

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 574 986**

51 Int. Cl.:

**H04W 8/26** (2009.01)

**H04W 4/12** (2009.01)

**H04W 76/02** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **02.04.2009 E 09726560 (7)**

97 Fecha y número de publicación de la concesión europea: **09.03.2016 EP 2294848**

54 Título: **Red de telecomunicaciones**

30 Prioridad:

**02.04.2008 GB 0805964**

**20.08.2008 GB 0815200**

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

**23.06.2016**

73 Titular/es:

**VODAFONE GROUP PLC (100.0%)**  
**Vodafone House The Connection Newbury**  
**Berkshire RG14 2FN, GB**

72 Inventor/es:

**GUMBRELL, RICHARD;**  
**SANDIESON, GRAEME;**  
**REEVE, GREG;**  
**SMITH, TONY y**  
**PRABDIAL, YAKEEN**

74 Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

**ES 2 574 986 T3**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

## Red de telecomunicaciones

La presente invención se refiere a una red de telecomunicaciones. En particular, la invención se refiere a una red celular que permite que los terminales con módulos de identificación establezcan una comunicación de datos en la que dicho módulo de identificación es asignado a un número telefónico único solamente cuando es necesario.

En las redes de telecomunicaciones celulares convencionales, la activación de un módulo de identificación de abonado (SIM, subscriber identification module) requiere que se satisfagan ciertas condiciones previas. De particular interés en este caso, el SIM debe estar asociado con un número de teléfono único (MSISDN). Este número telefónico familiar es utilizado generalmente por una parte que llama que desea realizar una llamada de voz (o de video) al terminal móvil en el que ha sido introducido el SIM. Sistemáticamente, el número telefónico es seleccionado (ya sea automáticamente o, en algunos casos, por los propios usuarios) a partir de un intervalo de números MSISDN disponibles pertenecientes a la compañía operadora de suministro, y el número seleccionado se asigna al SIM cuando la red de la compañía operadora se dirige al SIM por primera vez: generalmente, esto significa que el número telefónico tiene que ser asignado antes de que el usuario active por primera vez el SIM bajo un acuerdo de prepago o contractual.

El operador de red soporta un coste asociado con el suministro de un MSISDN válido al SIM, tanto por la reserva del MSISDN (reguladores tales como la ITU asignan intervalos de números MSISDN a las compañías operadoras) como por el tiempo del personal de ventas y los costes generales relativos al registro del número seleccionado para su utilización.

Cuando parece que el SIM ya no se utiliza durante un periodo predeterminado (o no se ha utilizado nunca), los operadores de red observan habitualmente este hecho e inician un proceso de "cuarentena" para devolver el número telefónico al conjunto de números disponibles. Por supuesto, este proceso de cuarentena tiene un coste asociado: también lo tiene la reasignación del número MSISDN, tal como ocurrirá finalmente cuando éste se confirme como no utilizado tras la expiración del periodo de cuarentena.

Tal como el lector apreciará fácilmente, el suministro de SIMs que se utilizan infrecuentemente o nunca, representa un claro inconveniente para el operador de red. Este inconveniente es significativo incluso considerando el suministro convencional de SIM a teléfonos móviles y tarjetas de datos/módems. Sin embargo, existe una tendencia actual a incorporar, o habilitar de otro modo por SIM, una gama muy extensa de artículos informáticos y otros artículos electrónicos. Por ejemplo, los PCs portátiles, los PCs ultra-móviles (UMPC, ultra-mobile PCs), los asistentes digitales personales (PDA, personal digital assistants), los dispositivos de posicionamiento por satélite, los descodificadores (STB, set top boxes), los puntos de acceso inalámbrico (APs, access points) e incluso los ordenadores a bordo de vehículos pueden estar, y últimamente están a menudo, equipados con módulos que aceptan SIM para permitir la comunicación sobre redes de telecomunicación celular. Claramente, esta tendencia implica un aumento concomitante en el número de SIM no utilizadas o utilizadas infrecuentemente, y un nivel consecuentemente mayor de trastorno para el operador de red que desea habilitar dichos dispositivos.

Surge otro problema en relación con la fabricación y gestión de tarjetas SIM para terminales telemáticos (por ejemplo, ordenadores a bordo de coches), en los que es deseable que los terminales se puedan exportar a diversas localizaciones geográficas, cada una con su propia red de telecomunicación.

Tal como se describe en las patentes anteriores GB2378097, GB2378094 y GB2378095, el problema se puede solucionar asegurándose de que todos los parámetros específicos y claves de operador relevantes se almacenan previamente en el SIM, en el momento de la fabricación. Por consiguiente, un SIM preparado adecuadamente se puede volver a registrar desde una red propia a otra red propia, cuando sea necesario. El SIM recibe instrucciones relativas a qué claves debe autenticación de utilizar en cada territorio y un nuevo número de identificador SIM correspondiente, IMSI.

Como resultado, cuando se exportan los coches, los SIM se pueden configurar para el país del fabricante y a continuación volver a configurarse para el país final. El procedimiento puede aplicar asimismo a otros dispositivos y pueden ser reconfigurados indefinidamente. Por lo tanto, un terminal puede ser utilizado en otra red (no como abonado itinerante) durante un tiempo significativo sin que se emita una nueva tarjeta SLIM. Claramente, la no utilización o la utilización infrecuente de dichos SIM "pre-equipados" no haría sino aumentar los problemas esbozados anteriormente, dado que esta solución requiere el suministro de una serie de MSISDN disponibles, uno para cada territorio contemplado en la fabricación.

En la solicitud de patente del Reino Unido GB 0805964.4 en tramitación con la presente, se propone un nuevo procedimiento y sistema para solucionar algunos de los problemas a los que se ha hecho referencia. En esta solución, se pueden establecer sesiones de comunicaciones de datos para terminales con módulos de identificación que tienen solamente números IMSI (y no números MSISDN) (por lo tanto, eludiendo la necesidad del suministro o de la cuarentena de SIM). Esto se consigue introduciendo elementos de red adicionales que pueden identificar terminales con dichos módulos de identificación, y manejar de manera consistente sus solicitudes de sesiones de datos. El sistema de la memoria GB 0805964.4 es adecuado principalmente para comunicaciones de sólo datos.

5 Sin embargo, existen circunstancias en las que un trayecto temporal de comunicaciones "de retorno" puede ser atractivo en asociación con un servicio por lo demás de sólo datos. Esto podría ser un servicio de telefonía (por ejemplo, voz CS, SMS, USSD, MMS, etc.) en el que el servidor inicia la comunicación con el dispositivo cliente. Un ejemplo de dicha circunstancia en telemática puede ser la necesidad de comunicaciones desde un proveedor de servicios telemáticos a un cliente telemático particular, requeridas a causa de un fallo o de patrones de uso anómalos. Convencionalmente, encaminar mensajes en este sentido requeriría un número telefónico único, tal como el MSISDN asociado con cada SIM.

10 En dichas circunstancias, permanecen los inconvenientes de utilizar SIMs con su MSISDN suministrado: el suministro y la cuarentena de estos SIM en terminales que nunca necesitan este canal de retorno haría prohibitivamente costosa la oferta del servicio a todos los dispositivos.

Por lo tanto, un objetivo de la invención es evitar, o por lo menos mitigar, los problemas mencionados anteriormente.

15 De acuerdo con un aspecto de la presente invención, se da a conocer una red de telecomunicaciones celular para asociar temporalmente números de conexión únicos con terminales que tienen módulos de identificación de testigo, incluyendo la red: un registro de posiciones para recibir solicitudes para acceder a la red desde terminales y, si las solicitudes están asociadas con un módulo de identificación de testigo, redirigir las solicitudes; un registro de testigos que recibe dichas solicitudes redirigidas, genera datos de identificación de conexión de testigo y transmite los datos de identificación de conexión de testigo al registro de posiciones para identificar el terminal al registro de posiciones; y un componente de pasarela de red para establecer una comunicación entre la red y el terminal de acuerdo con los datos de identificación de conexión de testigo; comprendiendo además la red: un componente de almacenamiento de red para almacenar una tabla de números de conexión únicos; y un componente de análisis sintáctico de mensajería para procesar mensajes dirigidos a terminales que tienen módulos de identificación de testigo, seleccionar un número de conexión determinado desde la tabla de números de conexión, asociar el número seleccionado con un archivo de registro de testigos para un módulo de identificación de testigo determinado y redirigir los mensajes al terminal que tiene el módulo de identificación de testigo determinado utilizando el número asociado, en el que el componente de análisis sintáctico de mensajería está acoplado comunicativamente con el registro de testigos y provoca la asociación del número seleccionado con el módulo de identificación de testigo mediante ordenar retirar de un archivo de registro de posiciones el módulo de identificación de testigo e inyectar el número seleccionado en el archivo de registro de testigos durante la reconexión.

20 La aplicación de análisis sintáctico de mensajería puede además desencadenar un contexto PDP con la confirmación de recepción satisfactoria de uno determinado de dichos mensajes redirigidos dentro del terminal, instigando de ese modo una conexión de datos entre el terminal y el originador de dicho mensaje redirigido.

30 Al completarse el intercambio de datos entre el terminal y el originador de dicho mensaje redirigido, cualquiera del terminal o el originador pueden abandonar el contexto PDP, terminando por lo tanto la sesión de datos.

35 El originador de dicho mensaje redirigido interpreta preferentemente la terminación de una sesión de datos como un desencadenante para volver a retirar el terminal del registro de testigos con el fin de recuperar el número asociado.

El terminal puede estar dotado además de componentes adecuados de altavoz, micrófono y procesamiento de señal.

40 En la totalidad de la presente descripción, se debe entender que el término "registro de posiciones" se refiere a una entidad de red que lleva a cabo la funcionalidad de un HLR, un VLR y/o un componente de pasarela de red, tal como un modo de soporte GPRS de servicio (SGSN, serving GPRS support node).

El registro de posiciones puede estar distribuido, teniendo un punto agregador para agregar funcionalidad de señalización y una entidad de red para llevar a cabo otra funcionalidad de registro de posiciones, estando dicho punto agregador y dicha entidad de red en comunicación entre sí. Ejemplos de otra funcionalidad de registro de posiciones incluyen el almacenamiento temporal de números IMSI.

45 De acuerdo con otro aspecto de la presente invención, se da a conocer un procedimiento para asociar temporalmente números de conexión únicos con dispositivos que tienen módulos de identificación de testigo, comprendiendo el procedimiento, por lo menos: proporcionar un repositorio de números de conexión únicos; en respuesta a una solicitud de comunicación con un dispositivo que incorpora un módulo de identificación de testigo, asignar uno seleccionado de los números del repositorio al primer módulo de identificación de testigo en un registro de testigos; e iniciar un evento de reconexión, ordenando retirar de un archivo de registro de posiciones el módulo de identificación de testigo, e inyectando a continuación el número seleccionado en un archivo de registro de testigos durante la reconexión, proporcionando de ese modo el número asignado al dispositivo.

50 La solicitud de comunicación puede ser una solicitud para entregar un mensaje dirigido a un dispositivo que tiene un módulo de identificación de testigo; en cuyo caso, el procedimiento puede comprender además: recibir dicho mensaje, y redirigir el mensaje al dispositivo utilizando el número asignado.

El procedimiento puede comprender además desencadenar un contexto PDP tras la confirmación de recepción satisfactoria de dicho mensaje redirigido dentro del terminal, instigando de ese modo una conexión de datos entre el dispositivo y el originador de dicho mensaje redirigido.

5 Al completarse el intercambio de datos entre el dispositivo y el originador de dicho mensaje redirigido, el contexto PDP puede ser abandonado, ya sea en el dispositivo o en el originador, terminando de ese modo la sesión de datos.

Una vez completada la comunicación, la asignación del número asignado se puede retirar del registro de posiciones. Por lo tanto, el procedimiento puede comprender además volver a retirar el dispositivo del registro de posiciones a la finalización de la sesión de datos con el fin de recuperar el número asignado.

10 En la totalidad de este documento, el repositorio de números de conexión se considera "único" en tanto que puede haber solamente una instancia de cada número de conexión en la red en cada momento. Por supuesto, un mismo número de conexión puede ser utilizado en serie para más de un dispositivo durante un periodo de tiempo, pero no simultáneamente.

Para una mejor comprensión de la presente invención, se hará referencia a continuación, solamente a modo de ejemplo, a los dibujos adjuntos en los cuales:

15 la figura 1 muestra elementos clave de una red de telecomunicaciones celular, y su funcionamiento;

la figura 2 muestra elementos clave de una red de telecomunicaciones celular, de acuerdo con la solicitud de patente del Reino Unido GB 0805964.4 en tramitación con la presente;

la figura 3 muestra los elementos en el establecimiento de un contexto PDP entre una red GPRS y un terminal (por ejemplo, una estación móvil) como resultado de una solicitud externa de comunicación con el terminal;

20 la figura 4 muestra el flujo de eventos en la provisión de sesiones de datos a un dispositivo para su utilización en un entorno de máquina a máquina, según la memoria GB 0805964.4; y

la figura 5 muestra el flujo de eventos en la activación de un mensaje de proveedor a entregar a un terminal que tiene un módulo de identificación con un IMSI pero no un número telefónico único, de acuerdo con la presente invención.

25 La figura 1 muestra la interrelación de los elementos clave de una red de telecomunicaciones celular que son relevantes para el funcionamiento de la invención.

Una red de telecomunicaciones 100 incluye una serie de estaciones base (BS, base stations) 3, 4, 5, 7, 8 y 9 y una red central 12.

30 Cada estación base (BS) corresponde a una respectiva celda de la red de telecomunicaciones y recibe llamadas desde, y transmite llamadas a un terminal en dicha celda mediante comunicación de radio inalámbrica en uno o ambos de los dominios de conmutación de circuitos o de conmutación de paquetes. Dicho terminal de abonado se muestra como 1. El terminal puede ser un teléfono móvil, un asistente digital personal (PDA) o un ordenador portátil equipado con una tarjeta de datos.

35 Cada estación base comprende una estación transceptora de base (BTS, base transceiver station) y un controlador de estación base (BSC, base station controller). Un BSC puede controlar más de una BTS. Las BTSs y los BSCs comprenden la red de acceso radio.

40 Convencionalmente, las estaciones base están dispuestas en grupos, y cada grupo de estaciones base está controlado por un centro de conmutación móvil (MSC, mobile switching centre), tal como el MSC 2 para las estaciones base 3, 4 y 5. Tal como se muestra en la figura 1, la red tiene otro MSC 6, que controla otras tres estaciones base 7, 8 y 9. En la práctica, la red incorporará muchos más MSCs y estaciones base de los que se muestran en la figura 1.

45 Cada abonado a la red está dotado, por lo menos, de una tarjeta inteligente o tarjeta de módulo de identidad de abonado (SIM) (estrictamente hablando, un UICC) que, cuando está asociado con el terminal móvil del usuario, identifica al abonado en la red. El terminal tiene habitualmente un identificador propio (la "identidad internacional de equipo móvil", IMEI), que se puede obtener en ciertas redes, si bien este ID del terminal no es esencial en la identificación del abonado para la red. La tarjeta SIM está preprogramada con un número de identificación único, la "identidad internacional de abonado móvil" (IMSI) a la que se puede acceder en la tarjeta pero que generalmente no es conocida (o utilizada directamente) por el abonado. Impreso en el exterior de cada SIM, hay otro número de identificación única, el ICCID/número de serie SIM (SSN, SIM Serial number), que no está relacionado con el  
50 número IMSI. Se emite al abonado otro número, conocido públicamente, es decir, el número de teléfono del abonado, mediante el cual la parte que llama inicia las llamadas al abonado. Este número es el número ISDN de abonado móvil (MSISDN, Mobile Subscriber ISDN Number).

- 5 La red central incluye un registro de posiciones propias (HLR, home location register) 10 que, para cada abonado a la red, almacena el IMSI y el correspondiente MSISDN junto con otros datos de abonado, tal como la posición actual, o la última conocida, del terminal móvil del abonado. Un segundo registro, el registro de posiciones de visitantes (VLR, visitor location register) 14, se utiliza para almacenar el IMSI y el correspondiente MSISDN para abonados que están temporalmente activos en la red.
- 10 Cuando el abonado desea activar su terminal en la red (de tal modo que pueda entonces realizar o recibir llamadas), el abonado coloca su tarjeta SIM en un lector de tarjetas asociado con el terminal (el terminal 1 en este ejemplo).
- 15 Cuando el terminal 1 se enciende, busca una red móvil a la que conectarse. Una vez que el terminal identifica la red deseada, envía un mensaje a la red (por medio de la estación base 3 asociada con la celda particular de la red en la que el terminal 1 está situado) para indicar que desea registrarse en dicha red particular. Este mensaje incluye el IMSI (leído desde la tarjeta). En una red convencional, la estación base (BS 3) transmite este mensaje que contiene el IMSI al MSC 2 que controla la BS 3.
- 20 Se produce una secuencia idéntica de eventos cada vez que se pierde la conexión (por ejemplo, como resultado de una 'reconexión forzada' en la red; como resultado de que el dispositivo entra en un área de mala cobertura - digamos, un túnel- volviendo a continuación a plena cobertura): en este caso, la secuencia de eventos se denomina reconexión.
- 25 El MSC 2 pasa el IMSI al VLR 14, que a su vez comprueba su base de datos para determinar si hay un archivo existente de dicho abonado particular.
- 30 Si no se encuentra dicho archivo, el VLR 14 lo indica al MSC 2, y el MSC 2 accede a la posición apropiada en el HLR 10 presente en la red central 12. El MSC 2 extrae a continuación el correspondiente MSISDN de abonado y otros datos de abonado de la posición de almacenamiento adecuada, y los almacena temporalmente en una posición en el VLR 14. A continuación, se envía un mensaje de acuse de recibo al terminal. De este modo, el nuevo abonado activo es registrado por lo tanto de manera efectiva con un MSC particular (MSC 2), y la información del abonado se almacena temporalmente en el VLR (VLR 14) asociado con dicho MSC.
- 35 Cuando el HLR 10 es interrogado por el MSC 2 de la manera descrita anteriormente, el HLR 10 lleva a cabo adicionalmente un procedimiento de autenticación para el terminal 1. El HLR 10 transmite datos de autenticación al MSC 2 en formas de "desafío" y "respuesta". Utilizando estos datos, el MSC 2 pasa un "desafío" al terminal 1 a través de la estación base 3. Al recibir estos datos, el terminal 1 pasa estos datos a su SIM y produce una "respuesta". Esta respuesta se genera utilizando un algoritmo de cifrado en el SIM y una clave única, Ki, en el SIM.
- 40 La respuesta se transmite de vuelta al MSC 2, que la verifica con información que ha obtenido para dicho abonado desde el HLR 10 con el fin de completar el proceso de autenticación. Si la respuesta del terminal 1 es la esperada, el terminal 1 se considera autenticado. En este momento, el MSC 2 solicita datos de abonado al HLR 10. El HLR 10 pasa a continuación los datos de abonado al VLR 14.
- 45 El proceso de autenticación se repetirá a intervalos regulares mientras el terminal 1 permanezca activado, y se puede repetir asimismo cada vez que el terminal solicite o reciba servicios de telefonía, si es necesario (este proceso se conoce como "radiobúsqueda").
- 50 Cada uno de los MSC de la red (el MSC 2 y el MSC 6) tiene un respectivo VLR (14 y 11) asociado con el mismo, y funciona del mismo modo que se ha descrito ya cuando un abonado activa un terminal en una de las celdas correspondientes a una de las estaciones base controladas por dicho MSC.
- 55 Cuando el abonado que utiliza el terminal 1 desea realizar una llamada de voz, habiendo ya introducido la tarjeta SIM en el lector asociado con este terminal, habiendo sido autenticada la SIM de la manera descrita, y habiéndose registrado satisfactoriamente el terminal en la red, se puede realizar una llamada introduciendo de la manera usual el número telefónico de la parte llamada. Esta información es recibida por la estación base 3 y, a continuación, encaminada a la parte llamada por medio del MSC 2. Mediante la información contenida en el VLR 14, el MSC 2 puede asociar la llamada con este abonado particular y, de ese modo, archivar información con propósitos de cobro.
- Los MSC 2 y 6 soportan comunicaciones en el dominio de conmutación de circuitos -habitualmente llamadas de voz. Están dispuestos correspondientes componentes de pasarela de red, SGSN 16 y 18, para soportar comunicaciones en el dominio de conmutación de paquetes -tal como transmisiones de datos GPRS. Los SGSNs 16 y 18 funcionan de manera análoga a los MSC 2 y 6. Los SGSNs 16, 18 están equipados con un equivalente al VLR para el dominio de conmutación de paquetes. En este caso, cada sesión activa tiene un contexto PDP asociado.
- La figura 2 muestra una disposición de red celular adecuada para permitir una comunicación de datos entre un terminal y la red, de acuerdo con la solicitud de patente del Reino Unido GB 0805964.4 en tramitación con la presente. Cuando los componentes son sustancialmente idénticos a los componentes mostrados en la figura 1, se adoptan en la figura 2 los mismos numerales de referencia.
- En este caso, los módulos de identificación se tratan como testigos únicos que aún no han sido asociados con un abonado particular; por consiguiente se denominan módulos de identificación de testigo, o TIMs. Habitualmente, una

tarjeta TIM tiene el mismo factor de forma que una tarjeta SIM y es intercambiable con ésta. Exactamente igual que las tarjetas SIM, las TIM están preprogramadas por lo menos con un número de identificación único, la "identidad internacional de abonado móvil" (IMSI) que es accesible en la tarjeta. Sin embargo, el TIM no está asociado con un número conocido públicamente (es decir, un MSISDN). En este sentido, el TIM se considera un SIM "sin suministro".

5 Dado que los TIM no tienen MSISDN asociados permanentemente consigo, pueden ser utilizados en entornos en los que es incierto cuándo será utilizado un TIM determinado, o incluso si un TIM llegará siquiera a ser utilizado. Esto es importante comercialmente en las redes celulares típicas en las que existe un coste asociado con el suministro de un MSISDN válido a un SIM, y un coste adicional asociado con la cuarentena y finalmente la reasignación de dicho número MSISDN cuando no se ha utilizado durante un periodo predeterminado (habitualmente, del orden de seis a  
10 nueve meses).

Para gestionar las solicitudes iniciales de conexión a la red, la red de la figura 2 incluye un HLR global (G-HLR) 210 y una entidad de red 10'.

15 Se puede observar que análogamente a la solicitud de patente del Reino Unido GB 0805964.4 en tramitación con la presente, la entidad de red 10' de la figura 2 representa un registro de posiciones y, por lo tanto, representa un registro de posiciones propias (HLR) local (idéntico al HLR 10 de la red de la figura 1), un VLR/MSC local (VLR 14 y MSC 2 de la red de la figura 1), un SGSN local (SGSN 16 en la red la figura 1) o una entidad SCP local (tal como un repetidor SCCP).

20 Cuando el usuario del terminal 1' desea activar su terminal en la red (de tal modo que pueda abrir a continuación una conexión de datos), el usuario coloca una tarjeta TIM en un lector de tarjetas asociado con el terminal (el terminal 1' en la figura 2). El terminal 1' se conecta a continuación con la red radioeléctrica (etapa 201).

25 Igual que en la figura 1, la conexión a la red radioeléctrica en la figura 2 equivale a una solicitud para registrar el terminal en la red utilizando el IMSI del TIM del terminal. A partir del análisis del IMSI, el registro de posiciones 10' determina que el número IMSI proporcionado por el TIM pertenece a otro registro. La solicitud de conexión se transfiere a continuación al G-HLR 210 (etapa 202). El G-HLR 210 extrae a continuación el número IMSI de esta solicitud y, asumiendo que el número IMSI está en un intervalo mantenido por el G-HLR 210, transmite una señal de testigo al registro de posiciones 10' (etapa 203) indicando que el IMSI ha sido reconocido por el G-HLR 210 (esta señal de testigo puede simplemente ser una señal de confirmación ('OK') pero puede incluir otra información del perfil).

30 El registro de posiciones 10', al recibir la señal de testigo, almacena el IMSI temporalmente en un almacén de registro de posiciones (éste podría ser el VLR 14, el SGSN 220 o ambos). De este modo, el usuario del terminal 1' se registra de manera efectiva dentro de un MSC particular (MSC 2) y/o de un SGSN (SGSN 220), y cualquier información del perfil asociada con el TIM se almacena temporalmente en el VLR (VLR 14) asociado con dicho MSC y/o con el SGSN 220.

35 El GHLR 210 lleva a cabo adicionalmente un procedimiento de autenticación del terminal 1'. El GHLR 210 transmite datos de autenticación al MSC 2 y/o al SGSN 220 en formas de "desafío" y "respuesta". Utilizando estos datos, el MSC 2 y/o el SGSN 220 pasa un "desafío" al terminal 1' a través de la estación base 3. Al recibir estos datos, el terminal 1' pasa estos datos a su TIM y produce una "respuesta". Esta respuesta se genera utilizando un algoritmo de cifrado en el TIM y una clave única, Ki', en el TIM. La respuesta se trasmite de vuelta al MSC 2 y/o al SGSN 220, que la verifica con información que ha obtenido para dicho testigo desde el G-HLR 210 con el fin de completar el  
40 proceso de autenticación. Si la respuesta del terminal 1' es la esperada, el terminal 1' se considera autenticado.

El proceso de autenticación se repetirá a intervalos regulares mientras el terminal 1' permanezca activado y se puede repetir asimismo cada vez que el terminal solicita o recibe servicios de telefonía, si es necesario.

45 Cuando el usuario del terminal 1' desea establecer una conexión de datos, habiéndose introducido ya la tarjeta TIM en el lector asociado con este terminal y habiéndose confirmado la validez del TIM por el G-HLR 210 de la manera descrita, la solicitud de una conexión de datos se pasa al componente 220 de pasarela de red (es decir, el SGSN 16) y se establece una sesión de pasarela.

50 El componente 220 de pasarela de red recibe desde el G-HLR 210 una correspondiente clave para el IMSI. Esta clave se utiliza, a su vez, para solicitar un componente 230 de monitorización de la red (por ejemplo NGME o GGSN) que determina si los datos de clave están asociados con una sesión válida existente (habitualmente, una sesión nativa DIAMETER o RADIUS). La señalización entre el componente 220 de pasarela de red y el componente 230 de monitorización de la red tiene preferentemente tarifa cero, de tal modo que no se cobra al usuario por el establecimiento de la sesión.

Si existe ya una sesión válida para estos datos de clave, se establece la conexión de datos (etapa 209). El terminal 1' tiene acceso a una inter-red solicitada 246 -habitualmente, internet o una intranet corporativa.

55 Sin embargo, si no se puede encontrar ninguna sesión válida que corresponda a la clave, el terminal 1' puede en cambio ser redirigido a una página web generada por un servidor web 240. La página web presentada está

personalizada para el terminal 1' de acuerdo con los datos de clave, y ofrece al usuario por lo menos una opción de acción del usuario.

5 El componente 230 de monitorización de la red actúa a continuación como una pasarela inter-red: denegando o permitiendo el acceso desde la red celular 100 a la inter-red solicitada 246 en función de la información introducida por el usuario en relación con la opción de acción de usuario seleccionada. En un escenario típico, la página web ofrece la opción de una sesión de tiempo limitado por un precio predeterminado. La selección de dicha opción conduce al usuario a un diálogo de usuario que solicita información de facturación del usuario, incluyendo por ejemplo: nombre, dirección, detalles de la tarjeta de crédito/débito, información de bonos/cupones, número telefónico existente al que facturar/SMS, etc.

10 Se proporciona el control de sesión mediante un servidor de control de sesión (preferentemente un servidor DIAMETER nativo). El servidor de control de sesión emite informes regulares sobre las sesiones que gestiona (denominados "tiques de eventos"). En una sesión nativa basada en DIAMETER, el componente 230 de monitorización de la red puede utilizar tiques de evento DIAMETER para cada sesión válida con el fin de monitorizar la utilización de sesiones de cada usuario.

15 Evidentemente, el componente 230 de monitorización de la red puede utilizar asimismo los tiques de evento DIAMETER para cada sesión válida con el fin de monitorizar la utilización de sesiones de grupos de usuarios (tal como se puede requerir en la provisión de servicios a un negocio o "empresa"). Esta disposición facilita la denominada "facturación intervenida", de manera que una empresa puede agregar facturas para grupos de usuarios de la empresa. La facturación intervenida se puede efectuar presentando información sobre sesiones monitorizadas a un administrador o agente para la empresa, a través de una aplicación de facturación central y monitorización de la empresa.

25 El contexto PDP es un término relacionado con una serie de puntos en la presente explicación. Adopta el siguiente significado convencional estandarizado, en todo el documento. El contexto PDP (protocolo de datos de paquetes, por ejemplo IP, X.25, FrameRelay) es una estructura de datos presente tanto en el SGSN como en el GGSN, que contiene la información de sesión del abonado, cuando el abonado tiene una sesión activa. Cuando un terminal móvil desea utilizar GPRS, debe primero acogerse a un contexto PDP y a continuación activarlo. Cuando una entidad externa desea establecer una conexión GPRS con el terminal móvil (etapa 302), la red tiene que establecer en primer lugar conexiones del elemento de red (notificación PDU) antes de solicitar la activación del contexto PDP mediante el terminal móvil objetivo (ver la figura 3). En cualquier caso, se asigna una estructura de datos de contexto PDP en el SGSN que el abonado está visitando actualmente y el GGSN que sirve al punto de acceso del abonado.

30 Los datos archivados incluyen:

Dirección IP del abonado

IMSI del abonado

Del abonado,

35 el ID del extremo del túnel (TEID, Tunnel Endpoint ID) en el GGSN

el ID del extremo del túnel (TEID, Tunnel Endpoint ID) en el SGSN

El ID del extremo del túnel (TEID) es un número asignado por el respectivo GSN que identifica los datos tunelizados relacionados con un contexto PDP particular.

40 El funcionamiento de la invención se puede entender considerando una realización específica, mostrada en las figuras 4 y 5. La figura 4 muestra el procesamiento de una solicitud para una sesión de datos de máquina a máquina, desde un terminal cliente de máquina a máquina, con un TIM incorporado pero al que no se ha suministrado un número MSISDN; mientras que la figura 5 se refiere a la entrega de un mensaje de proveedor a dicho terminal cliente M2M con un TIM incorporado.

45 En la figura 4, la red incluye un SCP 402 y un HLR global (G-HLR) 410. En este caso, el terminal móvil 401 es un cliente de máquina a máquina (M2M) con un TIM incorporado.

El SCP 402 puede subsumir la funcionalidad del HLR 10 en la red de la figura 1. Alternativamente, el SCP 402 puede subsumir la funcionalidad de un VLR 14 y MSC 2, y/o la funcionalidad de un SGSN 16. Evidentemente, el SCP 402 puede incorporar asimismo un agregador SS7 (tal como un repetidor SCCP) para agregar las funcionalidades de señalización que de lo contrario se exigirían del HLR 10, el VLR 14 y/o el SGSN 16.

50 Cuando el cliente M2M 401 requiere su activación en la red celular (de tal modo que pueda abrir a continuación una conexión de datos), el cliente "inicia" una aplicación de conexión de datos que se ejecuta en su sistema operativo, habitualmente en respuesta a un evento desencadenador. El cliente M2M 401 conecta a continuación con la red radioeléctrica (etapa 451).

- Igual que en la figura 1, la conexión a la red radioeléctrica en la figura 4 equivale a una solicitud para registrar el terminal en la red utilizando el IMSI del TIM del terminal. A partir del análisis del IMSI, el SCP 402 determina que el número IMSI proporcionado por el TIM pertenece a otro registro. La solicitud de conexión se redirige a continuación al G-HLR 410 (etapa 452). El G-HLR 410 extrae a continuación el número IMSI de esta solicitud y, asumiendo que el número IMSI está en un intervalo mantenido por el G-HLR 410, transmite una señal de testigo al SCP 402 (etapa 454) indicando que el IMSI ha sido reconocido por el G-HLR 410 (esta señal de testigo puede simplemente ser una señal de confirmación ('OK') pero puede incluir otra información del perfil).
- El SCP 402, al recibir la señal de testigo, almacena temporalmente el IMSI en un almacén de registro de posiciones (esto podría ser en el VLR (no mostrado), el SGSN 420 o ambos). De este modo, el cliente M2M 401 está por lo tanto registrado de manera efectiva con un MSC (no mostrado) y/o SGSN 420 particular, y cualquier información de perfil asociada con el TIM es almacenada temporalmente en el VLR asociado con dicho MSC y/o SGSN 420.
- La solicitud de una conexión de datos se transfiere mediante el SCP 402 al componente 420 de pasarela de red (es decir, el SGSN 16). El componente 420 de pasarela de red recibe del G-HLR 410 una clave correspondiente al IMSI (etapa 456). Tomando la clave, junto con la solicitud transmitida de una conexión de datos, el componente 420 de pasarela de red establece una sesión de pasarela. Esta clave se utiliza, a su vez, para solicitar un componente 430 de monitorización de la red (por ejemplo NGME o GGSN) que determina si los datos de clave están asociados con una sesión válida existente (habitualmente, una sesión nativa DIAMETER). La señalización (etapa 458) entre el componente 420 de pasarela de red y el componente 430 de monitorización de la red tiene preferentemente tarifa cero, de tal modo que el dispositivo cliente 401 no es facturado por el establecimiento de la sesión.
- Suponiendo que no existe ninguna sesión válida correspondiente a dicha clave, el componente 430 de monitorización de la red interactúa con un servidor DIAMETER 440 para autenticar una nueva sesión de datos M2M (etapa 462) para el cliente M2M 401.
- El servidor DIAMETER 440 señala a su vez al componente 430 de monitorización de la red que se debería abrir una sesión (etapa 464).
- El componente 430 de monitorización de la red redirige a continuación al usuario a un servidor M2M solicitado 450 por medio de una red de línea fija, tal como internet 470 (etapa 466) y cambia simultáneamente el estado de facturación de la sesión de cliente M2M, de tarifa cero a una tarifa de datos.
- A la finalización de una sesión previamente establecida, el servidor DIAMETER 440 ordena al componente 430 de monitorización de la red poner la sesión en espera (y ajusta la sesión a tarifa cero).
- El servidor DIAMETER 440 envía asimismo una alerta de utilización (utilizando tiques DIAMETER, etapa 468) a un motor de mediación de facturación 480, que genera un evento de facturación correspondiente a la utilización de sesión notificada.
- El cliente M2M envía y recibe mensajes cortos de texto (SMS) a una plataforma SMS M2M dedicada 495. Los mensajes SMS se transportan de manera convencional a través de una pasarela SMS 490 y a continuación a través de una conexión de internet 470 hasta la plataforma SMS M2M 495.
- Tal como se ha explicado anteriormente, existen situaciones en las que una parte externa puede desear transmitir un mensaje (o realizar una llamada de voz) al terminal cliente M2M.
- Para establecer una conexión desde el lado del proveedor (servidor), el proveedor envía un mensaje de proveedor (etapa 502) desde la plataforma SMS M2M 495 dirigido al terminal M2M 401: estando el mensaje formateado para incluir el número IMSI terminal (en ausencia de un MSISDN) en el campo de destino. En dichos mensajes, la parte B puede estar indicada mediante un código corto único para la plataforma SMS 495 del proveedor. El mensaje se transfiere por medio de la pasarela SCP 402 y finalmente a la pasarela SMS 490.
- La pasarela SCP 402 recibe el mensaje del proveedor con el número IMSI en el campo de destino, y lo transfiere a una aplicación 550 de análisis sintáctico de mensajería (etapa 503), pudiendo ser ejecutada la aplicación en un VLR, HLR, SGSN u otra entidad SCP (tal como un repetidor SCCP). La aplicación 550 de análisis sintáctico pone los mensajes de proveedor entrantes (etapa 504) en una cola de mensajes 552, accede a una tabla de números MSISDN en repositorio (PADS) e inyecta uno seleccionado de los números de conexión del repositorio al archivo de suscripción HLR del terminal y ordena retirar del HLR (etapa 506) el archivo IMSI objetivo correspondiente a dicho terminal, al G-HLR 410 (forzando al terminal que tiene dicho número IMSI a experimentar una reconexión, etapa 508).
- Durante su siguiente solicitud de reconexión (etapa 510) el terminal 401 desencadenará automáticamente un evento de actualización de la posición. De acuerdo con 3GPP TS 23.012, el procedimiento de actualización de la posición incluye una etapa mediante la cual el terminal suministra su número IMSI al HLR y solicita la reconexión a la red.
- Al recibir un acuse de recibo indicando que la reconexión se ha completado (etapa 511), la aplicación de análisis sintáctico sobrescribe el IMSI en el mensaje del proveedor con el MSISDN recién asignado (etapa 512) y



proporciona el mensaje del proveedor junto con el MSISDN a la pasarela SMS 490 (etapa 513). La pasarela SMS 490 puede transferir a continuación el mensaje del proveedor al terminal 401 como un SMS convencional, dirigido ahora al MSISDN asignado (etapa 514).

- 5 El acuse de recibo de la entrega del mensaje del proveedor al terminal 401 (etapa 515/516) se señala a la aplicación 550 de análisis sintáctico, lo que permite que la aplicación de análisis sintáctico envíe un informe de utilización (CDR) al motor de mediación 480 (etapa 518) y un aviso de entrega a la plataforma SMS M2M 495 del proveedor (etapa 519/520) (este aviso solo necesita confirmar la entrega al IMSI del terminal).

La recepción satisfactoria de este SMS dentro del terminal puede desencadenar un contexto PDP iniciado por cliente, instigando una conexión de datos entre el terminal cliente 401 y un servidor M2M 450.

- 10 Al completarse el intercambio de datos, cualquiera del terminal o el servidor M2M puede abandonar el contexto PDP, terminando de ese modo la sesión de datos. El servidor M2M puede considerar esto un desencadenante para volver a retirar el terminal del GHLR (tal como se ha descrito anteriormente en la retirada inicial) con el fin de recuperar el MSISDN asignado.

- 15 En otra realización, un terminal está dotado además de componentes adecuados de altavoz, micrófono y procesamiento de señal. La invención permite entonces que el terminal maneje una capacidad de voz limitada. Existen un par de escenarios en los que esto puede ser necesario: llamadas desde el terminal a un número de servicio M2M y establecimiento de una llamada a servicios de emergencia.

- 20 En relación con el caso de la entrega de mensajes de proveedor, el proveedor puede alternativamente solicitar al cliente M2M una conexión de voz. La solicitud inicial se debe realizar a través del SCP 402, donde se detecta la ausencia de MSISDN (u otro número telefónico asociado único), se introduce un MSISDN temporal en el archivo del GHLR y se retira el cliente M2M de la red para obtener un MSISDN temporal de la manera mostrada en la figura 5. La solicitud de llamada se transfiere al VLR utilizando el MSISDN como número A.

- 25 En los casos en los que el proveedor (o el operador de red) desee archivar los cargos de costes contra un usuario particular, la red requiere la introducción de un nodo de red inteligente (IN, intelligent network) para realizar un seguimiento de los cargos por llamada.

**REIVINDICACIONES**

1. Una red de telecomunicaciones celular para asociar temporalmente números de conexión únicos con terminales que tienen módulos de identificación de testigo, incluyendo la red:
- 5 un registro de posiciones adaptado para recibir desde terminales solicitudes para acceder a la red y, si las solicitudes están asociadas con un módulo de identificación de testigo, adaptado para redirigir las solicitudes;
- un registro de testigos que está adaptado para recibir dichas solicitudes redirigidas, y adaptado para generar datos de identificación de conexión de testigo y transmitir los datos de identificación de conexión de testigo al registro de posiciones con el fin de identificar el terminal al registro de posiciones; y
- 10 un componente de pasarela de red adaptado para establecer una comunicación entre la red y el terminal, de acuerdo con los datos de identificación de conexión de testigo; comprendiendo además la red:
- un componente de almacenamiento de red adaptado para almacenar una tabla de números de conexión únicos; y
- un componente de análisis sintáctico de mensajería adaptado para procesar mensajes dirigidos a terminales que tienen módulos de identificación de testigo, para seleccionar un número de conexión determinado a partir de la tabla de números de conexión, para asociar el número seleccionado con un archivo de registro de testigos para un
- 15 módulo de identificación de testigo determinado y para redirigir los mensajes al terminal que tiene el módulo de identificación de testigo determinado utilizando el número asociado,
- en el que el componente de análisis sintáctico de mensajería está acoplado comunicativamente con el registro de testigos y está adaptado para provocar la asociación del número seleccionado con el módulo de identificación de testigo mediante ordenar retirar de un archivo de registro de posiciones el módulo de identificación de testigo e
- 20 inyectar el número seleccionado en el archivo de registro de testigos durante la reconexión.
2. Una red según la reivindicación 1, en la que la aplicación de análisis sintáctico de mensajería está adaptada además para desencadenar un contexto PDP tras la confirmación de una recepción satisfactoria de uno determinado de dichos mensajes redirigidos dentro del terminal, instigando de ese modo una conexión de datos entre el terminal y el originador de dicho mensaje redirigido.
- 25 3. Una red según la reivindicación 2, en la que al completarse el intercambio de datos entre el terminal y el originador de dicho mensaje redirigido, el terminal está adaptado para abandonar el contexto PDP, terminando de ese modo la sesión de datos.
4. Una red según la reivindicación 2, en la que al completarse el intercambio de datos entre el terminal y el
- 30 originador de dicho mensaje redirigido, el originador está adaptado para abandonar el contexto PDP, terminando de ese modo la sesión de datos.
5. Una red según cualquiera de las reivindicaciones 2, 3 ó 4, en la que el originador de dicho mensaje redirigido está adaptado para interpretar la terminación de dicha sesión de datos como un desencadenante para volver a retirar el terminal del registro de testigos con el fin de recuperar el número asociado.
- 35 6. Una red según cualquiera de las reivindicaciones anteriores, en la que el terminal está dotado además de componentes adecuados de altavoz, micrófono y procesamiento de señal.
7. Una red según cualquiera de las reivindicaciones anteriores, en la que el registro de posiciones está distribuido, teniendo un punto agregador adaptado para agregar funcionalidad de señalización y una entidad de red adaptada para llevar a cabo funcionalidad adicional de registro de posiciones, estando dicho punto agregador y dicha entidad de red en comunicación entre sí.
- 40 8. Un procedimiento para asociar temporalmente números de conexión únicos con dispositivos que tienen módulos de identificación de testigo, comprendiendo el procedimiento por lo menos:
- proporcionar un repositorio de números de conexión únicos;
- en respuesta a una solicitud de comunicación con un dispositivo que incorpora un módulo de identificación de testigo, asignar uno seleccionado de los números del repositorio al módulo de identificación de testigo en un registro
- 45 de testigos; e
- iniciar un evento de reconocimiento, mediante ordenar retirar de un archivo de registro de posiciones el módulo de identificación de testigo e inyectar a continuación el número seleccionado en un archivo de registro de testigos durante la reconexión, proporcionando de ese modo el número asignado al dispositivo.
- 50 9. El procedimiento según la reivindicación 8, en el que la solicitud de comunicación es una solicitud para entregar un mensaje dirigido a un dispositivo que tiene un módulo de identificación de testigo; comprendiendo además el procedimiento:

recibir dicho mensaje, y

redirigir el mensaje al dispositivo utilizando el número asignado.

5 10. El procedimiento según la reivindicación 9, que comprende además desencadenar un contexto PDP tras la confirmación de recepción satisfactoria de dicho mensaje redirigido dentro del terminal, instigando de ese modo una conexión de datos entre el dispositivo y el originador de dicho mensaje redirigido.

11. El procedimiento según la reivindicación 10, que comprende además, al completarse el intercambio de datos entre el dispositivo y el originador de dicho mensaje redirigido, abandonar, en el dispositivo, el contexto PDP, terminando de ese modo la sesión de datos.

10 12. El procedimiento según la reivindicación 10, que comprende además, al completarse el intercambio de datos entre el dispositivo y el originador de dicho mensaje redirigido, abandonar, en el originador, el contexto PDP, terminando de ese modo la sesión de datos.

13. El procedimiento, según cualquiera de las reivindicaciones 10, 11 ó 12, que comprende además, volver a retirar el dispositivo del registro de testigos tras la terminación de una sesión de datos con el fin de recuperar el número asignado.

15

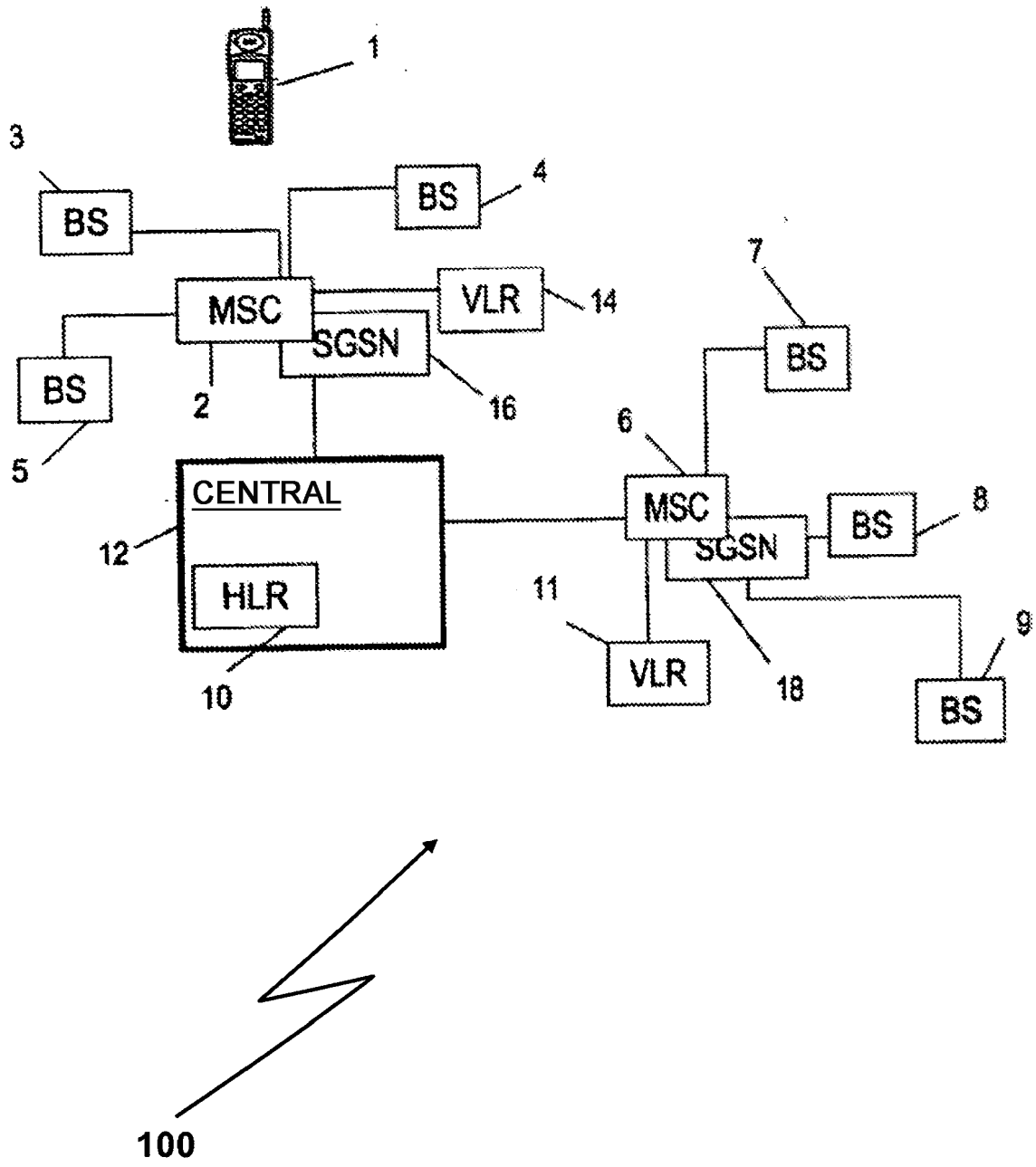


Fig 1

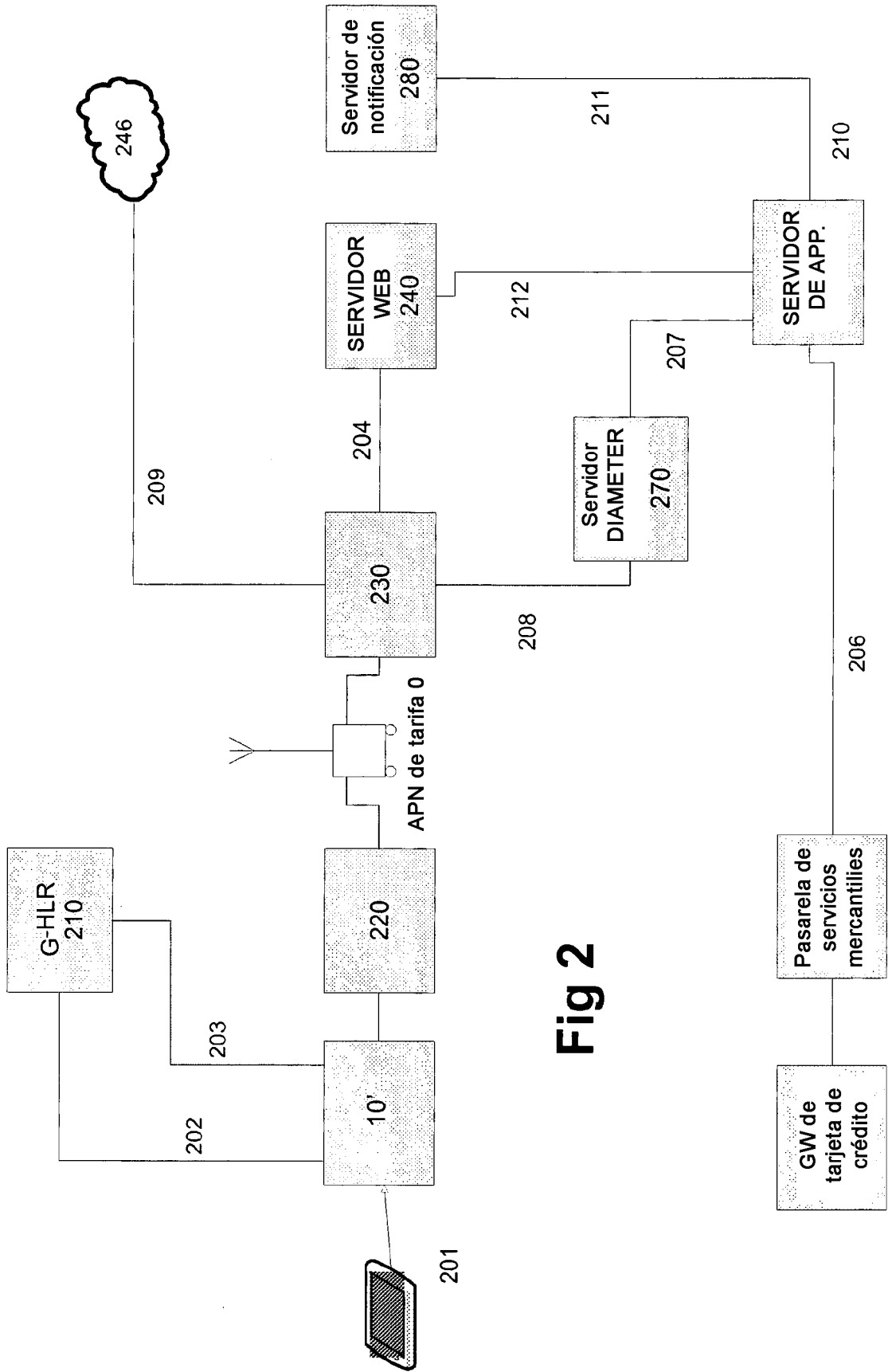


Fig 2

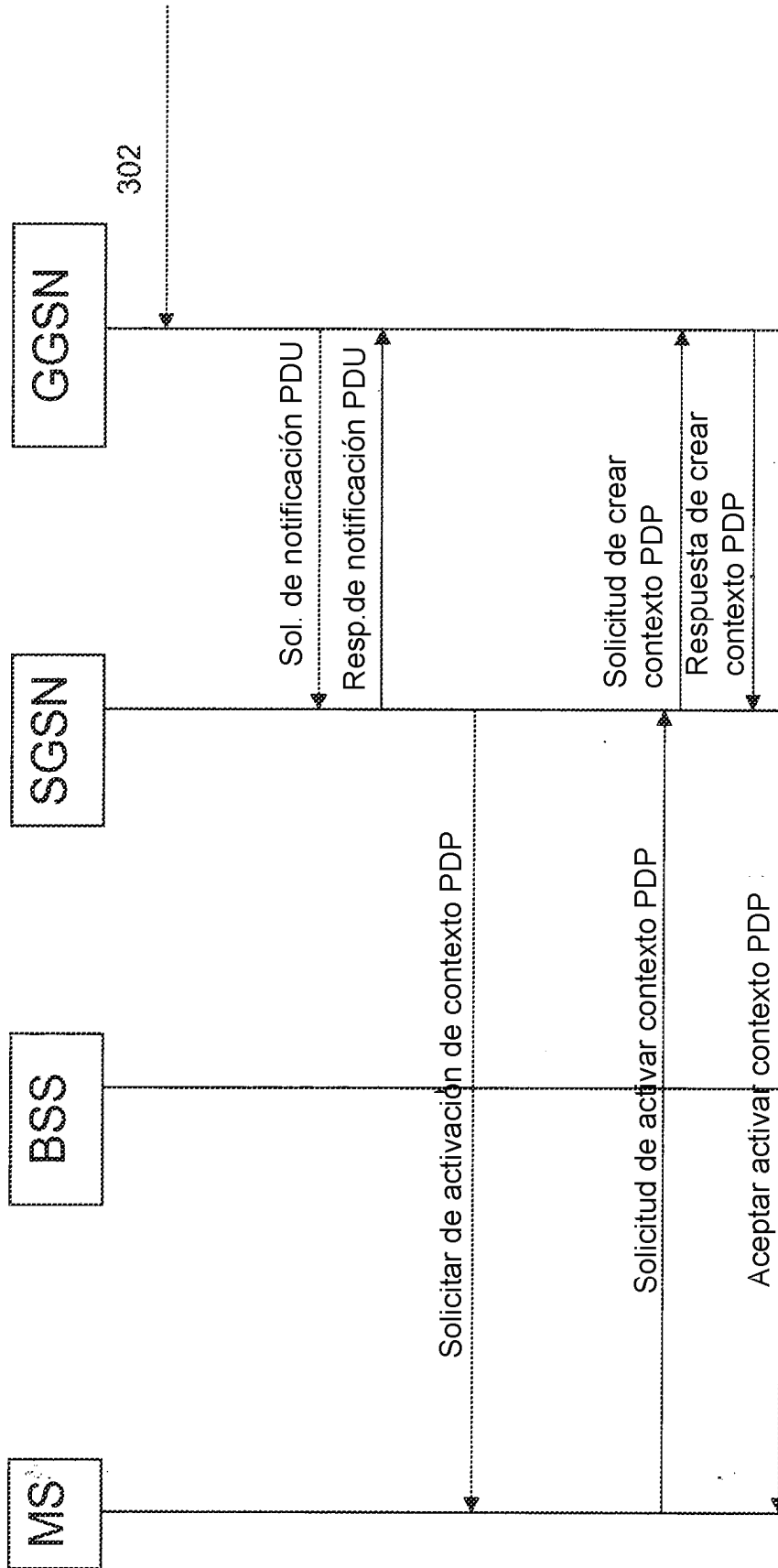


Fig 3



