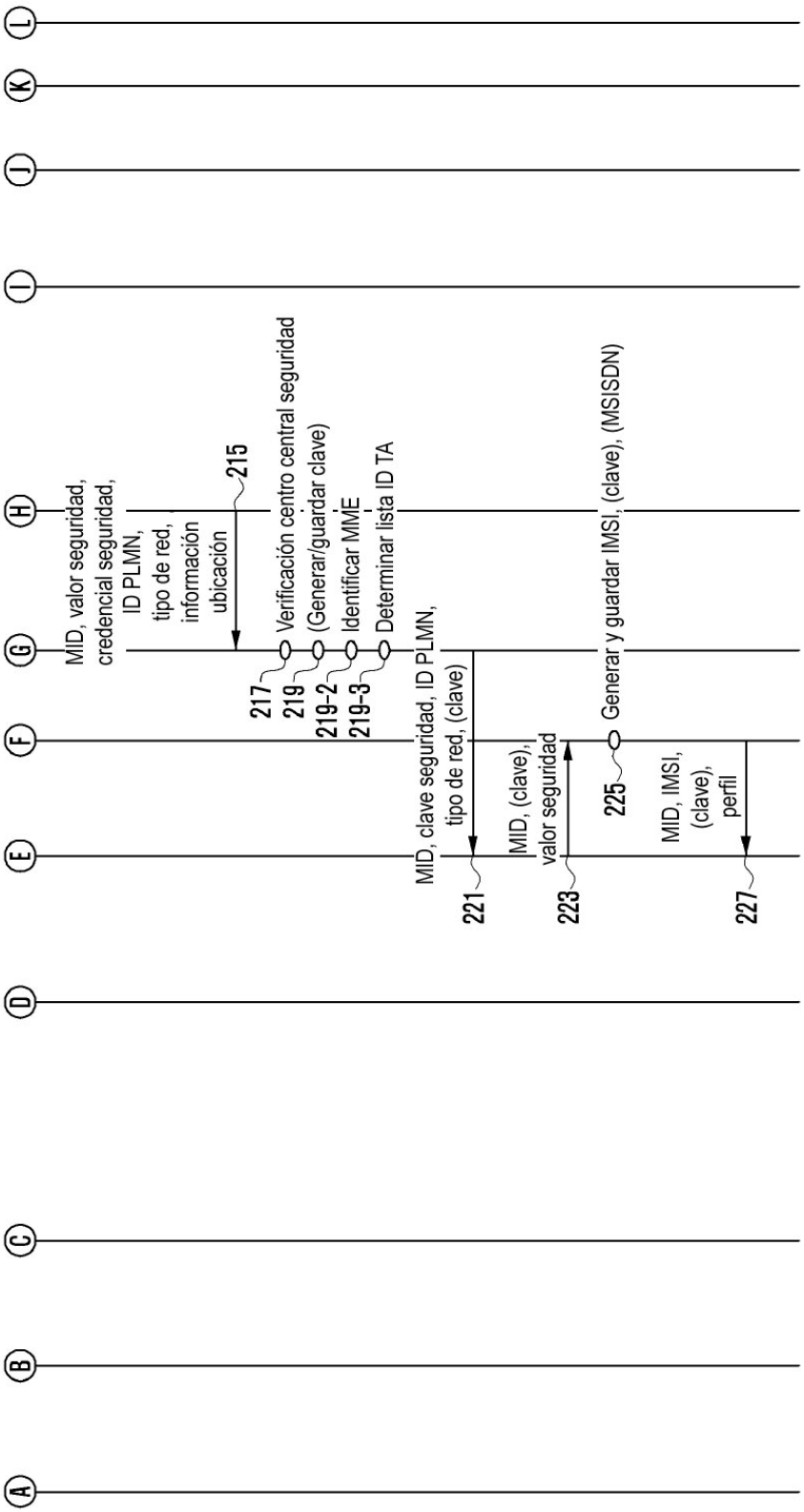

A
B
C
D
E
F
G
H
I
J
K
L
MID, valor seguridad, credencial seguridad, ID PLMN, tipo de red, información ubicación
215
Verificación centro central seguridad
(Generar/guardar clave)
Identificar MME
Determinar lista ID TA
217
219
219-2
219-3
MID, clave seguridad, ID PLMN, tipo de red, (clave)
221
MID, (clave), valor seguridad
223
Generar y guardar IMSI, (clave), (MSISDN)
225
MID, IMSI, (clave), perfil
227

FIG. 5A

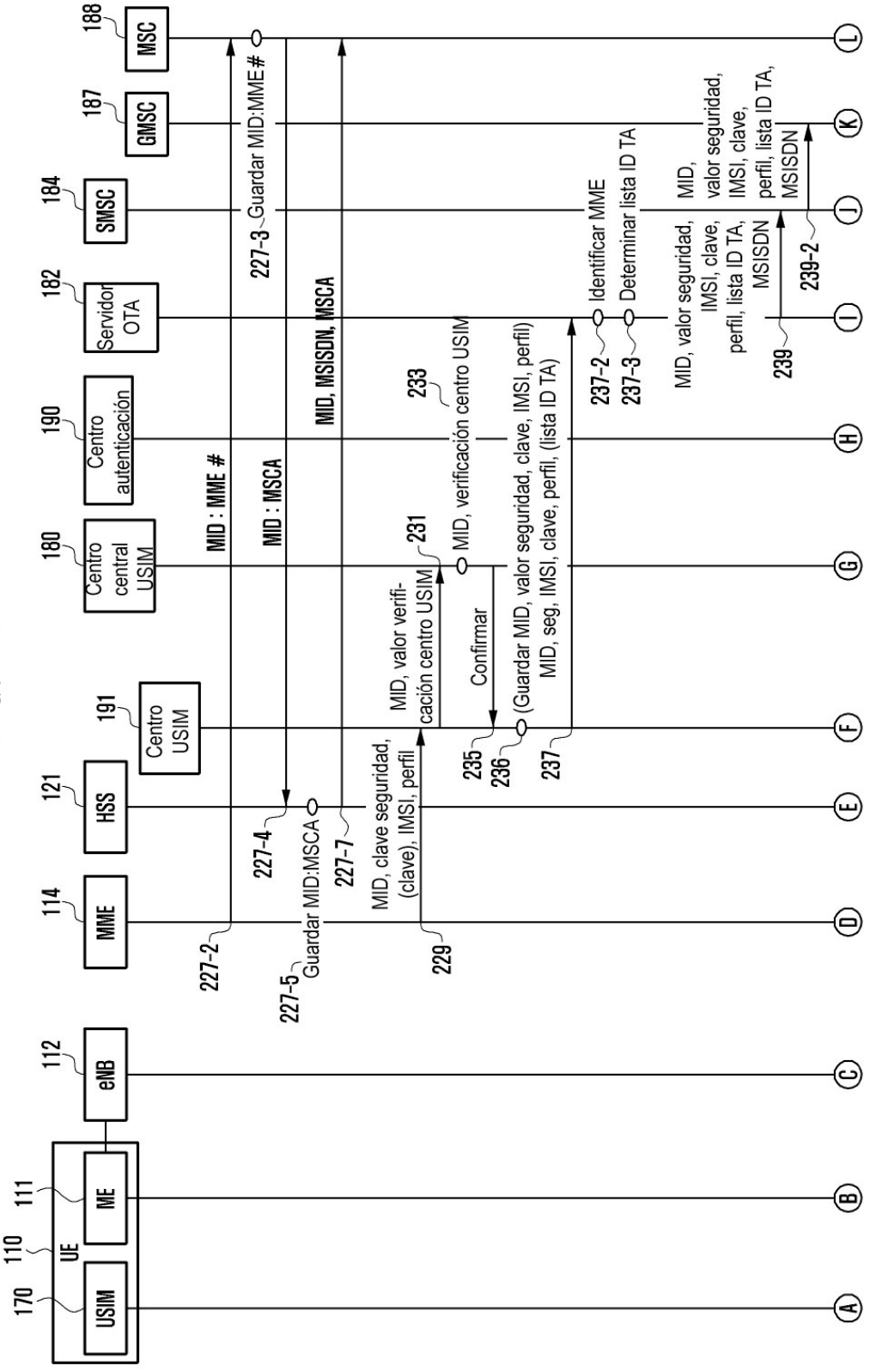

170
USIM
110
UE
111
ME
112
eNB
114
MME
121
HSS
191
Centro USIM
180
Centro central USIM
190
Centro autenticación
182
Servidor OTA
184
SMSC
187
GMSC
188
MSC
A
B
C
D
E
F
G
H
I
J
K
L
227-2
227-3 Guardar MID:MME#
227-4
227-5 Guardar MID:MSCA
227-7
229
231
233
235
236
237
237-2
237-3
239
239-2
MID : MME #
MID : MSCA
MID, MSISDN, MSCA
MID, clave seguridad, (clave), IMSI, perfil
MID, valor verificación centro USIM
MID, verificación centro USIM
Confirmar
(Guardar MID, valor seguridad, clave, IMSI, perfil)
MID, seg, IMSI, clave, perfil, (lista ID TA)
Identificar MME
Determinar lista ID TA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MSISDN

FIG. 5B

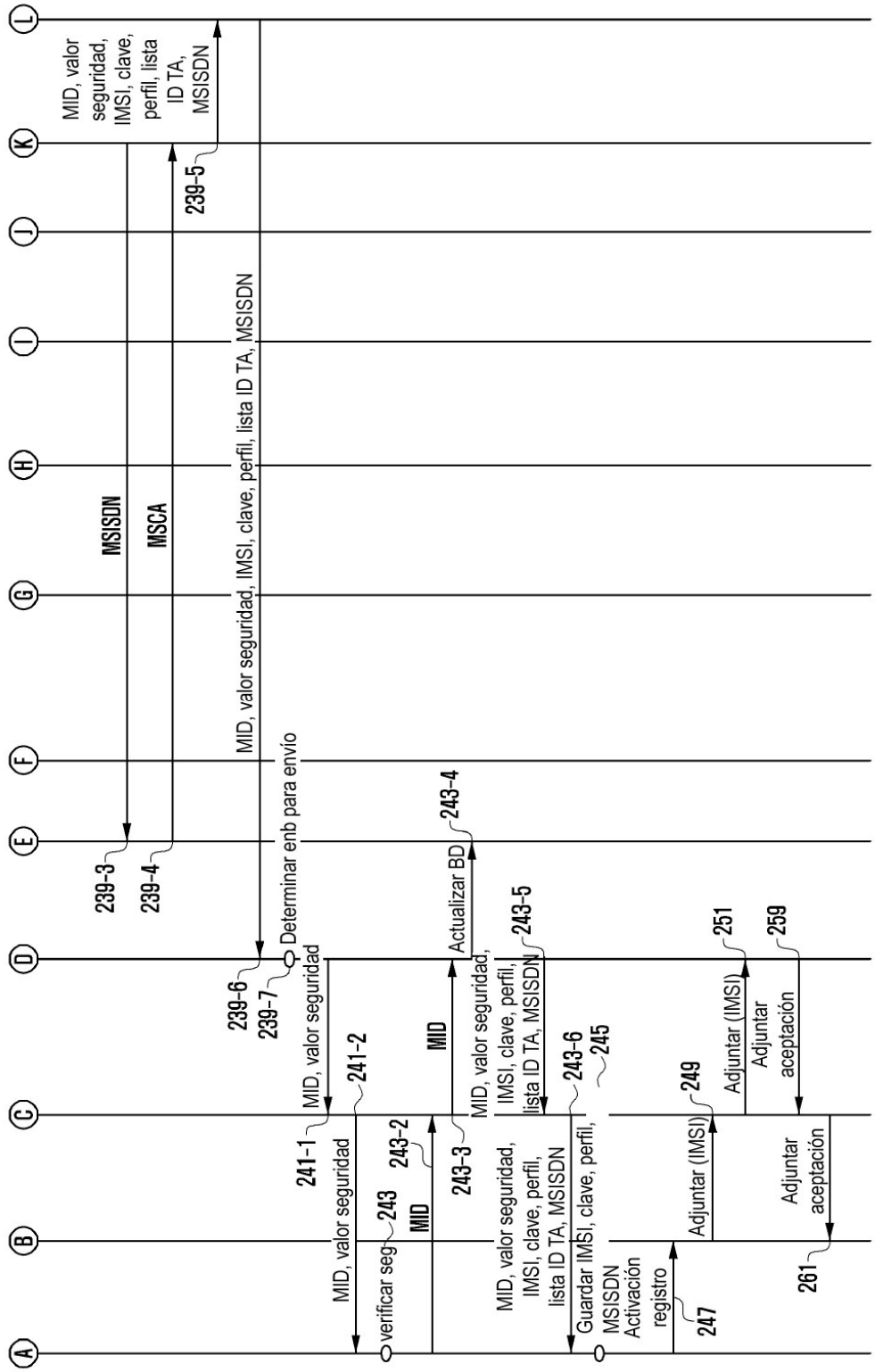

A
B
C
D
E
F
G
H
I
J
K
L
MSISDN
MSCA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
239-3
239-4
239-5
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
Determinar enb para envío
239-6
239-7
MID, valor seguridad
241-2
241-1
MID, valor seguridad
243
verificar seg
243-2
MID
MID
243-3
Actualizar BD
243-4
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
243-5
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
243-6
245
Guardar IMSI, clave, perfil, MSISDN
Activación registro
247
Adjuntar (IMSI)
249
Adjuntar (IMSI)
251
Adjuntar aceptación
259
Adjuntar aceptación
261

FIG. 6A

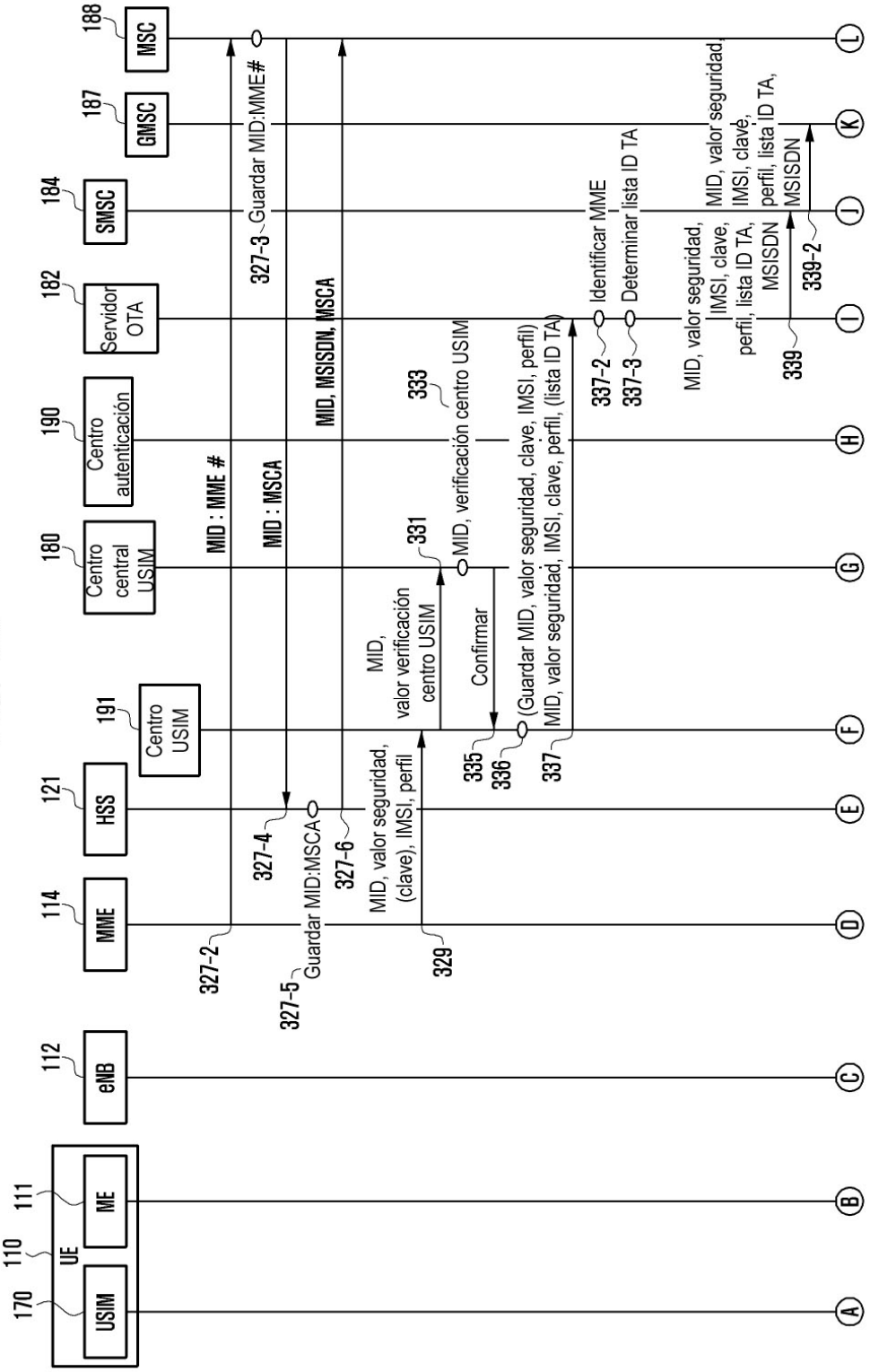

UE
USIM
ME
eNB
MME
HSS
Centro USIM
Centro central USIM
Centro autenticación
Servidor OTA
SMSC
GMSC
MSC
MID : MME #
MID : MSCA
MID, MSISDN, MSCA
Guardar MID:MME#
Guardar MID:MSCA
MID, valor seguridad, (clave), IMSI, perfil
MID, valor verificación centro USIM
MID, verificación centro USIM
Confirmar
(Guardar MID, valor seguridad, clave, IMSI, perfil)
MID, valor seguridad, IMSI, clave, perfil, (lista ID TA)
Identificar MME
Determinar lista ID TA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
327-2
327-3
327-4
327-5
327-6
329
331
333
335
336
337
337-2
337-3
339
339-2

FIG. 6B

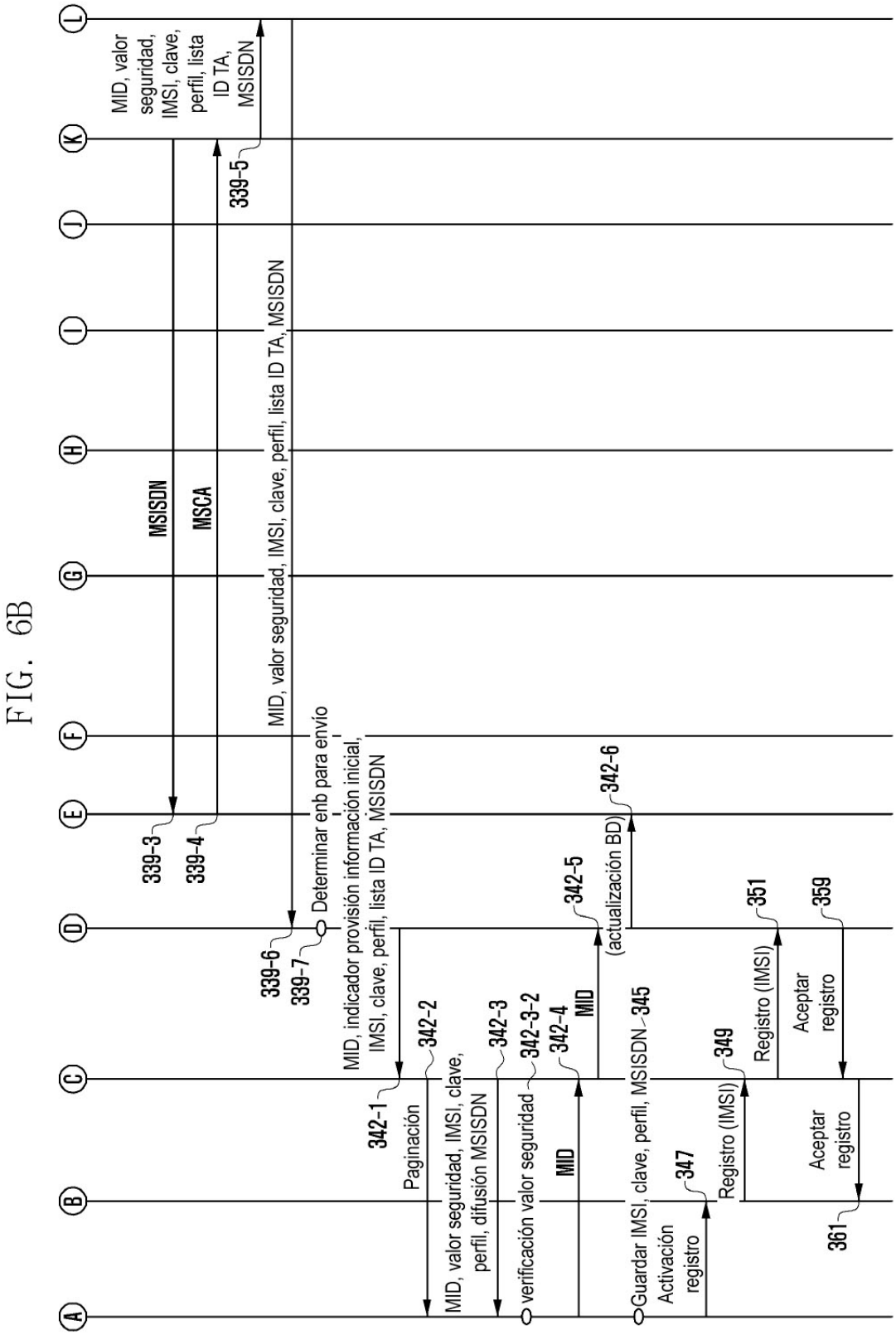

A
B
C
D
E
F
G
H
I
J
K
L
MSISDN
MSCA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
339-3
339-4
339-5
339-6
339-7
Determinar enb para envío
MID, indicador provisión información inicial, IMSI, clave, perfil, lista ID TA, MSISDN
342-1
Paginación
342-2
MID, valor seguridad, IMSI, clave, perfil, difusión MSISDN
342-3
verificación valor seguridad
342-3-2
342-4
MID
342-5
(actualización BD)
342-6
Guardar IMSI, clave, perfil, MSISDN
345
Activación registro
347
Registro (IMSI)
349
Registro (IMSI)
351
Aceptar registro
359
Aceptar registro
361

FIG. 7A

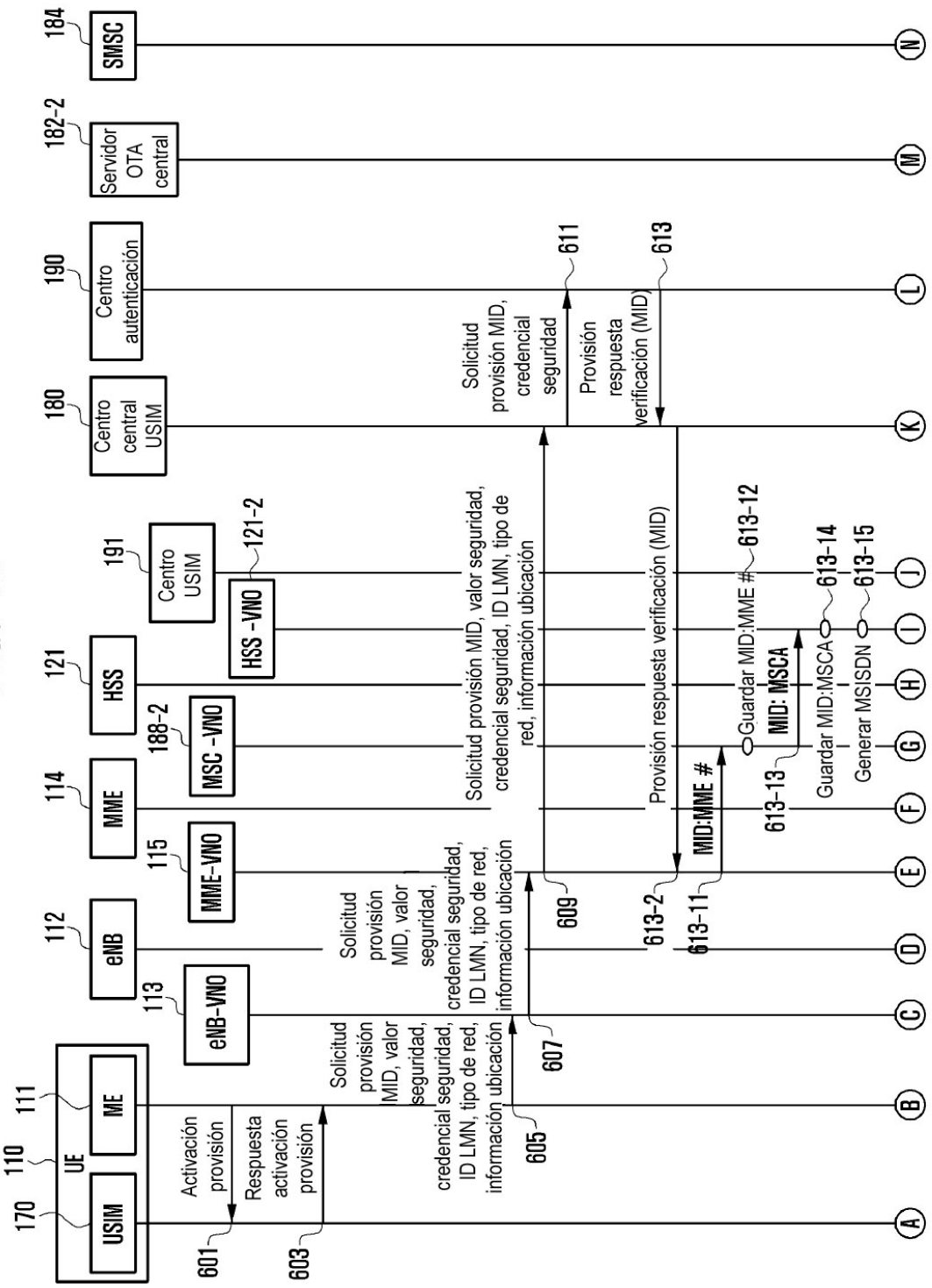

170
110
111
UE
USIM
ME
112
eNB
113
eNB-VNO
114
MME
115
MME-VNO
188-2
MSC -VNO
121
HSS
121-2
HSS -VNO
191
Centro USIM
180
Centro central USIM
190
Centro autenticación
182-2
Servidor OTA central
184
SMSC
Activación provisión
601
Respuesta activación provisión
603
Solicitud provisión MID, valor seguridad, credencial seguridad, ID LMN, tipo de red, información ubicación
605
607
Solicitud provisión MID, valor seguridad, credencial seguridad, ID LMN, tipo de red, información ubicación
609
Solicitud provisión MID, credencial seguridad
611
Provisión respuesta verificación (MID)
613
Solicitud provisión MID, valor seguridad, credencial seguridad, ID LMN, tipo de red, información ubicación
Provisión respuesta verificación (MID)
613-2
MID:MME #
613-11
Guardar MID:MME #
613-12
MID: MSCA
613-13
Guardar MID:MSCA
613-14
Generar MSISDN
613-15
A
B
C
D
E
F
G
H
I
J
K
L
M
N

FIG. 7B

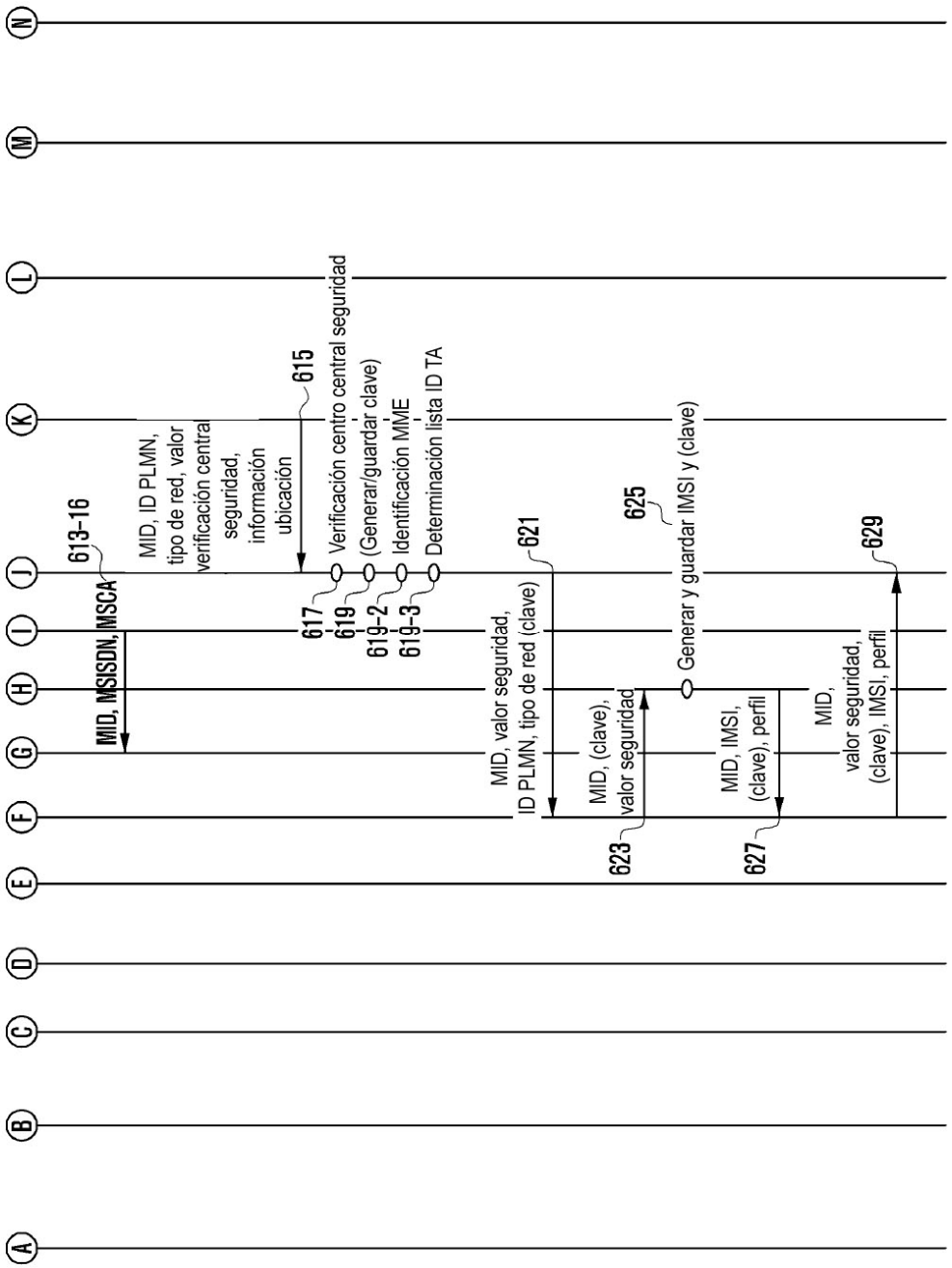

A
B
C
D
E
F
G
H
I
J
K
L
M
N
613-16
MID, MSISDN, MSCA
MID, ID PLMN, tipo de red, valor verificación central seguridad, información ubicación
615
Verificación centro central seguridad
617
(Generar/guardar clave)
619
Identificación MME
619-2
Determinación lista ID TA
619-3
621
MID, valor seguridad, ID PLMN, tipo de red (clave)
623
MID, (clave), valor seguridad
625
Generar y guardar IMSI y (clave)
627
MID, IMSI, (clave), perfil
629
MID, valor seguridad, (clave), IMSI, perfil

FIG. 8A

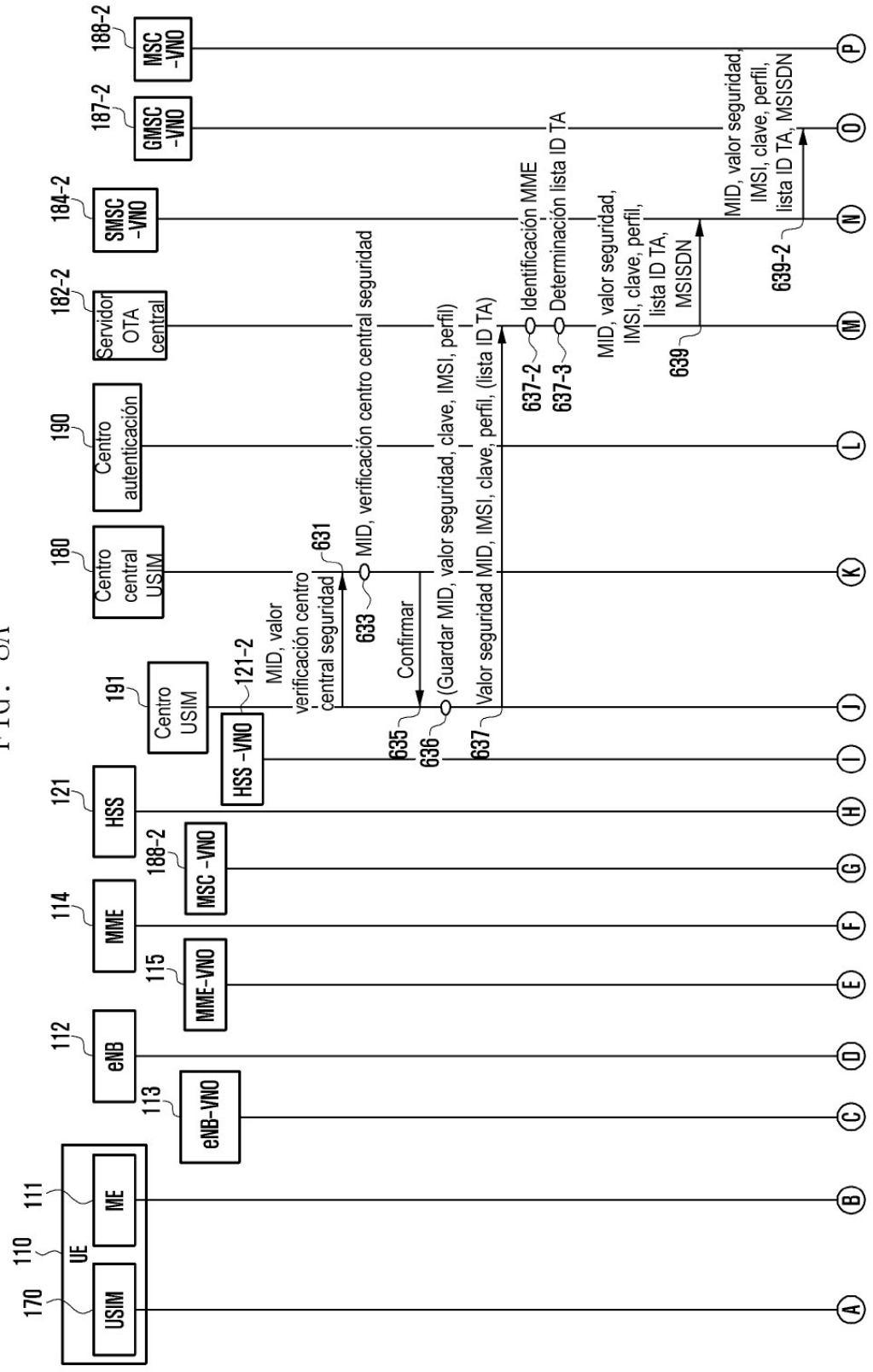

USIM
ME
UE
170
110
111
eNB-VNO
113
eNB
112
MME-VNO
115
MME
114
MSC -VNO
188-2
HSS
121
HSS -VNO
Centro USIM
191
Centro central USIM
180
Centro autenticación
190
Servidor OTA central
182-2
SMSC -VNO
184-2
GMSC -VNO
187-2
MSC -VNO
188-2
121-2
MID, valor verificación centro central seguridad
631
MID, verificación centro central seguridad
633
Confirmar
635
(Guardar MID, valor seguridad, clave, IMSI, perfil)
636
Valor seguridad MID, IMSI, clave, perfil, (lista ID TA)
637
637-2
Identificación MME
637-3
Determinación lista ID TA
639
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
639-2
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P

FIG. 8B

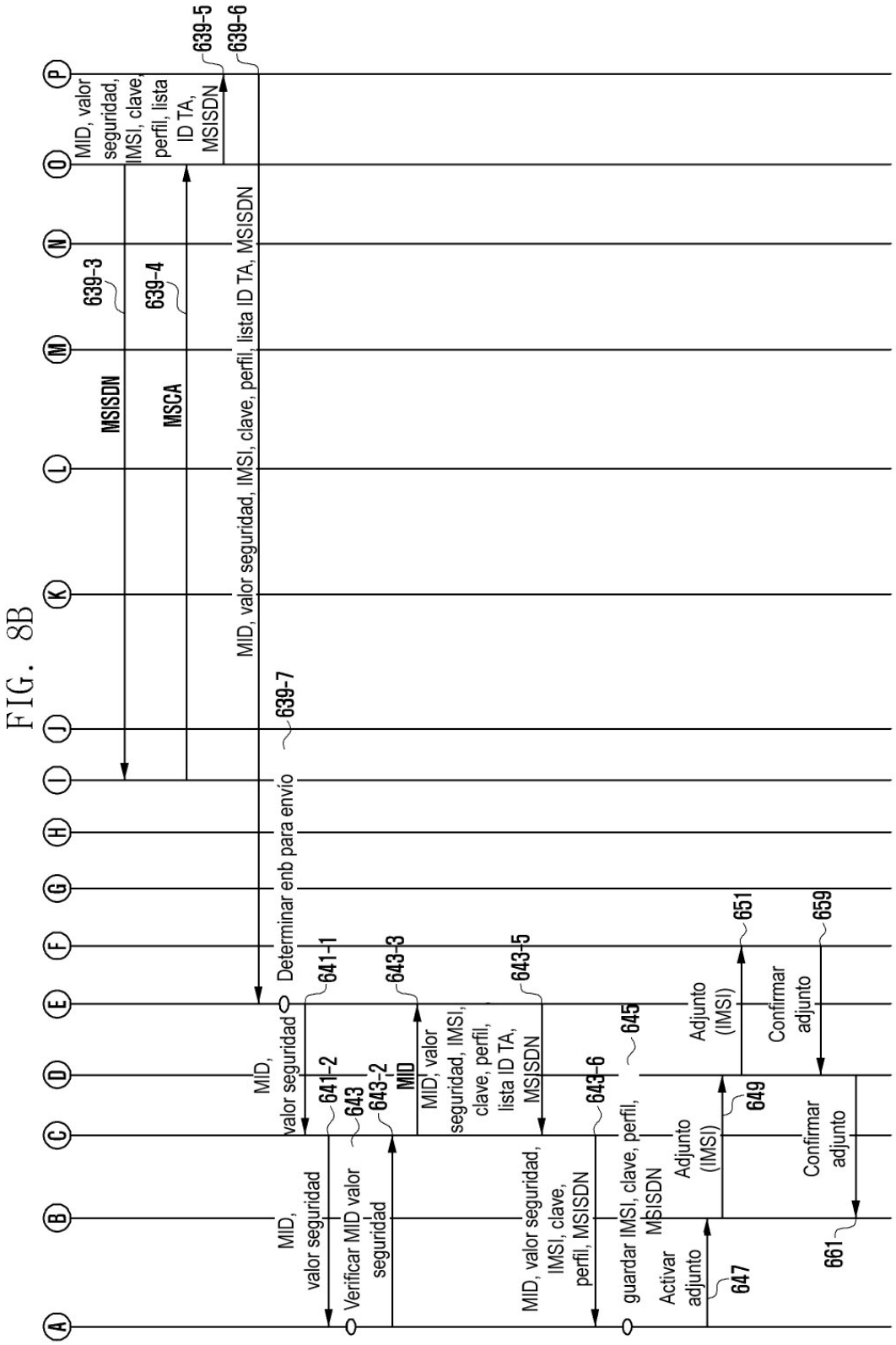

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
MSISDN
MSCA
639-3
639-4
639-5
639-6
639-7
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
Determinar enb para envío
641-1
MID, valor seguridad
641-2
643
643-2
MID
643-3
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
643-5
643-6
645
649
651
659
661
647
MID, valor seguridad
Verificar MID valor seguridad
MID, valor seguridad, IMSI, clave, perfil, MSISDN
guardar IMSI, clave, perfil, MSISDN
Activar adjunto
Adjunto (IMSI)
Adjunto (IMSI)
Confirmar adjunto
Confirmar adjunto

FIG. 9A

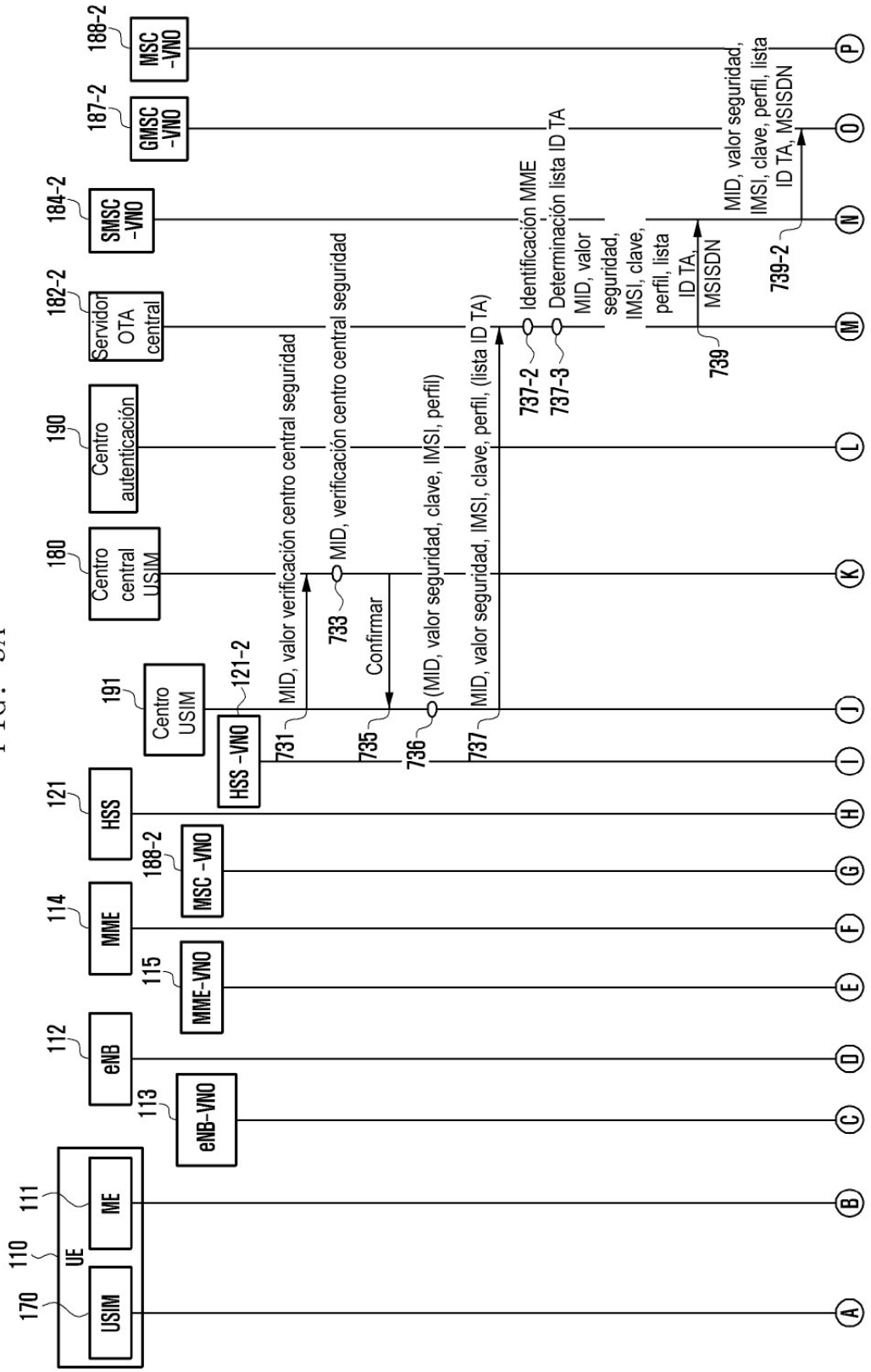

UE
USIM
ME
eNB
eNB-VNO
MME
MME-VNO
MSC -VNO
HSS
Centro USIM
HSS -VNO
Centro central USIM
Centro autenticación
Servidor OTA central
SMSC -VNO
GMSC -VNO
MSC -VNO
MID, valor verificación centro central seguridad
MID, verificación centro central seguridad
Confirmar
(MID, valor seguridad, clave, IMSI, perfil)
MID, valor seguridad, IMSI, clave, perfil, (lista ID TA)
Identificación MME
Determinación lista ID TA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN

FIG. 9B

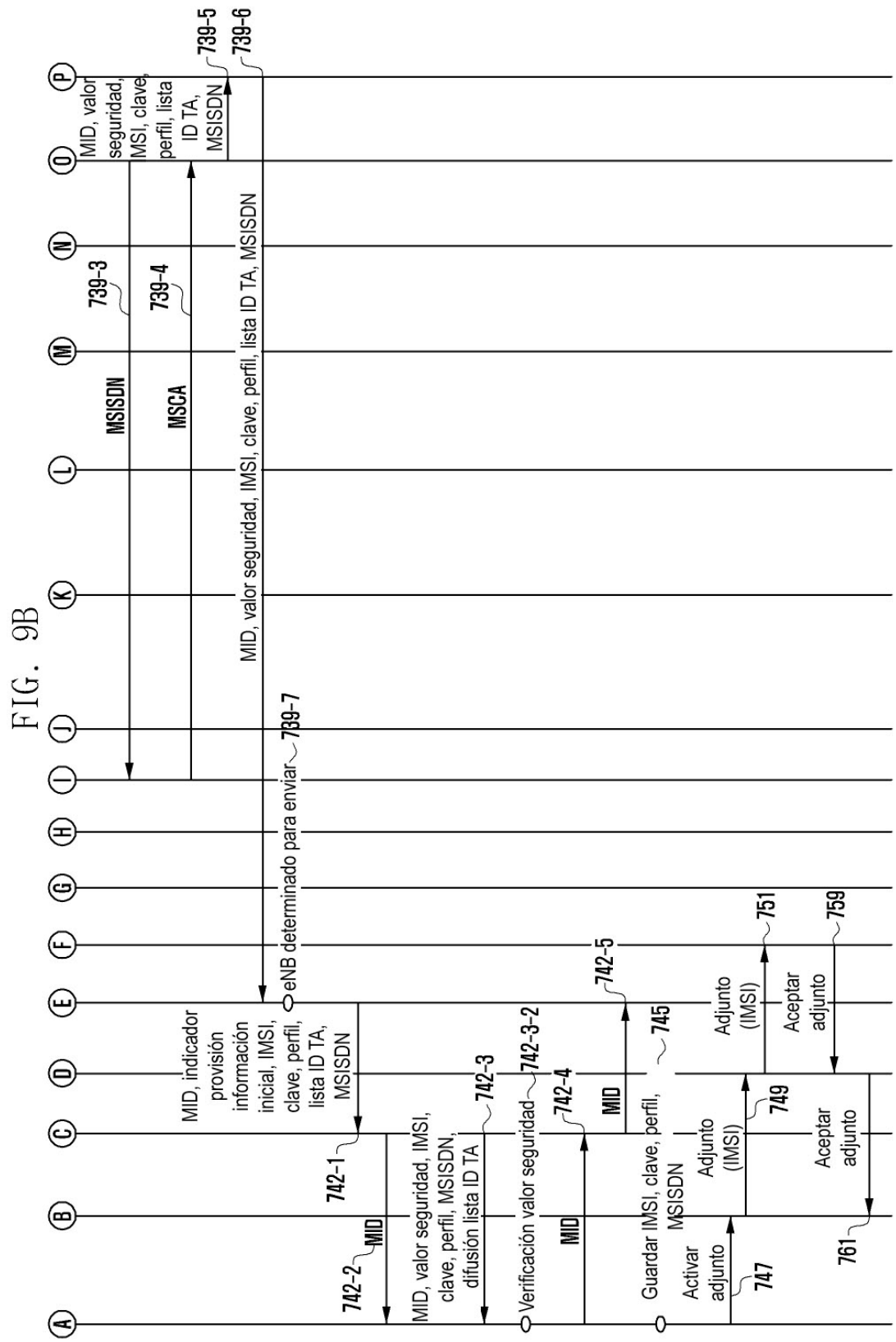

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
MID, valor seguridad, MSI, clave, perfil, lista ID TA, MSISDN
739-5
739-6
739-3
739-4
MSISDN
MSCA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
739-7
eNB determinado para enviar
MID, indicador provisión información inicial, IMSI, clave, perfil, lista ID TA, MSISDN
742-1
742-2
MID
MID, valor seguridad, IMSI, clave, perfil, MSISDN, difusión lista ID TA
742-3
742-3-2
Verificación valor seguridad
742-4
MID
742-5
745
Guardar IMSI, clave, perfil, MSISDN
Activar adjunto
747
Adjunto (IMSI)
749
751
Aceptar adjunto
759
761

FIG. 10A

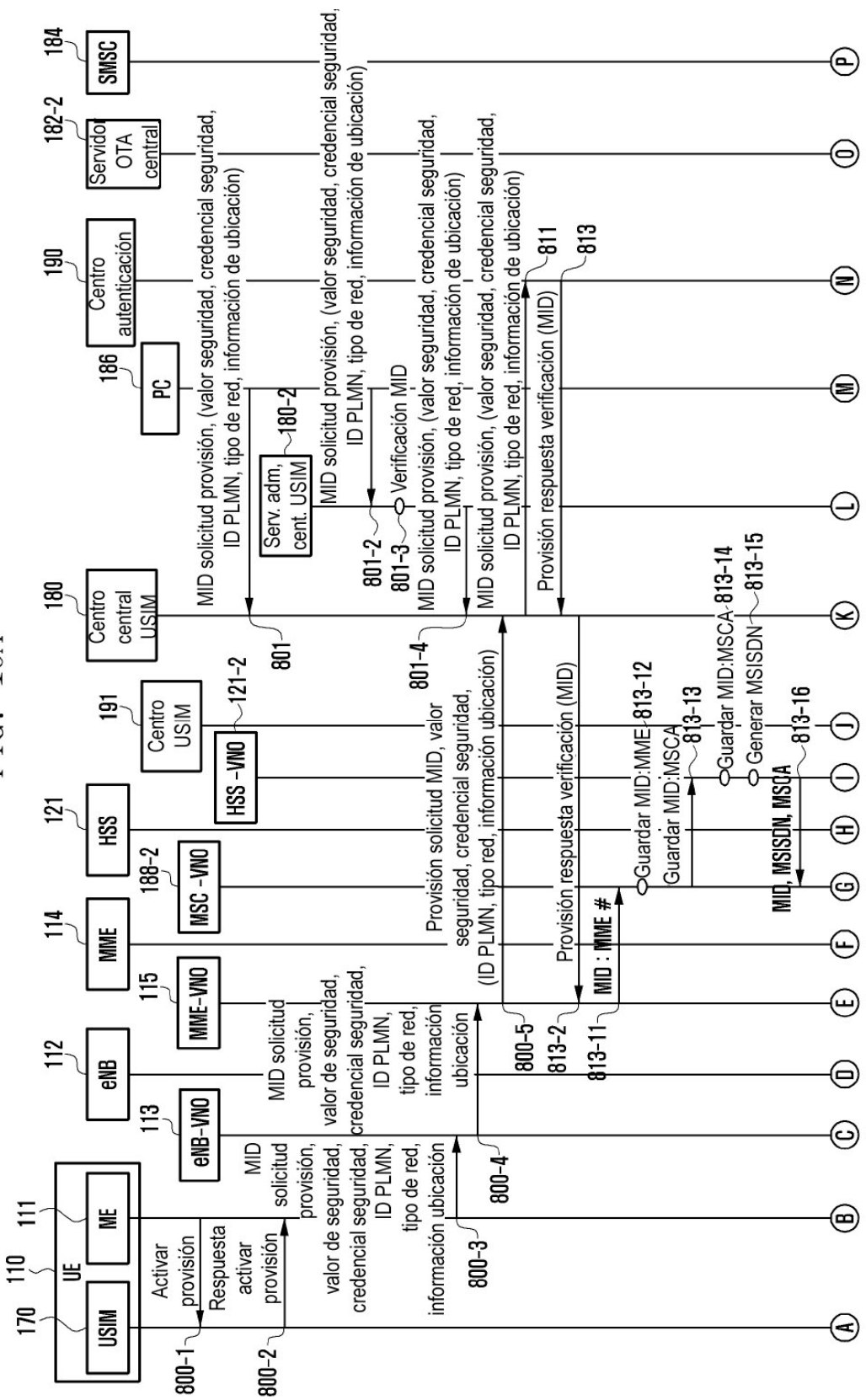

170
110
111
UE
USIM
ME
Activar provisión
Respuesta activar provisión
800-1
800-2
112
eNB
113
eNB-VNO
115
MME-VNO
114
MME
188-2
MSC -VNO
121
HSS
HSS -VNO
191
Centro USIM
121-2
180
Centro central USIM
801
801-2
801-3
801-4
186
PC
190
Centro autenticación
182-2
Servidor OTA central
184
SMSC
Serv. adm, cent. USIM
180-2
MID solicitud provisión, (valor seguridad, credencial seguridad, ID PLMN, tipo de red, información de ubicación)
MID solicitud provisión, (valor seguridad, credencial seguridad, ID PLMN, tipo de red, información de ubicación)
MID solicitud provisión, (valor seguridad, credencial seguridad, ID PLMN, tipo de red, información de ubicación)
MID solicitud provisión, (valor seguridad, credencial seguridad, ID PLMN, tipo de red, información de ubicación)
Verificación MID
MID solicitud provisión, (valor seguridad, credencial seguridad, ID PLMN, tipo de red, información de ubicación)
Provisión solicitud MID, valor seguridad, credencial seguridad, (ID PLMN, tipo red, información ubicación)
Provisión respuesta verificación (MID)
Provisión respuesta verificación (MID)
811
813
MID solicitud provisión, valor de seguridad, credencial seguridad, ID PLMN, tipo de red, información ubicación
800-3
800-4
800-5
813-2
813-11
MID : MME #
Guardar MID:MME
813-12
Guardar MID:MSCA
813-13
Guardar MID:MSCA
813-14
Generar MSISDN
813-15
MID, MSISDN, MSCA
813-16
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P

FIG. 10B

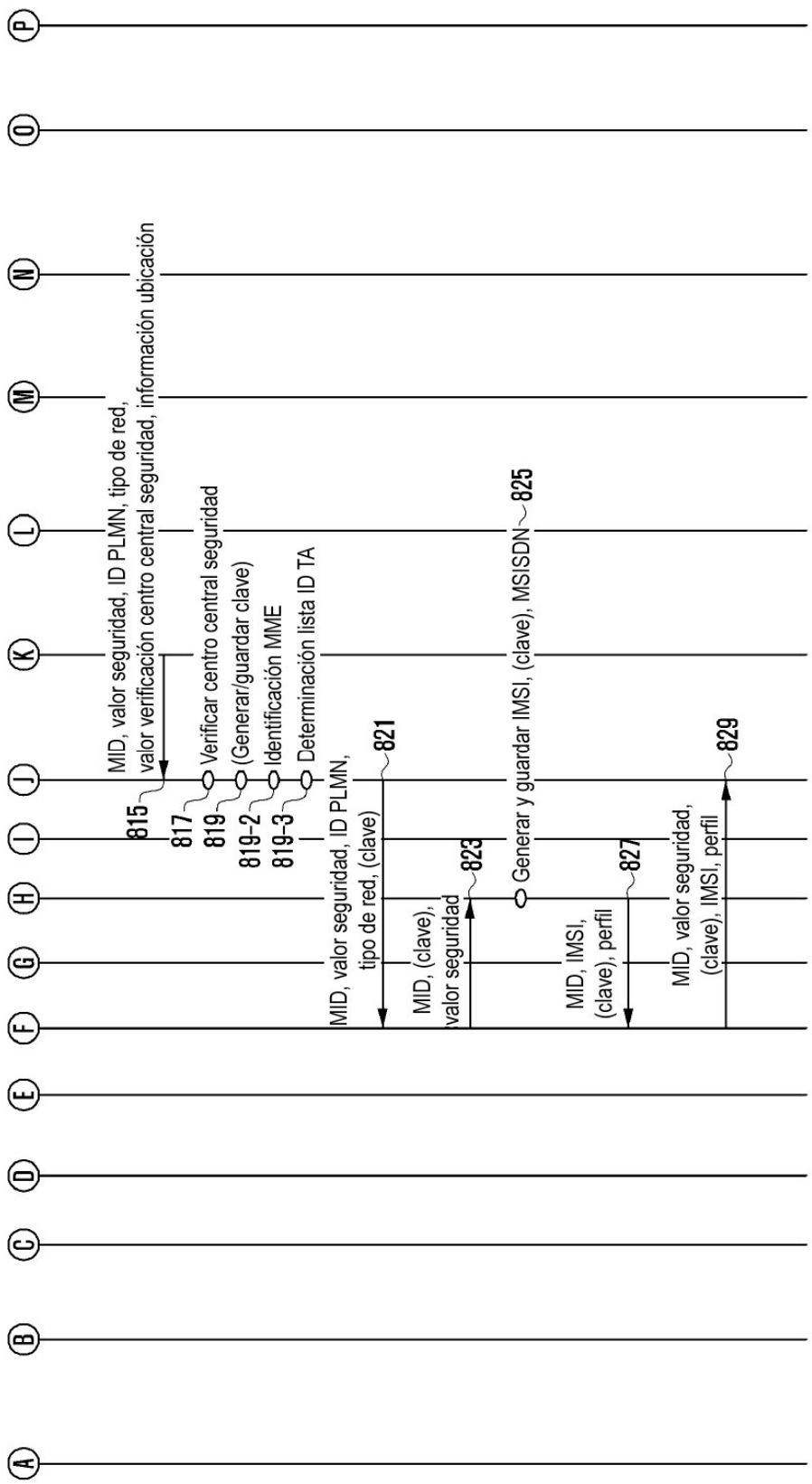

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
MID, valor seguridad, ID PLMN, tipo de red,
valor verificación centro central seguridad, información ubicación
815
Verificar centro central seguridad
817
(Generar/guardar clave)
819
Identificación MME
819-2
Determinación lista ID TA
819-3
MID, valor seguridad, ID PLMN,
tipo de red, (clave)
821
MID, (clave),
valor seguridad
823
Generar y guardar IMSI, (clave), MSISDN
825
MID, IMSI,
(clave), perfil
827
MID, valor seguridad,
(clave), IMSI, perfil
829

FIG. 11A

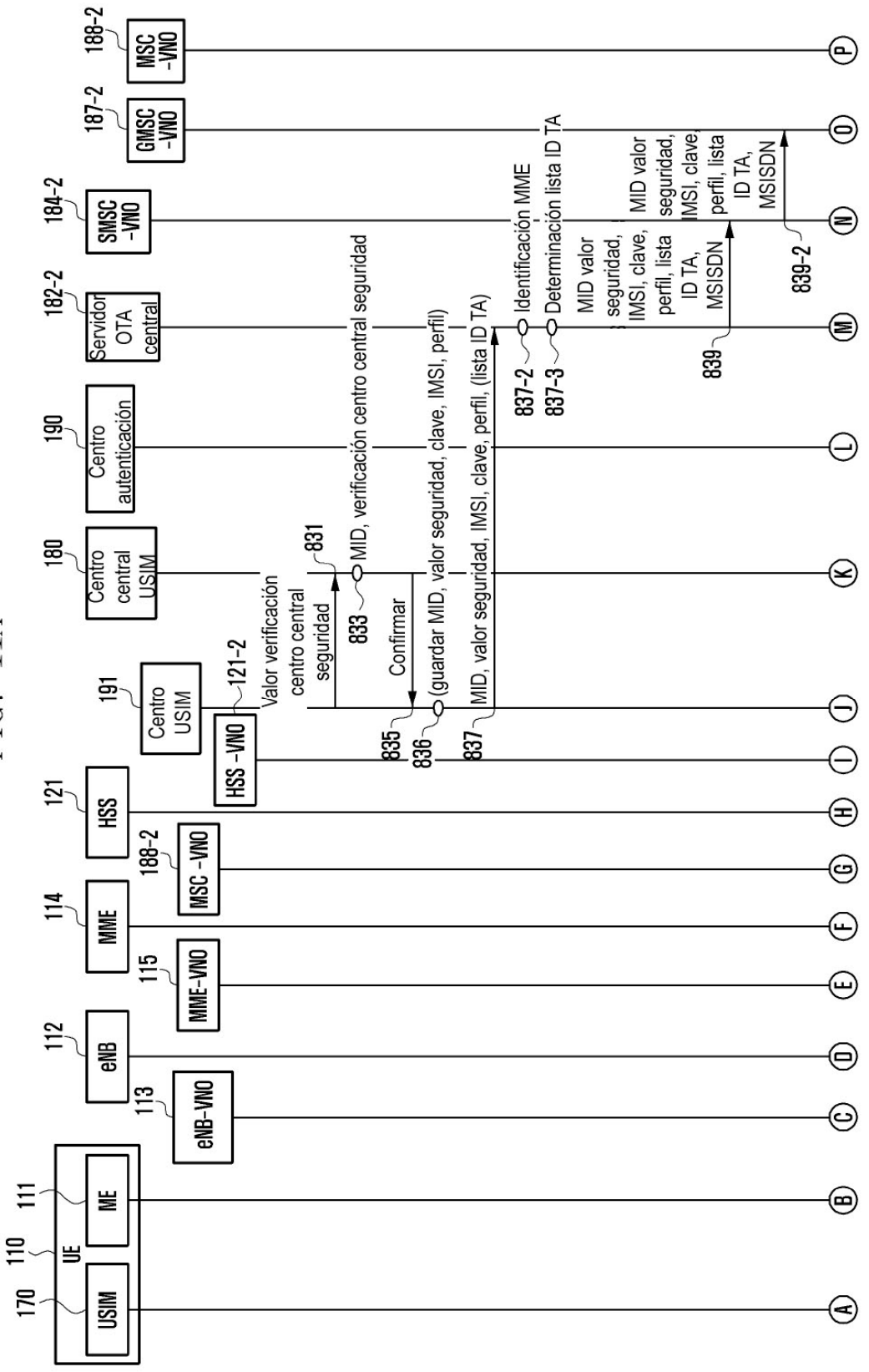

UE
USIM
ME
eNB
eNB-VNO
MME
MME-VNO
MSC -VNO
HSS
HSS -VNO
Centro USIM
Centro central USIM
Centro autenticación
Servidor OTA central
SMSC -VNO
GMSC -VNO
MSC -VNO
Valor verificación centro central seguridad
MID, verificación centro central seguridad
Confirmar
(guardar MID, valor seguridad, clave, IMSI, perfil)
MID, valor seguridad, IMSI, clave, perfil, (lista ID TA)
Identificación MME
Determinación lista ID TA
MID valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID valor seguridad, IMSI, clave perfil, lista ID TA, MSISDN
170
110
111
112
113
114
115
121
188-2
191
121-2
180
831
833
835
836
837
190
182-2
184-2
187-2
188-2
837-2
837-3
839
839-2
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P

FIG. 11B

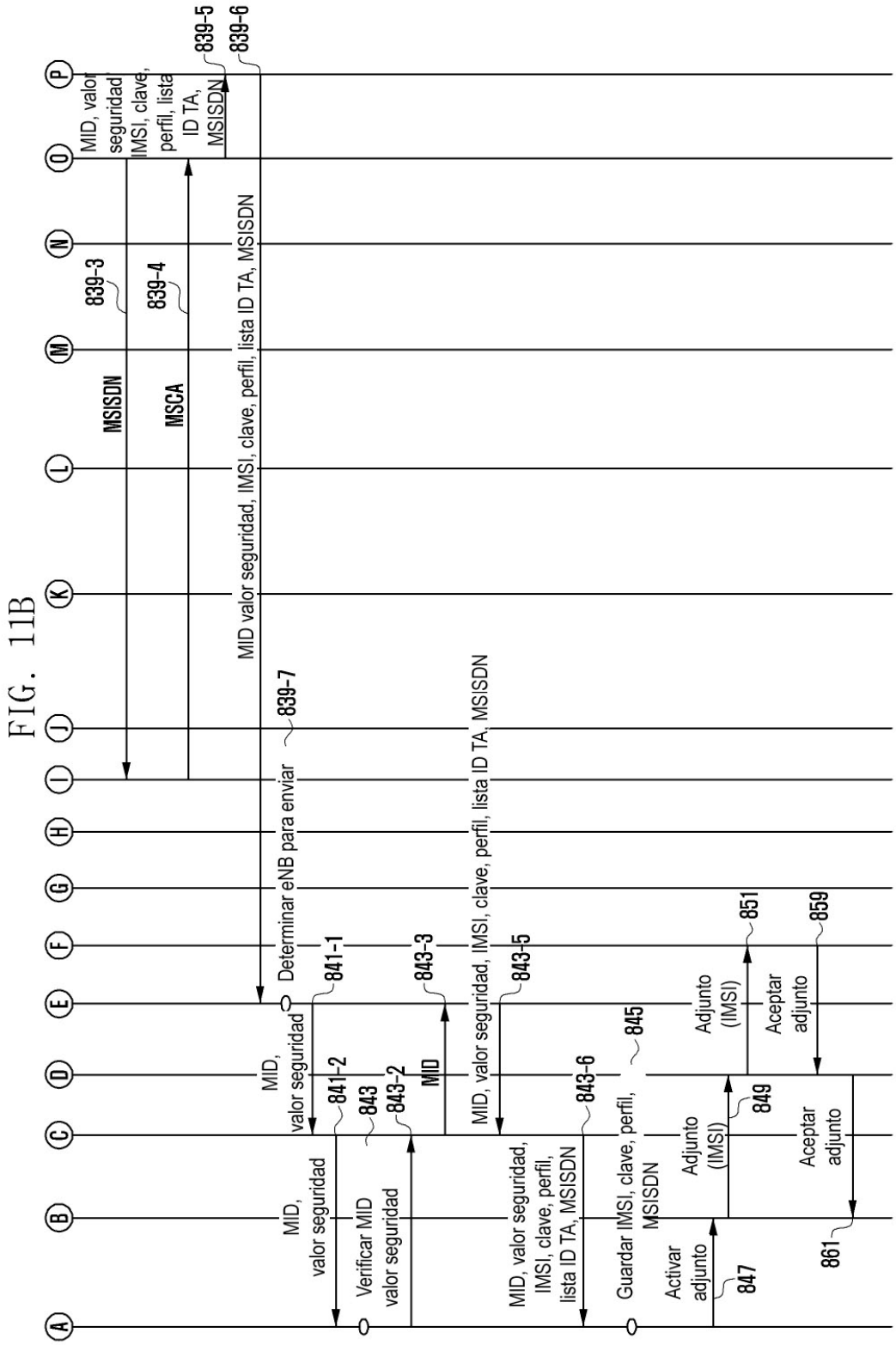

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
MSISDN
MSCA
839-3
839-4
839-5
839-6
839-7
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
Determinar eNB para enviar
MID, valor seguridad
841-1
841-2
843
843-2
MID
843-3
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
843-5
843-6
845
Adjunto (IMSI)
851
Aceptar adjunto
859
849
MID, valor seguridad
Verificar MID valor seguridad
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
Guardar IMSI, clave, perfil, MSISDN
Adjunto (IMSI)
Aceptar adjunto
Activar adjunto
847
861

FIG. 12A

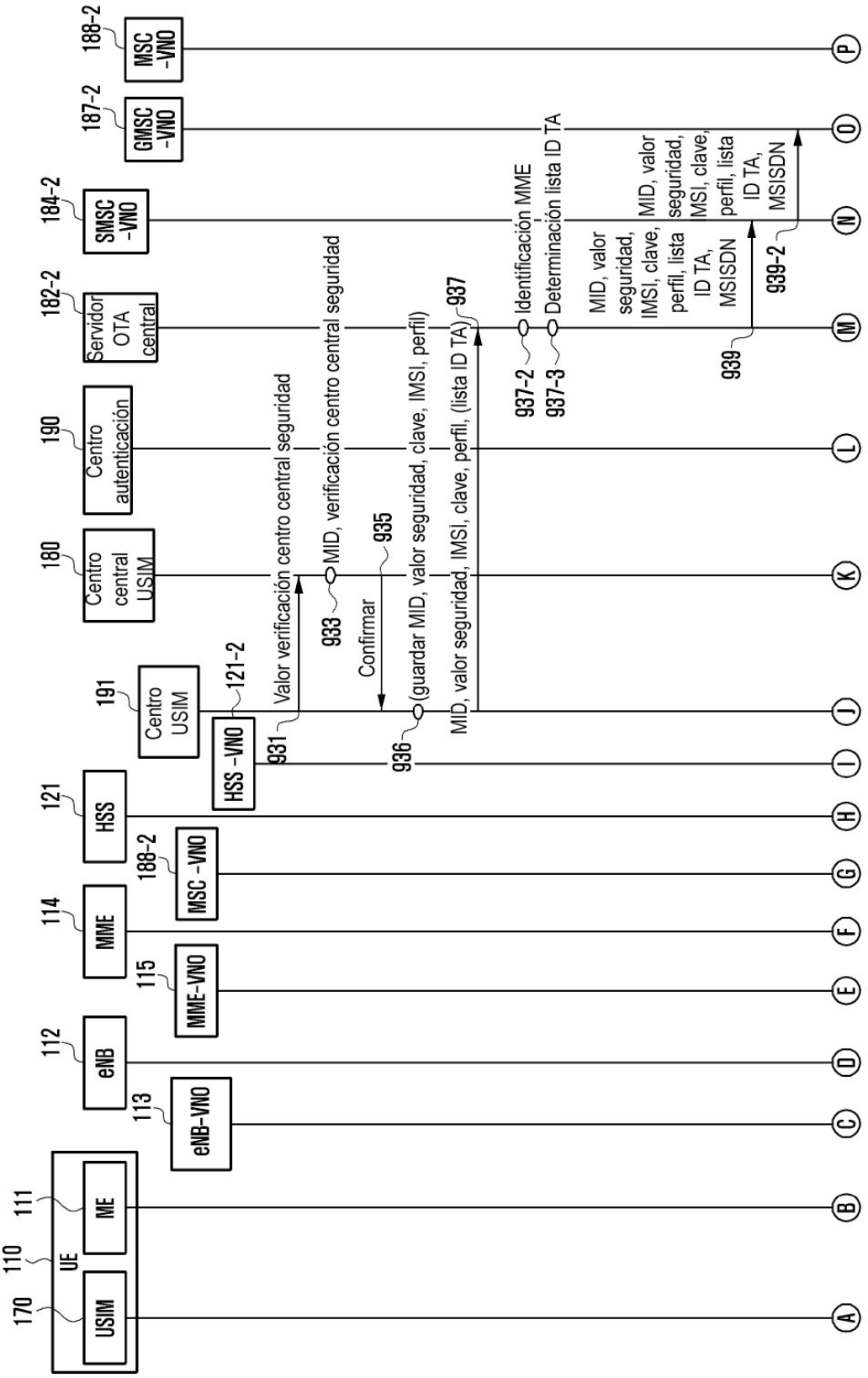
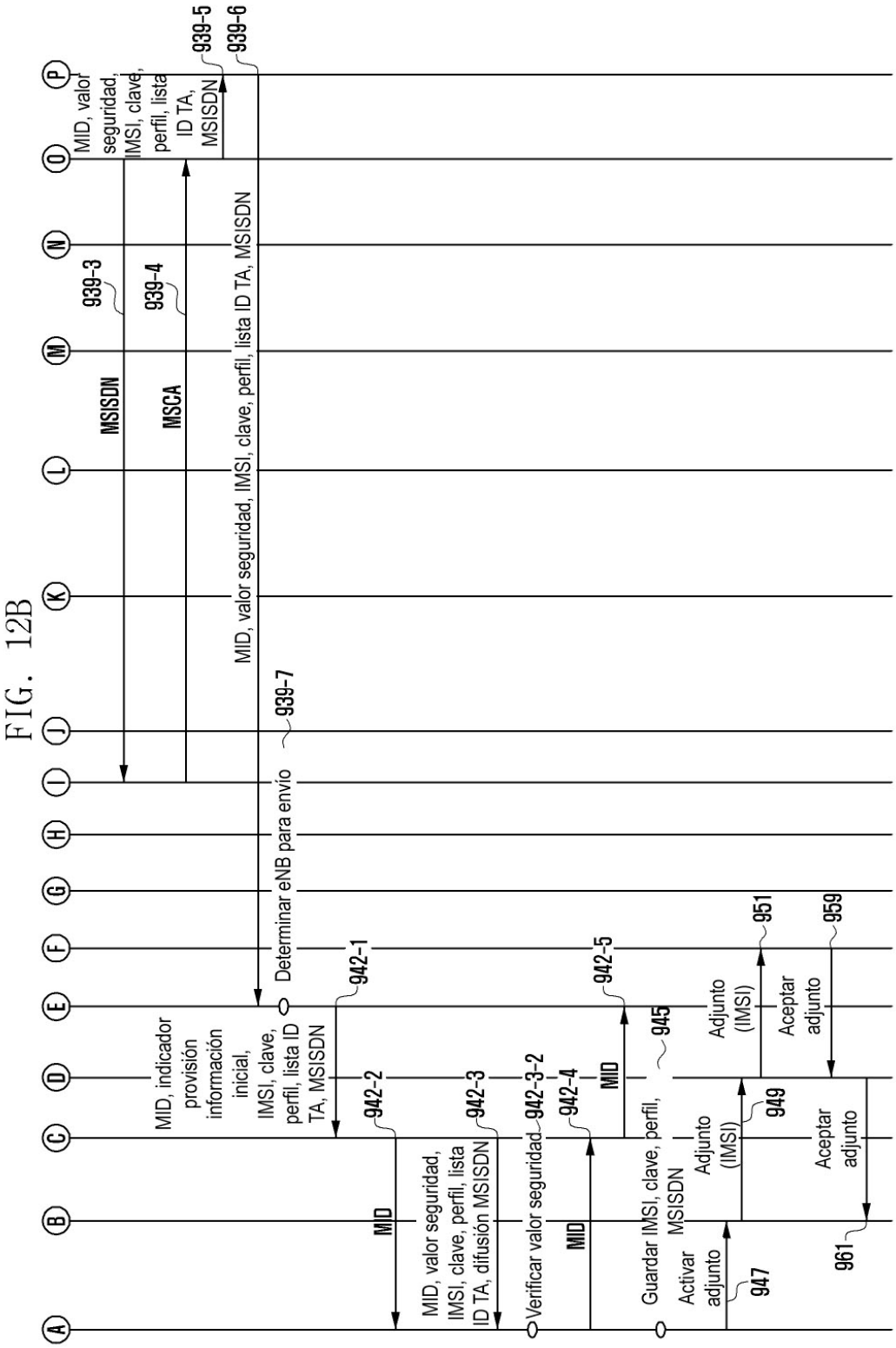

UE
USIM
ME
eNB
eNB-VNO
MME
MME-VNO
MSC -VNO
HSS
HSS -VNO
Centro USIM
Centro central USIM
Centro autenticación
Servidor OTA central
SMSC -VNO
GMSC -VNO
MSC -VNO
Valor verificación centro central seguridad
MID, verificación centro central seguridad
Confirmar
(guardar MID, valor seguridad, clave, IMSI, perfil)
MID, valor seguridad, IMSI, clave, perfil, (lista ID TA)
Identificación MME
Determinación lista ID TA
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID, valor seguridad, MSI, clave, perfil, lista ID TA, MSISDN
931
933
935
936
937
937-2
937-3
939
939-2

FIG. 12B


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
MSISDN
MSCA
939-3
939-4
939-5
939-6
939-7
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, MSISDN
Determinar eNB para envío
942-1
942-2
942-3
942-3-2
942-4
942-5
MID, indicador provisión información inicial, IMSI, clave, perfil, lista ID TA, MSISDN
MID
MID, valor seguridad, IMSI, clave, perfil, lista ID TA, difusión MSISDN
Verificar valor seguridad
MID
945
Guardar IMSI, clave, perfil, MSISDN
Activar adjunto
947
Adjunto (IMSI)
949
Aceptar adjunto
951
Adjunto (IMSI)
959
Aceptar adjunto
961