(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 828 575**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 4/06 (2009.01)
H04W 88/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.10.2016 E 16382468 (3)**

(97) Fecha y número de publicación de la concesión europea: **09.09.2020 EP 3310018**

(54) Título: **Acceso a través de una segunda red de telecomunicaciones móviles a los servicios ofrecidos por una primera red de telecomunicaciones móviles**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.05.2021

(73) Titular/es:

TELEFONICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Via 28
28013 Madrid, ES

(72) Inventor/es:

SERNA, JORGE;
NEYSTADT, JOHN y
GALLEGOS, DAVID

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Acceso a través de una segunda red de telecomunicaciones móviles a los servicios ofrecidos por una primera red de telecomunicaciones móviles

Campo técnico de la invención

La presente invención se refiere, en general, a la gestión de acceso a los servicios de comunicación móvil y, más específicamente a proporcionar acceso a servicios de comunicación móvil ofrecidos, a través de una primera red de telecomunicaciones móviles, desde una segunda red de telecomunicaciones, tal como una red de datos de radio.

Antecedentes de la invención

Las empresas de telecomunicaciones han desarrollado mecanismos que permiten a los usuarios acceder a sus servicios usuales de telecomunicaciones por una conexión Wifi, manteniendo su identidad usual. Este servicio se conoce como "llamada Wifi", lo cual es especialmente útil en áreas con cobertura débil de portadora, tales como la zona rural residencial o cualquier edificio con recepción irregular.

Las llamadas Wifi permiten a la gente llamar y utilizar mensajes de texto, incluso si no tienen una señal de teléfono, sencillamente conectando un teléfono móvil a una red Wifi. Funciona mediante la apertura de una conexión IPSec (Protocolo de Seguridad de Internet) entre el dispositivo y la red móvil doméstica, después de la autenticación requerida en base al SIM (Módulo de Identidad de Abonado), y el establecimiento luego de comunicaciones basadas en el SIP (Protocolo de Inicio de Sesiones). Por lo tanto, en lugar de utilizar la conexión a la red de telecomunicaciones del portador usual, los usuarios pueden realizar llamadas de voz o mensajes de texto a través de una red Wifi. Desde el punto de vista del usuario, esto es en realidad como cualquier otra llamada telefónica, y todavía usa sus contactos usuales. Puede ser configurado, en caso de que se pierda la señal de teléfono usual, para que, entonces, el teléfono móvil conmute automáticamente a la llamada Wifi, para que sea totalmente transparente para el usuario.

Por otro lado, las personas que viajan al extranjero que quieren mantenerse en contacto, a menudo aprovechan más la conexión Wifi (cuando están disponibles en hoteles, cafés, plazas públicas...,) que los planes de itinerancia porque desconfían del coste y los servicios incluidos o simplemente no pueden acceder a sus servicios regulares. Por lo tanto, es obvio que los usuarios se benefician de un área de cobertura más amplia gracias a la llamada Wifi, pero todavía están ligados a una cobertura de Wifi.

El documento US 2015/327207 A1 se refiere a la gestión del registro del servicio de Subsistema Multimedia de Protocolo de Internet (IMS) en un dispositivo de comunicación inalámbrica que tenga al menos una SIM que admita los servicios de I MS. El dispositivo de comunicación sin conexión desvelado por el documento US 2015/327207 puede acceder a las políticas del operador de red almacenadas en las SIM e identificar los servicios IMS habilitados para cada SIM. Además, este dispositivo de comunicación inalámbrica también puede identificar, en función de las políticas de operador de red a las que se accede, el tipo de registro para cada servicio IMS habilitado en cada SIM y determinar si se debe realizar un registro único o un registro IMS dual para cada SIM. Sin embargo, el documento US 2015/327207 no se ocupa del registro del dispositivo de comunicación inalámbrica a las llamadas Wifi.

Por las razones antes mencionadas, cualquier solución que aumente las opciones de los usuarios para acceder a sus servicios regulares de comunicaciones móviles, especialmente cuando está en el extranjero, sería una gran contribución técnica a la técnica anterior.

Sumario de la invención

La presente invención está definida por la materia objeto de las reivindicaciones independientes. Las realizaciones preferentes están definidas en las reivindicaciones dependientes.

Descripción de los dibujos

Para completar la descripción que se está realizando, y con el objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo a un ejemplo preferido de realización práctica de la misma, acompañando a dicha descripción como una parte integrante de la misma, hay un dibujo en el que, a modo de ilustración y no de manera restrictiva, se ha representado lo siguiente:

La **figura 1** muestra una representación esquemática de una eUICC con múltiples perfiles dotados de MNO.
La **figura 2** muestra el flujo implicado en un SIM Dual, con registro de llamadas de Wifi, de acuerdo con una realización de la presente invención.
La **figura 3** muestra la secuencia de mensajes para establecer un canal de comunicación (Canal S1) con el operador visitado por la primera red de comunicación móvil, de acuerdo con una realización de la invención.
La **figura 4** muestra la secuencia de mensajes para establecer un canal de comunicación (túnel de IPsec) con el operador de origen, de acuerdo con una realización de la invención.
La **figura 5** muestra la secuencia de mensajes para configurar un canal del GTP (Protocolo de Túneles del GPRS) y para establecer el registro del IMS en el núcleo del IMS del operador doméstico, de acuerdo con una realización

de la invención.

Descripción detallada de la invención

Los asuntos definidos en esta descripción detallada se proporcionan para facilitar un exhaustivo entendimiento de la invención.

La invención actual desvela un procedimiento para proporcionar acceso a los servicios de comunicación móvil ofrecidos a través de una primera red de telecomunicaciones móviles desde una segunda red de telecomunicaciones.

A saber, la presente invención desvela un procedimiento para utilizar el enfoque de llamadas Wifi en los teléfonos provistos de múltiples SIM, siendo un teléfono móvil con múltiples SIM un dispositivo que contiene al menos dos tarjetas SIM (dual-SIM), una tarjeta SIM primaria y una tarjeta SIM secundaria. Esto es útil, por ejemplo, cuando se vaga por la itinerancia, ya que permite a los usuarios acceder a una red externa mientras mantienen la tarjeta local existente. Por lo tanto, el teléfono móvil se configura de modo que una SIM primaria se utiliza para la autenticación IPSec y SIP contra el usuario HLR (Home Location Register), pero bloquea la itinerancia de datos en esa SIM primaria, y tiene todos los datos para pasar a través de la SIM secundaria. Por lo tanto, el usuario puede seguir utilizando su identidad habitual, es decir, número de teléfono, mientras que el uso de una suscripción secundaria para el tráfico de datos, que puede ser útil en varios escenarios, tal como evitar cargos por itinerancia, beneficiarse de la conexión de datos móviles con un rendimiento superior al ofrecido por la red o que el usuario tiene la suscripción primaria, para cambiar a otra suscripción una vez que se ha consumido el plan de datos del usuario, etc. La SIM secundaria, de acuerdo con una realización de la invención, es una e-SIM. Por lo tanto, una de las alternativas propuestas por la presente invención se refiere a tener una tarjeta SIM física y una tarjeta SIM integrada (eSIM), en su lugar dos tarjetas SIM físicas, que permite gestionar de forma más fácil y transparente el intercambio de tarjeta SIM en diferentes países. De acuerdo con esta realización, el SIM primaria es una tarjeta SIM física que se utiliza para la autenticación del operador local de origen y la autenticación de llamadas de Wifi en la red doméstica, pero, cuando el usuario está en itinerancia en lo que respecta a esa suscripción primaria, la conexión de datos se proporciona a través de una red de datos de 3G/4G, proporcionada por un operador local utilizando un eSIM como SIM secundario.

Una tarjeta e-SIM es una tarjeta SIM integrada que puede ser operada de forma remota. La arquitectura de la tarjeta SIM integrada permite tener múltiples perfiles almacenados en el chipset eUICC (Tarjeta electrónica Universal de Circuitos Integrados). Como una ventaja adicional para el despliegue de servicios basados en el uso de una tarjeta e-SIM como una tarjeta SIM secundaria, podría ser tener provistos varios perfiles de MNO inhabilitados. Esto significa que podría ser posible definir alianzas entre los operadores para proveer previamente algunos perfiles de MNO para proporcionar este tipo de servicio a los clientes cuando están utilizando su equipo de mano en un país visitado. Luego, una vez que el multiSIM está habilitado, un escenario típico podría ser de usuarios manteniendo su SIM físico para la autenticación con la compañía de telecomunicaciones de origen, pero comprando un e-SIM local en itinerancia.

La **figura 1** muestra una representación esquemática de una eUICC (1) con múltiples perfiles de MNO (Operador de Redes Móviles) provistos, tanto perfiles habilitados (2) como perfiles inhabilitados (3). Se puede observar cómo los perfiles de MNO de la eUICC están diseñados según el estado de la técnica. Los perfiles están contenidos dentro de dominios de seguridad (SD) en la eUICC, dejando así disponibles los mecanismos de seguridad de los SD. De acuerdo con la Arquitectura Incrustada de Provisión Remota de SIM de la GSMA:

- El sistema operativo (OS) (4) contiene las características básicas de la plataforma:
- El ECASD (5) (Dominio de Seguridad de la Autoridad Certificadora de eUICC): se crea dentro de una eUICC en el momento de su fabricación y no puede ser eliminado o inhabilitado después de la entrega.
- El ISD - R (6) (Dominio de seguridad del Emisor - Raíz) es el representante en la tarjeta del SM-SR (Gestor de Abonos – Encaminamiento Seguro) que ejecuta los comandos de gestión de plataforma. Un ISD-R deberá crearse dentro de una eUICC en el momento de la fabricación, asociarse a un SM-SR y no ser eliminado o inhabilitado;
- El ISD-P (7) (Dominio de seguridad del emisor - Perfil) es el representante en la tarjeta del MNO, o de la SM-DP (Preparación de Datos del Gestor de Abonos), si está delegada por el MNO. Un ISD-P, de acuerdo con la Arquitectura Incrustada de Provisión Remota de SIM de la GSMA:

    a. será una entidad separada e independiente en la eUICC;
    b. constará de un Perfil que incluye el sistema de ficheros, las NAA y las Reglas de Política;
    c. contendrá una máquina de estados relacionada con la creación, habilitación e inhabilitación del Perfil;
    d. contendrá claves para la gestión de Perfiles, para la fase de carga e instalación;
    e. Implementará un protocolo de establecimiento de claves para generar un conjunto de claves para la personalización del ISD-P;
    f. será capaz de recibir y descifrar, cargar e instalar el Perfil creado por la SM-DP;
    g. será capaz de establecer su propio estado como inhabilitado, una vez que se instala el Perfil;
    h. proporcionará capacidades del Protocolo Seguro de Canal 03 (SCP03) para asegurar su comunicación con el Gestor de Abonos - Preparación de Datos (SM-DP);
    i. será capaz de contener un CASD. Este CASD es optativo dentro del perfil y presta servicios únicamente a los dominios de seguridad del Perfil, y sólo cuando el Perfil está en estado Habilitado.

- El MNO-SD (8) es el representante en tarjeta del MNO. Un MNO-SD se asociará a sí mismo, contendrá las Claves OTA (por el aire) del MNO y proporcionará un canal OTA seguro
- El Administrador de Servicios de Plataforma (10) es un servicio del sistema operativo que ofrece funciones de gestión de la plataforma y un mecanismo de ejecución de Reglas de Política (Ejecutor de Reglas de Criterios (12)). Llamado por el DSI-R o el ISD-P, ejecuta las funciones de acuerdo con las Reglas de Política. Además, puede recuperar la información genérica del ISD-P (es decir, Identificador de perfil, Estado de Perfil) que puede ser compartida con las entidades autorizadas, a petición.
- El Entorno de Telecomunicaciones (11) es un servicio del sistema operativo que proporciona algoritmos estandarizados de autenticación de red a las NAA alojadas en los ISD-P. Además, proporciona las capacidades para configurar el algoritmo con los parámetros necesarios.

Un perfil de MNO puede comprender un sistema de ficheros (13), las NAA (Redes como un Servicio) (14), el CASD (Dominio de Seguridad de la Autoridad Certificadora) (15), las miniaplicaciones (16), el SSD (controlador de estado sólido) (17) y/o las reglas de política (18).

Además de un dispositivo habilitado para multi-SIM, la presente invención necesita otro requisito para ser implementada. El dispositivo debe desplegar un cliente de Llamadas Wifi, lo que significa implementar los requisitos especificados por el 3GPP para la autenticación y la autorización para el acceso al EPC (Núcleo Evolucionado por Paquetes) mediante una red de acceso no fiable y no del 3GPP, tal como se define en el documento 3GPP TS 24.302, V13.5.0 (2016-03), sección 6.4.

De acuerdo con una realización de la presente invención, se permite al usuario elegir tarjeta SIM para el registro en el servicio de Llamadas Wifi, de acuerdo a una lista de operadores que están configurados en el teléfono, o que reciben esta lista desde el servicio de configuración de la red.

En una realización de la invención, el software incluido en el equipo de mano del teléfono inteligente expone una opción para que el usuario habilite las llamadas Wifi, si es apoyada por algunos de los operadores que han emitido un SIM físico, o un eSIM, habilitado en el teléfono. Si el servicio de Llamadas Wifi está disponible por parte de más de un proveedor, entonces sería necesario incluir una opción adicional para seleccionar el servicio de Llamadas Wifi del operador, para estar conectado.

La arquitectura de las llamadas Wifi, según lo definido por la GSMA, permite al software del teléfono utilizar los protocolos de VoIP para conectarse a la red del IMS Portadora mediante redes no confiables, incluyendo Internet. De acuerdo con una arquitectura de llamadas Wifi/ePDG, una vez que el equipo de mano está configurado con una dirección de EPDG & P-SCSF, se establece un túnel seguro de IPSec al elemento de red EPDG (servidor de VPN), y luego se autentica utilizando el SIM situado en el teléfono (usando el mecanismo de EAP-AKA (Protocolo de Autenticación Extensible - Autenticación y Concordancia de Claves)) (como se describe en el documento 3GPP 24.302 V13.5.0 (2016-03), sección 6.5). Entonces, se registra en el núcleo del IMS usando el SIP por ese túnel de IPSec, utilizando nuevamente el SIM del teléfono, mediante el protocolo de autenticación IMS-AKA (como se describe en el documento 3GPP 24.229 V13.5.1 (2016-03), sección 5.1.1.2.). Por último, una vez que el teléfono está registrado en la red del IMS por IPSec, puede hacer y recibir llamadas y mensajes de texto y realizar otros servicios con la red del IMS, de la misma manera como lo haría por una red de paquetes de radio, de 3G o 4G.

Gestión de servicios de la tarjeta SIM

De acuerdo con una realización de la presente invención, el teléfono está configurado con una opción de configuración específica para seleccionar qué tarjeta SIM utilizar para la autenticación de llamadas Wifi, lo que significa que sería capaz de seleccionar la tarjeta SIM que se va a utilizar para los procedimientos de autenticación de EAP-AKA e IMS-AKA. Por lo tanto, es posible acceder al servicio de Llamadas Wifi con una tarjeta SIM diferente a la del proveedor nativo del servicio. Una de las principales ventajas de esta funcionalidad es aislar el procedimiento de autenticación del canal de comunicación que, en los dispositivos del estado de la técnica, es el mismo, por lo que podría ser posible conectarse al servicio de Llamadas Wifi a través de todos los canales de conectividad disponibles para el teléfono, de Wifi y de 3G/4G.

Por lo tanto, se necesita una nueva característica de configuración en el teléfono inteligente para elegir qué conexión de datos elegir, en caso de que tenga llamadas Wifi - habilitar la conexión de datos del SIM secundario (además de Wifi) para el registro de llamadas Wifi, que se realiza mediante el establecimiento del túnel de IPSec a la EPDG (Pasarela Evolucionada de Datos en Paquetes) (tal como se define en el documento 3GPP 23.234, V12.0.0 (2014-09), sección 5.7), autenticando aún a la vez, utilizando la tarjeta SIM primaria.

La **figura 2** muestra el flujo implicado en un SIM Dual, con registro de llamadas de Wifi. Una vez que se habilita la configuración anterior, se abrirá un túnel IPSec (20) sobre la conexión de datos SIM secundaria (21), pero todavía utilizando la SIM primaria (p-SIM) (22) para la autenticación en el túnel IPSec EPDG (23).

Una vez establecido el túnel de IPSec, el equipo de mano (24) establecerá el registro del SIP sobre la autenticación del túnel de IPSec, utilizando las credenciales de la SIM primaria (como se describe en el documento 3GPP 24.229 V13.5.1 (2016-03), sección 5.1.1.2.2).
Tras el registro exitoso del SIP, el usuario podrá acceder a todos los servicios de voz, de mensajería y de otros

servicios de telecomunicaciones de la red del operador de la SIM primaria (25), mediante el servicio VoWifi, a través del canal de datos (26) proporcionado por la red del operador del SIM secundario (27).

Como se ha mencionado antes, en el caso de que el SIM secundario sea un eSIM, el operador puede proveerlo previamente en la eUICC del teléfono inteligente, o el usuario puede adquirirlo electrónicamente en línea, después de adquirir el dispositivo móvil.

A continuación, se proporciona el diagrama de secuencia de la configuración de servicio completa para una realización de la presente invención. Por lo tanto, el *flujo total para los dispositivos de SIM Dual con configuración del servicio de Llamadas Wifi* se divide en 4 etapas diferentes:

1. **Configuración del canal S1**, donde el dispositivo establece la conectividad de LTE con el Núcleo Evolucionado por Paquetes en el Operador Móvil.

2. La **creación de canales de IPSec**, donde el dispositivo establece la conectividad del TCP (*Protocolo de Control de Transmisión*) con la ePDG para el servicio de Llamadas Wifi.

3. La configuración de **canales del GTP** (Protocolo de tunelación del GPRS), en esta etapa, tiene establecido el túnel del GPRS para la comunicación entre la ePDG (Pasarela Evolucionada de Datos en Paquetes) y la PGW (Pasarela de Red de Datos en Paquetes), y también para el descubrimiento de la P-CSCF (Función de Control de Sesión de Llamada - Delegada).

4. **Registro del IMS** (Subsistema de Multimedios de IP), cuando el equipo de mano está registrado en el núcleo del IMS para comenzar a utilizar todos los servicios de voz y de mensajes.

La **figura 3** desvela la primera etapa del flujo total para los dispositivos de SIM Dual con la configuración del servicio de Llamadas Wifi, de acuerdo con una realización de la invención. Por lo tanto, se explica a continuación toda la secuencia de mensajes (301 a 330) para establecer el canal S1 con el operador visitado (30) que da soporte al Canal de Servicios de Datos por la primera red de comunicación móvil, en este caso, de 3G/4G, y que va a ser utilizado para el servicio VoWifi con el operador de origen del abonado.

301. El proceso comienza con la Configuración de S1, donde el eNB (31) está unido inicialmente a la red. El eNB es el elemento de red que da soporte a la interfaz aérea de la LTE.
302. La Entidad de Gestión Móvil (MME) (32) registra con éxito el eNodoB. Mientras el eNB esté unido correctamente, la configuración de S1 permanecerá intacta.
303. El teléfono inteligente (24) lee el valor inicial del vector de autenticación a partir del registro de EFimsi, que se utilizará para la configuración del canal S1 con la Pasarela Servidora (SGW).
304. El registro de EFimsi que identifica un SIM se obtiene del SIM secundario (21).
305. Una vez que el teléfono inteligente aparece, se establece una conexión de control de recursos de radio (RRC) para la comunicación con la red.
306. El teléfono inteligente, a continuación, envía una solicitud de anexión, junto con una petición de conectividad de PDN a la red. La anexión es para unirse a la red.
307. Una vez que la MME recibe la solicitud de anexión, consulta el HSS por detalles de autenticación.
308. El HSS (Servidor de Abonado Doméstico) (35) envía entonces los vectores de autenticación a la MME en una respuesta de información de autenticación.
309. La red solicita al teléfono inteligente los vectores de autenticación.
310. Envío de una respuesta al teléfono inteligente con un reto de autenticación y seguridad.
311. El teléfono inteligente accede al SIM secundario para ejecutar el algoritmo del GSM y generar una respuesta al reto.
312. El SIM secundario proporciona vectores RES y Kc para el reto de autenticación.
313. La respuesta de autenticación al reto es enviada por el eNodoB a la MME. 314. La MME compara los parámetros de autenticación con lo que el HSS ha enviado.
315. Si los vectores de autenticación coinciden, el teléfono inteligente es autenticado.
316. La respuesta exitosa se envía al teléfono inteligente para su autenticación.
317. Se genera un nuevo grupo de vectores de autenticación ejecutando el algoritmo del GSM para cifrar todos los mensajes intercambiados.
318. Los vectores de autenticación para cifrar mensajes son obtenidos por el teléfono inteligente. 319. El teléfono inteligente envía una solicitud para completar la etapa de seguridad.
320. Después de que el flujo de llamadas de la LTE se desplaza a través de la etapa de seguridad, la red crea las portadoras de EPS.
321. Una vez creadas las portadoras de radio, las direcciones de enlace descendente del eNB se envían a la SGW (36) (Pasarela Servidora) en los mensajes del GTP.
322. Para la funcionalidad de movilidad, la dirección de origen de PMIP (IPv6 Móvil Delegado) y la dirección de atención se asignan en la PGW (37) (Pasarela de PDN).
323. Los parámetros de enlace de PMIP están registrados en la SGW.
324. En esta etapa, el canal del GTP se ha creado y se utilizará para todas las comunicaciones con la SGW.
325. El canal del GTP ha sido establecido.

326. A continuación, se crean las portadoras de radio y las conexiones de RRC se modifican en consecuencia.
327. Las portadoras de radio son enviadas por la red para ser modificadas por el teléfono inteligente. 328. El nuevo conjunto de portadores es reconfigurado por el teléfono inteligente.
329. Y el canal S1 es finalmente creado y establecido.
330. Canal S1 creado.

La **figura 4** desvela la segunda etapa del flujo total para los dispositivos de SIM Dual con la configuración del servicio de Llamadas Wifi, de acuerdo con una realización de la invención. Por lo tanto, se explica a continuación toda la secuencia de mensajes (401 a 422) para establecer el canal de IPSec con el operador de origen que presta soporte al servicio VoWifi. En esta etapa, se obtiene el acceso al núcleo del IMS del operador de origen, para utilizar sus servicios.

401. El teléfono inteligente (24) lee el valor inicial del vector de autenticación desde el registro EFimsi en la SIM primaria (22), que se utilizará para la configuración de los canales de IPSec con la ePDG (42) en la HPLMN (Red Móvil Terrestre Pública Doméstica) del abonado.
402. En esta etapa, el valor inicial de autenticación no se obtiene desde la misma tarjeta SIM que el canal S1.
403. El teléfono inteligente envía Respuesta de EAP/Identidad de AKA para iniciar el proceso de establecimiento del canal de IPSec.
404. La ePDG envía una Solicitud de Diámetro de EAP al servidor de AAA (Autenticación, Autorización y Contabilidad) (43) para iniciar el proceso de autenticación con su par.
405. Respuesta del servidor de AAA con la solicitud de Identidad a la ePDG.
406. La ePDG envía la solicitud de identidad al teléfono inteligente.
407. El teléfono inteligente envía la identidad para el proceso de autenticación; es la IMSI (Identidad Internacional de Abonado Móvil) recuperada desde la SIM primaria.
408. La ePDG envía una Solicitud de Diámetro de EAP al servidor de AAA para iniciar el proceso de autenticación de la identidad proporcionada (IMSI de la SIM primaria).
409. El servidor de AAA captura el perfil de usuario y los vectores de autenticación del HSS (44) a través de la interfaz SWx. El servidor de AAA busca la IMSI del usuario autenticado en base al usuario recibido.
410. El HSS generará luego vectores de autenticación y los enviará de vuelta al servidor de AAA.
411. El servidor de AAA comienza el reto de autenticación y responde con una Respuesta de Diámetro de EAP.
412. La ePDG responde con IKE_AUTH, de acuerdo con el protocolo de Intercambio de Claves de Internet. La identidad es la dirección de IP de la ePDG; la carga útil AUTH autentica la primera respuesta IKE_SA_INIT. El mensaje de EAP recibido desde el servidor de AAA se incluye con el fin de iniciar el procedimiento de EAP sobre IKEv2.
413. Validar AT_MAC a partir del reto del servidor de AAA.
414. El teléfono inteligente comprueba los parámetros de autenticación y solicita nuevos vectores de autenticación a partir de la SIM primaria, para responder al reto de autenticación.
415. Los parámetros de autenticación son recuperados desde la SIM primaria.
416. El teléfono inteligente calcula la respuesta al reto usando la PMK (Clave Maestra en Pares) proporcionada por la SIM primaria y el valor de AT_MAC proporcionado para el servidor de AAA.
417. El teléfono inteligente envía la respuesta al reto a la ePDG.
418. La ePDG envía una Solicitud de Diámetro de EAP al servidor de AAA con la respuesta al reto (carga útil del EAP).
419. El servidor de AAA actualiza el HSS con la información de Dirección del Servidor de AAA para el usuario autenticado.
420. El HSS envía la Respuesta de Asignación del Servidor.
421. El servidor de AAA envía una Respuesta de Diámetro de EAP exitosa a la ePDG si el abonado está autorizado para el acceso no del 3GPP.
422. La ePDG envía una respuesta de éxito del EAP y se establece el canal de IPSec.

La **Figura 5** desvela las etapas tercera y cuarta del flujo total para los dispositivos de SIM Dual con la configuración del servicio de Llamadas Wifi, de acuerdo con una realización de la invención. Por lo tanto, a continuación se explica toda la secuencia de mensajes (501 a 523) para establecer el canal del GTP y establecer el registro del IMS en el núcleo del IMS del operador de origen, lo que permitirá el uso de todos los servicios del IMS en el teléfono inteligente, a través de los servicios de datos de 3G/4G del operador visitado.

501. El teléfono inteligente descubre la GW de la PDN (Agente de Origen) mediante IKEv2 durante la configuración del túnel. Se establece una asociación de seguridad entre el teléfono inteligente y la GW de la PDN, para asegurar los mensajes entre el UE (51) (equipo de usuario) y la GW de la PDN (52), y para la autenticación entre el UE y la GW de la PDN. El teléfono inteligente inicia el establecimiento de la asociación de seguridad utilizando IKEv2.
502. La ePDG (42) inicia la creación de canales del GTP con la P-CSCF (53) a través de la interfaz S2b, usando el APN (Nombre de Punto de Acceso) especificado por el teléfono inteligente en la solicitud de autenticación de IKEv2.
503. El teléfono inteligente se une a la P-CSCF antes de realizar los registros del IMS y el inicio de las sesiones del SIP; para la unión a una P-CSCF dada, el UE realiza los procedimientos de descubrimiento de P-CSCF. En estos procedimientos, el UE primero establece la portadora de la red de acceso de conectividad de IP (IP-CAN). Entonces, el UE envía una consulta al servidor del DHCP para recuperar las direcciones de IP y el FQDN (Nombre

de Dominio Totalmente Calificado) de la P-CSCF. Después de la consulta al DHCP, el UE realiza una consulta al DNS sobre el FQDN recibido desde el servidor del DHCP. En respuesta a la consulta del DNS, se devuelve la dirección de IP de la P-CSCF. Esto se conoce como el procedimiento de DHCP-DNS para el descubrimiento de P-CSCF. Sin embargo, en algunas realizaciones, puede ser posible que el FQDN de la P-CSCF esté configurado previamente en el UE. En estos escenarios, el UE puede consultar directamente al servidor de DNS y obtener la dirección de IP de la P-CSCF.

504. La PGW proporciona la dirección de IP de la P-CSCF en la respuesta a la ePDG para el procedimiento de creación de sesión del GTP.

505. La dirección de IP de la P-CSCF se proporciona al teléfono inteligente en la respuesta de la solicitud de autenticación de IKEv2 desde la ePDG. En este punto, se establece el canal del GTP entre la ePDG y la PGW, y el teléfono inteligente se puede conectar directamente con la P-CSCF para comenzar el registro del IMS.

506. Todos los canales se establecen entre el teléfono inteligente y la red central del IMS, por lo que se inicia el procedimiento de registro de IMS-AKA y un mensaje de REGISTRO del SIP es enviado por el teléfono inteligente con la IMPI/IMPU (Identidad Pública de Multimedios del IP) recuperada desde la tarjeta SIM primaria, insertada en el dispositivo sin parámetros de autenticación.

507. La P-CSCF envía un comando de Solicitud-de-Autorización-de-Usuario (UAR) al HSS (44) con el fin de solicitar la autorización del registro del teléfono inteligente. 508. Si existe el abonado en el HSS, se envía una Respuesta-de-Autorización-de-Usuario (UAA) exitosa a la P-CSCF.

509. Después de validar la IMPI/IMPU en el HSS, la P-CSCF remite la petición de REGISTRAR del SIP a la S-CSCF (54), para comenzar el proceso de autenticación con el abonado.

510. La S-CSCF envía un comando de Solicitud-de-Autorización-de-Multimedios (MAR) al HSS con el fin de solicitar información de seguridad para la IMPI proporcionada por el teléfono inteligente.

511. El HSS proporciona los vectores de autenticación para el reto de autenticación con el teléfono inteligente.

512. La S-CSCF responde con un mensaje 401 NO-AUTORIZADO del SIP, donde los vectores las autenticaciones se colocan en la carga útil del mensaje. Es el comienzo del reto para la autenticación del teléfono inteligente.

513. El mensaje 401 NO-AUTORIZADO del SIP es remitido por la P-CSCF al teléfono inteligente.

514. El teléfono inteligente ejecuta el algoritmo del GSM para generar los parámetros de autenticación a partir de la tarjeta SIM primaria, utilizando los vectores de autenticación proporcionados por el HSS.

515. Los parámetros de autenticación RES y Kc, a utilizar en el reto de autenticación, se obtienen desde la tarjeta SIM primaria.

516. Un nuevo mensaje de REGISTRO del SIP es enviado por el teléfono inteligente a la P-CSCF, esta vez, con los parámetros de autenticación para responder al reto de autenticación iniciado por la S-CSCF.

517. La P-CSCF envía un comando de Solicitud-de-Autorización-de-Usuario (UAR) al HSS con el fin de solicitar la autorización del registro del teléfono inteligente.

518. Si existe el abonado en el HSS, una Respuesta-de-Autorización-de-Usuario (UAA) exitosa es enviada a la P-CSCF.

519. Después de validar la IMPI/IMPU en el HSS, la P-CSCF remite la petición de REGISTRAR del SIP a la S-CSCF para continuar el proceso de autenticación con el abonado.

520. La S-CSCF valida los parámetros de autenticación enviados por el teléfono inteligente con los vectores de autenticación proporcionados por el HSS. Si coincide la información de autenticación, la S-CSCF envía un comando de Solicitud-de-Asignación-de-Servidor (SAR) con el fin de solicitarle almacenar el nombre del servidor que está actualmente sirviendo al usuario.

521. Si el servidor se almacena correctamente, el HSS envía un comando de Respuesta-de-Asignación-de-Servidor (SAA) exitoso, que contiene la información que la S-CSCF necesita para dar servicio al usuario.

522. La S-CSCF responde con un mensaje 200 OK del SIP, que significa que el proceso de registro se ha concluido con éxito y que el teléfono inteligente puede comenzar a utilizar los servicios de llamadas y mensajes en el núcleo del IMS.

523. El mensaje 200 OK del SIP desde la S-CSCF es remitido por la P-CSCF al teléfono inteligente; en este momento, el teléfono inteligente está totalmente operativo para enviar comandos del SIP para utilizar los servicios de la plataforma del IMS.

Por lo tanto, en vista del flujo máximo para dispositivos de SIM Dual con la configuración del servicio de Llamadas Wifi descrita anteriormente, de acuerdo con una realización de la invención, se obtienen varias ventajas, tales como permitir desacoplar el abono móvil que se utiliza para fines de conectividad de datos y el utilizado para los servicios de comunicación móvil, es decir, el que determina la identidad utilizada y, específicamente, para el caso en que estos servicios se ofrecen a través de una red de terceros que, en este caso, es otra red móvil. Esto permite, por ejemplo, la prestación de servicios eficaces de itinerancia al cliente, con conectividad local desvinculada del operador de acogida. Por lo tanto, el cliente no está vinculado a los acuerdos de itinerancia entre su operador y los operadores en el país visitado, pero puede utilizar sus recursos de origen mediante cualquier operador en el país, con servicios de datos y cobertura total.

Además, en base al uso del eSIM, podría ser posible hacerlo de forma transparente por los operadores, pero esta solución no sólo es aplicable para el caso del uso del eSIM; podría ser aplicable también para dispositivos físicos de SIM dual; por supuesto, es más transparente y cómodo con el eSIM, pero podría ser posible proporcionar ambas opciones.

REIVINDICACIONES

1. Procedimiento de registro de un dispositivo de comunicación móvil (24) para llamadas WiFi, para acceder a través de una segunda red de telecomunicaciones móviles (27), a los servicios ofrecidos por una primera red de telecomunicaciones móviles (25); comprendiendo el procedimiento las etapas de:

a) establecer un primer canal de comunicación de datos (26) entre el dispositivo de comunicación móvil y la segunda red de telecomunicaciones móviles, en base a la información almacenada en una tarjeta SIM secundaria (21), asociada al dispositivo de comunicación móvil;
b) establecer un segundo canal de comunicación (20) entre el dispositivo de comunicación móvil y la primera red de telecomunicaciones móviles utilizando el primer canal de comunicación de datos mediante el establecimiento de un túnel entre el dispositivo móvil y un ePDG, Puerta de Enlace de Datos en Paquetes evolucionado, (23) elemento de red de la primera red de telecomunicaciones móviles, en el que el túnel es un túnel seguro implementado bajo Protocolo de Seguridad de Internet IPsec, y en el que un usuario del dispositivo de comunicación móvil se autentica en la primera red de telecomunicaciones móviles utilizando la información almacenada en una tarjeta SIM primaria (22) asociada al dispositivo de comunicación móvil;
c) registrar, a través del segundo canal de comunicación, el usuario del dispositivo de comunicación móvil en la primera red de telecomunicaciones móviles, usando la información almacenada en la tarjeta SIM primaria;
d) acceder desde el dispositivo de comunicación móvil a los servicios ofrecidos por la primera red de telecomunicaciones móviles, a través del segundo canal de comunicación.

2. Procedimiento de acuerdo con la reivindicación 1, en el que la segunda red de telecomunicaciones móviles es una red de datos de radio celular.

3. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores en el que la autenticación en la primera red de telecomunicaciones móviles utilizando la información almacenada en una tarjeta SIM primaria comprende la lectura de un valor inicial vectorial de autenticación almacenado en la tarjeta SIM primaria.

4. Procedimiento de acuerdo con la reivindicación 3, en el que establecer un segundo canal de comunicación entre el dispositivo de comunicación móvil y la primera red de telecomunicaciones móviles utilizando el primer canal de comunicación comprende, además el establecimiento de un túnel GPRS para la comunicación entre la ePDG y una PGW, Puerta de Enlace de Datos en Paquetes, elemento de red de la primera red de telecomunicaciones móviles.

5. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores en el que el registro del usuario en la primera red de telecomunicaciones móviles comprende un registro SIP a través del segundo canal de comunicación.

6. Procedimiento de acuerdo con la reivindicación 5 en el que el registro SIP se realiza en un Subsistema Multimedia IP IMS, núcleo de la primera red de telecomunicaciones móviles.

7. Procedimiento de acuerdo con la reivindicación 5, en el que el registro SIP comprende un mecanismo de autenticación y control de acceso basado en IMS-AKA.

8. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores en el que la tarjeta SIM secundaria es una tarjeta e-SIM integrada en un chipset UICC del dispositivo de comunicación móvil.

9. Procedimiento de acuerdo con la reivindicación 8, que comprende además proporcionar el chipset UICC con múltiples perfiles de operador de red móvil deshabilitados, que se habilitan y deshabilitan de forma remota actuando en la e-SIM.

10. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores que comprende además la habilitación, por parte del usuario, de un servicio de llamadas Wifi en el dispositivo de comunicación móvil y la selección, por parte del usuario, de una conexión de datos basada en la información almacenada en la tarjeta SIM secundaria para registrarse en dicho servicio de llamadas Wifi, donde dicho servicio de llamadas Wifi es ofrecido por la primera red de telecomunicaciones móviles.

11. Sistema para registrarse en llamadas Wifi que comprende:

- una primera (25) y una segunda (27) red de telecomunicaciones móviles;
- una tarjeta SIM primaria (22) y una secundaria (21);
- un dispositivo de comunicación móvil (24) configurado para:

  - establecer un primer canal de comunicación de datos (26) con la segunda red de telecomunicaciones móviles, en base a la información almacenada en la tarjeta SIM secundaria (21);
  - establecer un segundo canal de comunicación (20) con la primera red de telecomunicaciones móviles utilizando el primer canal de comunicación de datos mediante el establecimiento de un túnel entre el dispositivo móvil y una ePDG, Puerta de Enlace de Datos en Paquetes evolucionado, (23) elemento de red de la primera red de telecomunicaciones móviles, en el que el túnel es un túnel seguro implementado bajo Protocolo de Seguridad de Internet IPsec, y en el que un usuario del dispositivo de comunicación móvil se autentica en la

primera red de telecomunicaciones móviles utilizando la información almacenada en una tarjeta SIM primaria (22);
- registrar, a través del segundo canal de comunicación, el usuario del dispositivo de comunicación móvil en la primera red de telecomunicaciones móviles, usando la información almacenada en la tarjeta SIM primaria;
- acceder a los servicios ofrecidos por la primera red de telecomunicaciones móviles, a través del segundo canal de comunicación.

12. Dispositivo móvil para registrarse en llamadas Wifi para acceder a través de una segunda red de telecomunicaciones móviles (27) a los servicios ofrecidos por una primera red de telecomunicaciones móviles (25), en el que el dispositivo móvil está configurado para:

a) establecer un primer canal de comunicación de datos (26) con la segunda red de telecomunicaciones móviles, en base a la información almacenada en una tarjeta SIM secundaria (21), asociada al dispositivo de comunicación móvil;
b) establecer un segundo canal de comunicación (26) con la primera red de telecomunicaciones móviles utilizando el primer canal de comunicación de datos mediante el establecimiento de un túnel entre el dispositivo móvil y una ePDG, Puerta de Enlace de Datos en Paquetes evolucionado, (23) elemento de red de la primera red de telecomunicaciones móviles, en el que el túnel es un túnel seguro implementado bajo Protocolo de Seguridad de Internet IPsec, y en las que un usuario del dispositivo de comunicación móvil se autentica en la primera red de telecomunicaciones móviles utilizando la información almacenada en una tarjeta SIM primaria (22) asociada al dispositivo de comunicación móvil;
c) registrar, a través del segundo canal de comunicación, el usuario del dispositivo de comunicación móvil en la primera red de telecomunicaciones móviles, usando la información almacenada en la tarjeta SIM primaria;
d) acceder a los servicios ofrecidos por la primera red de telecomunicaciones móviles, a través del segundo canal de comunicación.

13. Producto de programa informático que comprende código de programa informático adaptado para realizar el procedimiento de acuerdo con cualquiera de las reivindicaciones 1-10 cuando dicho código de programa se ejecuta en un ordenador, un procesador de señal digital, una matriz de puerta programable en campo, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

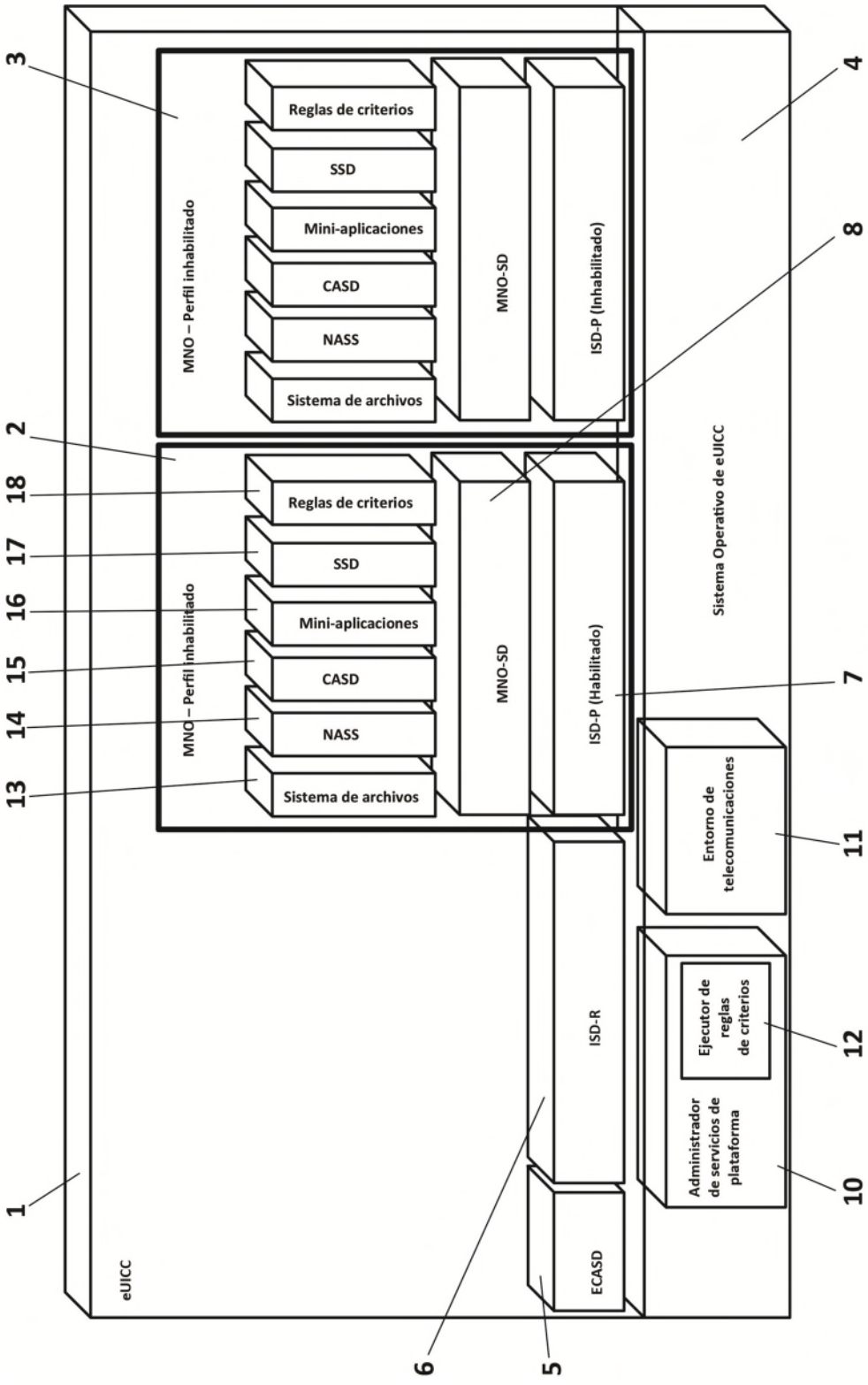
1
2
3
4
5
6
7
8
10
11
12
13
14
15
16
17
18
eUICC
ECASD
ISD-R
MNO – Perfil inhabilitado
Reglas de criterios
SSD
Mini-aplicaciones
CASD
NASS
Sistema de archivos
MNO-SD
ISD-P (Inhabilitado)
MNO – Perfil inhabilitado
Reglas de criterios
SSD
Mini-aplicaciones
CASD
NASS
Sistema de archivos
MNO-SD
ISD-P (Habilitado)
Sistema Operativo de eUICC
Entorno de telecomunicaciones
Ejecutor de reglas de criterios
Administrador de servicios de plataforma

FIG. 1

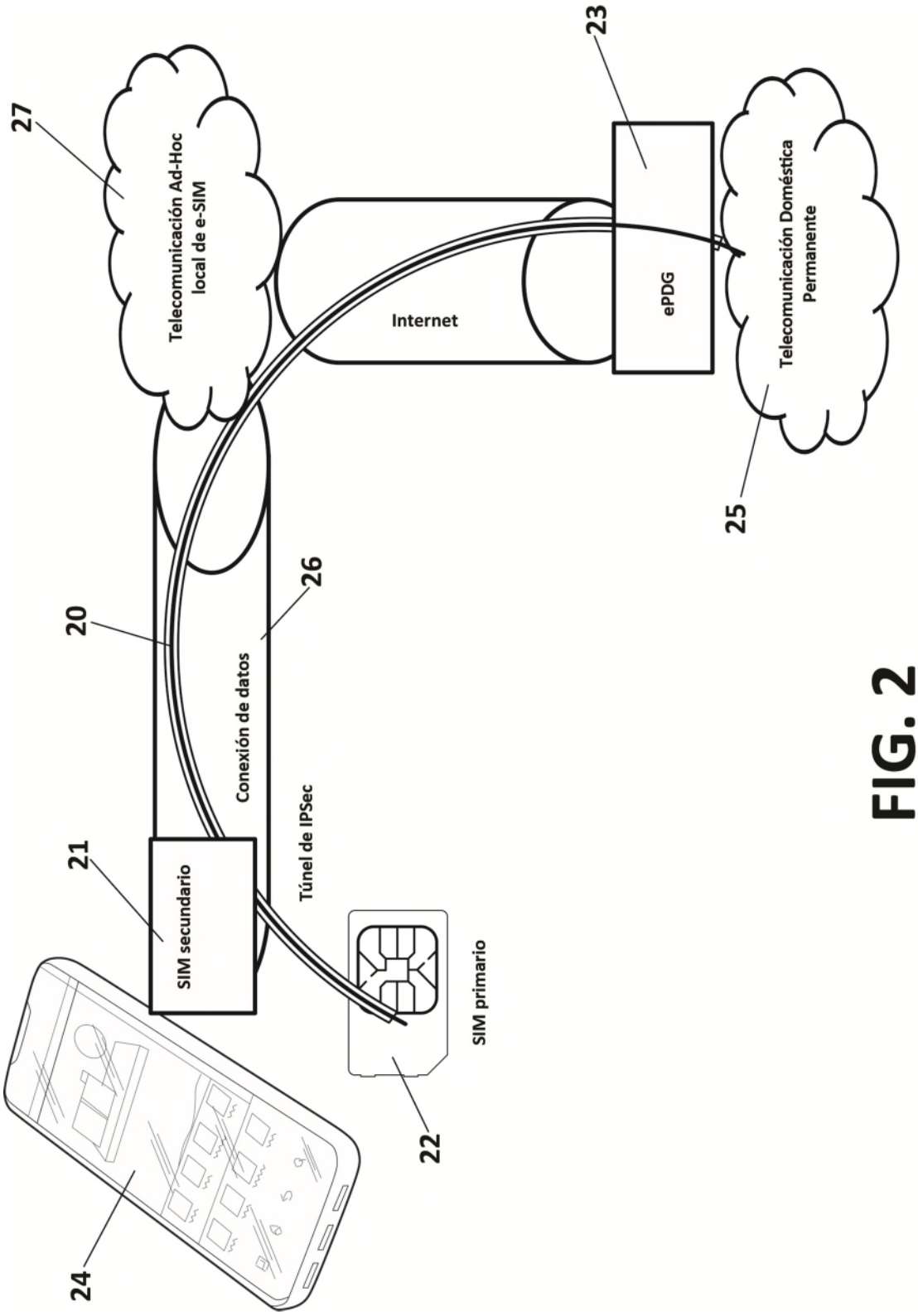
27
Telecomunicación Ad-Hoc local de e-SIM
23
Internet
ePDG
Telecomunicación Doméstica Permanente
25
20
26
Conexión de datos
Túnel de IPSec
21
SIM secundario
SIM primario
22
24

FIG. 2

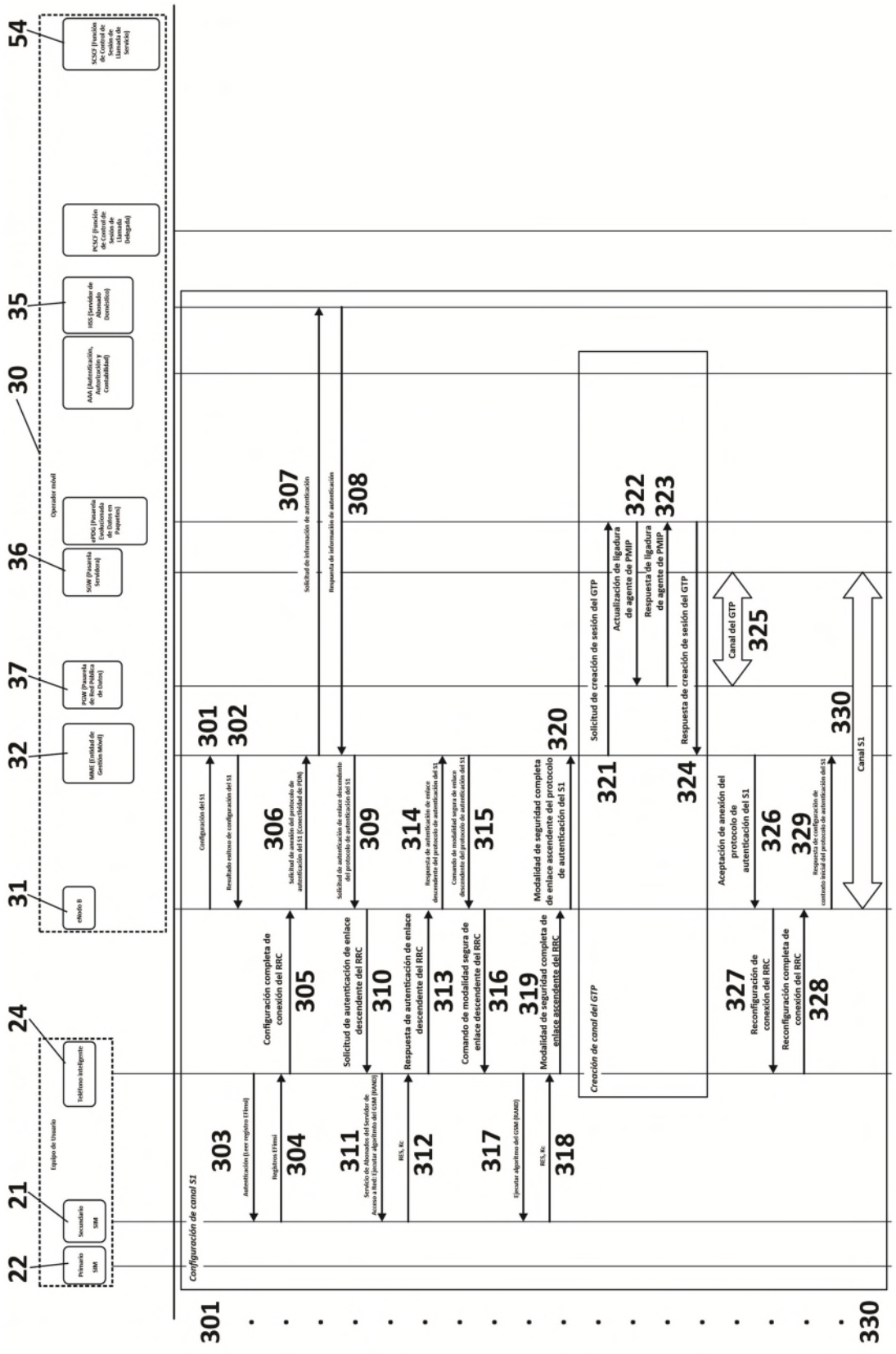
Equipo de Usuario
Teléfono Inteligente
Secundario SIM
Primario SIM
eNodo B
MME (Entidad de Gestión MME)
PCRF (Pasarela de Política de Red)
SGW (Pasarela Servidora)
ePDG (Pasarela Evolucionada de Datos en Paquetes)
Operador móvil
AAA (Autenticación, Autorización y Contabilidad)
HSS (Servidor de Abonado Doméstico)
PCSCF (Función de Control de Sesión de Llamada (delegada)
SCSCF (Función de Control de Sesión de Llamada de Servicio)
Configuración del S1
Resultado exitoso de configuración del S1
Solicitud de información de autenticación
Respuesta de información de autenticación
Solicitud de creación de sesión del GTP
Actualización de ligadura de agente de PMIP
Respuesta de ligadura de agente de PMIP
Respuesta de creación de sesión del GTP
Canal del GTP
Canal S1
Configuración de canal S1
Creación de canal del GTP
Autenticación (Leer registro EImsi)
Registros EImsi
Configuración completa de conexión del RRC
Solicitud de autenticación de enlace descendente del RRC
Respuesta de autenticación de enlace descendente del RRC
Comando de modalidad segura de enlace descendente del RRC
Modalidad de seguridad completa de enlace descendente del RRC
Aceptación de anexión del protocolo de autenticación del S1
Reconfiguración de conexión del RRC
Reconfiguración completa de conexión del RRC
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330

FIG. 3

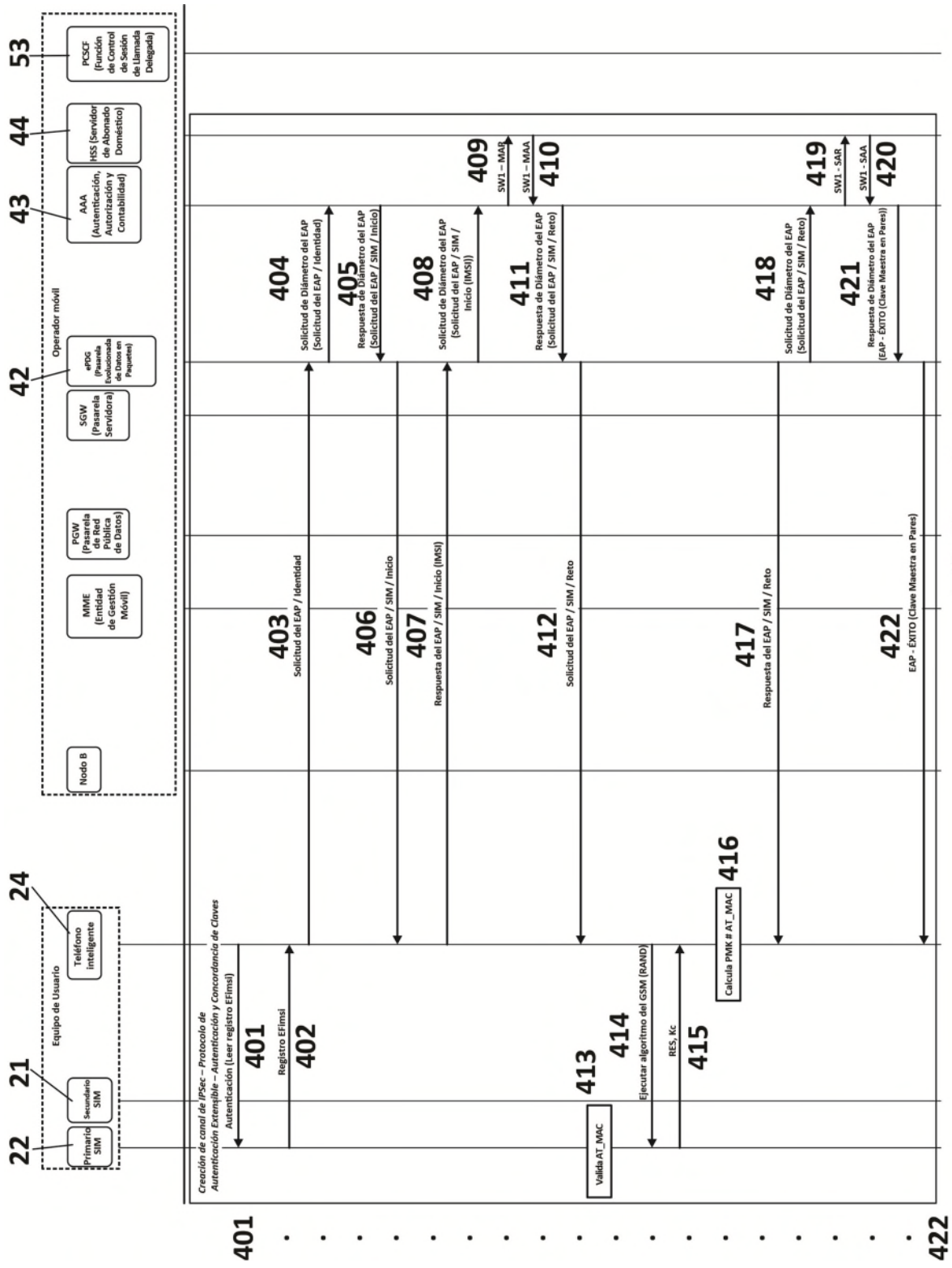
Equipo de Usuario
Primario SIM
Secundario SIM
Teléfono inteligente
Operador móvil
Nodo B
MME (Entidad de Gestión Móvil)
PGW (Pasarela de Red Pública de Datos)
SGW (Pasarela Servidora)
ePDG (Pasarela Evolucionada de Datos en Paquetes)
AAA (Autenticación, Autorización y Contabilidad)
HSS (Servidor de Abonado Doméstico)
PCSCF (Función de Control de Sesión de Llamada Delegada)
Creación de canal de IPSec – Protocolo de Autenticación Extensible – Autenticación y Concordancia de Claves
Autenticación (Leer registro EFimsi)
401 Registro EFimsi
402 Solicitud del EAP / Identidad
403 Solicitud del EAP / SIM / Inicio
404 Solicitud de Diámetro del EAP (Solicitud del EAP / Identidad)
405 Respuesta de Diámetro del EAP (Solicitud del EAP / SIM / Inicio)
406 Solicitud del EAP / SIM / Inicio (IMSI)
407 Solicitud de Diámetro del EAP (Solicitud del EAP / SIM / Inicio (IMSI))
408 Respuesta de Diámetro del EAP (Solicitud del EAP / SIM / Reto)
409 SW1 – MAR
410 SW1 – MAA
411 Solicitud del EAP / SIM / Reto
412 Valida AT_MAC
413 Ejecutar algoritmo del GSM (RAND)
414 RES, Kc
415 Calcula PMK # AT_MAC
416 Respuesta del EAP / SIM / Reto
417 Solicitud de Diámetro del EAP (Solicitud del EAP / SIM / Reto)
418 SW1 - SAR
419 SW1 - SAA
420 Respuesta de Diámetro del EAP (EAP - ÉXITO (Clave Maestra en Pares))
421 EAP - ÉXITO (Clave Maestra en Pares)
422
401
422

FIG. 4

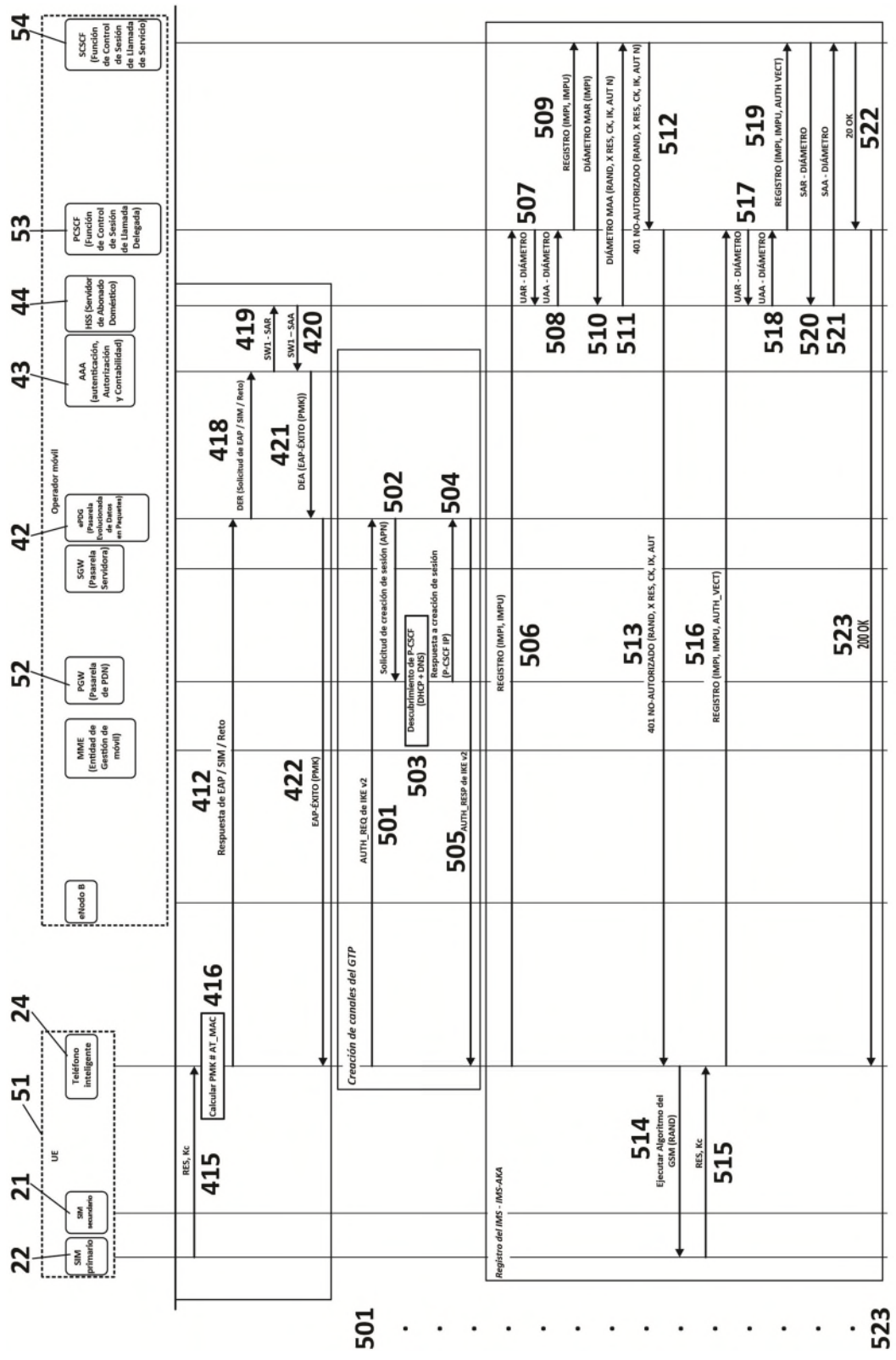
UE
SIM primario
SIM secundario
Teléfono inteligente
eNodo B
MME (Entidad de Gestión de móvil)
PGW (Pasarela de PDN)
SGW (Pasarela Servidora)
ePDG (Pasarela Evolucionada de Datos en Paquetes)
Operador móvil
AAA (autenticación, Autorización y Contabilidad)
HSS (Servidor de Abonado Doméstico)
PCSCF (Función de control de sesión de Llamada Delegada)
SCSCF (Función de Control de Sesión de Llamada de Servicio)
RES, Kc
Calcular PMK # AT_MAC
Respuesta de EAP / SIM / Reto
EAP-ÉXITO (PMK)
DER (Solicitud de EAP / SIM / Reto)
DEA (EAP-ÉXITO (PMK))
SW1 - SAR
SW1 – SAA
Creación de canales del GTP
AUTH_REQ de IKE v2
Solicitud de creación de sesión (APN)
Descubrimiento de P-CSCF (DHCP + DNS)
Respuesta a creación de sesión (P-CSCF IP)
AUTH_RESP de IKE v2
REGISTRO (IMPI, IMPU)
UAR - DIÁMETRO
UAA - DIÁMETRO
REGISTRO (IMPI, IMPU)
DIÁMETRO MAR (IMPI)
DIÁMETRO MAA (RAND, X RES, CK, IK, AUT N)
401 NO-AUTORIZADO (RAND, X RES, CK, IK, AUT N)
401 NO-AUTORIZADO (RAND, X RES, CK, IK, AUT
REGISTRO (IMPI, IMPU, AUTH_VECT)
UAR - DIÁMETRO
UAA - DIÁMETRO
REGISTRO (IMPI, IMPU, AUTH VECT)
SAR - DIÁMETRO
SAA - DIÁMETRO
200 OK
Ejecutar Algoritmo del GSM (RAND)
RES, Kc
Registro del IMS - IMS-AKA
501
523
22
21
51
24
52
42
43
44
53
54
415
416
412
422
501
503
505
502
504
418
421
419
420
506
513
516
523
507
508
509
510
511
512
517
518
519
520
521
522
514
515

FIG. 5