(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 565 081**

(51) Int. CI.:

H04W 8/26 (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 09727153 (0)**

(97) Fecha y número de publicación de la concesión europea: **10.02.2016 EP 2294849**

(54) Título: **Red de telecomunicaciones**

(30) Prioridad:

02.04.2008 GB 0805964

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2016

(73) Titular/es:

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

(72) Inventor/es:

GUMBRELL, RICHARD;
SMITH, TONY;
PRABDIAL, YAKEEN y
WONTNER, EDMUND

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

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 versa sobre una red de telecomunicaciones. En particular, la invención versa sobre una red celular que permite que los terminales que tengan módulos de identificación establezcan una comunicación de datos sin que ese módulo de identificación esté asociado con un abonado.

En redes celulares de telecomunicaciones convencionales, la activación de un módulo de identificación de abonado (SIM) requiere que se satisfagan ciertos prerrequisitos. De particular interés aquí, el SIM debe estar asociado con un único número de teléfono (MSISDN). Generalmente, este familiar número de teléfono es usado por un llamante que desee hacer una llamada de voz (o de vídeo) al terminal móvil en el que se ha insertado el SIM. Invariablemente, el número de teléfono es seleccionado (ya sea automáticamente o, en algunos casos, por los propios usuarios) de una gama de números MSISDN disponibles propiedad de la empresa explotadora de suministro y el número seleccionado es asignado al SIM cuando el SIM es objeto de direccionamiento por vez primera por la red de la empresa explotadora: generalmente, esto significa que el número de teléfono debe ser asignado antes de que un usuario active por vez primera el SIM con un sistema de prepago o de contrato.

La empresa explotadora de la red soporta un coste asociado con la dotación al SIM de un MSISDN válido, tanto para la reserva del MSISDN (los organismos reguladores tales como la ITU asignan intervalos de números MSISDN a las empresas explotadoras) como para el tiempo y los gastos administrativos del personal minorista en el registro del número seleccionado para su uso.

Cuando ese SIM ya no aparece usado (o parece no haberlo sido nunca) durante un periodo predeterminado, las empresas explotadoras de la red normalmente se fijan en este hecho e inician un proceso de “cuarentena” para devolver el número de teléfono al conjunto de números disponibles. Por supuesto, este proceso de cuarentena tiene un coste asociado: también lo tiene reasignar ese número MSISDN, como ocurrirá en último término cuando se confirme no usado después de que expire el periodo de cuarentena.

Según apreciará inmediatamente el lector, el suministro de los SIM que son usados infrecuentemente o nunca representa un claro inconveniente para la empresa explotadora de la red. Este inconveniente es significativo incluso cuando se considera el suministro convencional de teléfonos móviles y tarjetas de datos/módems con los SIM. Sin embargo, hay una tendencia actual a embeber o habilitar el SIM de otro modo en una gama mucho más amplia de productos informáticos y electrónicos distintos. Por ejemplo, PC portátiles, PC ultramóviles (UMPC), agendas electrónicas (PDA), dispositivos de ubicación por satélite, decodificadores (STB), puntos de acceso inalámbrico (AP) e incluso ordenadores a bordo de vehículos pueden estar dotados, y últimamente suelen estarlo, de módulos que aceptan SIM para permitir la comunicación en redes celulares de telecomunicaciones. Está claro que esta tendencia implica un aumento concomitante en el número de SIM no usados o usados infrecuentemente y un nivel consiguientemente mayor de alternación para la empresa explotadora de la red que desea habilitar tales dispositivos.

Surge un problema adicional en relación con la producción y la gestión de tarjetas SIM para terminales telemáticos (por ejemplo, ordenadores a bordo de automóviles), cuando sea deseable que los terminales puedan ser exportados a diversas ubicaciones geográficas, cada una con su propia red de telecomunicaciones.

Según se ha descrito en las patentes anteriores GB2378097, GB2378094 y GB2378095, se puede abordar el problema garantizando que todos los parámetros específicos y las claves relevantes de la empresa explotadora estén almacenados de antemano en el SIM, en el momento de la fabricación. En consecuencia, un SIM adecuadamente preparado puede ser registrado de nuevo, dándolo de baja de una red principal y dándolo de alta en otra red principal, según sea necesario. Se envían instrucciones al SIM en cuanto a qué claves de autenticación ha de usar en qué territorio y un correspondiente nuevo número identificador del SIM, IMSI.

En consecuencia, cuando se exportan automóviles, los SIM pueden ser configurados para el país de fabricación y después reconfigurados para el país de destino. El método también puede ser aplicado a otros dispositivos y puede ser reconfigurado indefinidamente. Por ende, un terminal puede ser usado en otra red (no como un abonado itinerante) durante un tiempo significativo sin que se emita una nueva tarjeta SIM. Está claro que la falta de uso o el uso infrecuente de tales SIM “preinstalados” solo amplificaría los problemas esbozados más arriba, dado que esta solución requiere la dotación de *varios* MSISDN disponibles, uno para cada territorio previsto en el momento de la fabricación.

Por lo tanto, es un objeto de la presente invención obviar o al menos mitigar los problemas anteriormente mencionados.

Según un aspecto de la presente invención, se proporciona una red celular de telecomunicaciones para facilitar conexiones de comunicación para terminales que tienen módulos de identificación por testigo, incluyendo la red:

un registro de ubicación para recibir solicitudes de acceso a la red y, si las solicitudes están asociadas con un módulo de identificación por testigo, adaptado para redirigir las solicitudes;
un registro de testigos que recibe solicitudes redirigidas, genera datos de identificación de conexión y transmite los datos de identificación de conexión al registro de ubicación para identificar el terminal ante el registro de ubicación;
un componente de pasarela de red para establecer una comunicación entre la red y el terminal según los datos de identificación de conexión;
un componente de pasarela de red para establecer una comunicación entre la red y el terminal según los datos de identificación de conexión por testigo; y
un componente de monitorización de red para realizar una gestión del servicio.

Las conexiones de comunicación son, preferentemente, conexiones de comunicación solo de datos.

Cada solicitud de acceso a la red procedente de un terminal que tiene un módulo de identificación por testigo incluye, preferentemente, un número IMSI que identifica de forma única al módulo de identificación por testigo.

La red, además, puede incluir: un servidor que está adaptado para servir páginas electrónicas de diálogos de usuario a terminales móviles según los datos de identificación de conexión por testigo, presentando cada página electrónica al usuario al menos una opción de acciones de usuario; y una pasarela de interconexión de redes que gobierna el acceso de la red celular a una interconexión de redes; incluyendo la verificación de autenticación de la sesión llevada a cabo por el componente de monitorización de red determinar si los datos de identificación de conexión por testigo están asociados con una sesión válida; dirigiendo el componente de pasarela de red al terminal a una página electrónica de diálogos de usuario servida por un servidor de Web cuando el componente de monitorización de red determina que no hay ninguna sesión asociada válida, y dándosele acceso al terminal a la interconexión de redes dependiendo de la indicación de la opción de acciones de usuario desde el terminal.

Alternativamente, la red, además, incluye una pasarela de interconexión de redes que gobierna el acceso de la red celular a un servidor M2M por medio de una interconexión de redes; incluyendo la verificación de autenticación de la sesión llevada a cabo por el componente de monitorización de red determinar si los datos de identificación de conexión por testigo están asociados con una sesión M2M válida; y dirigiendo el componente de monitorización de red al terminal al servidor M2M cuando el componente de monitorización de red determina que los datos de identificación de conexión por testigo están asociados con una sesión M2M válida.

La interconexión de redes puede ser Internet o una intranet.

El registro de ubicación puede estar distribuido, teniendo un punto de agregación para agregar funcionalidad de señalización y una entidad de red para realizar una funcionalidad adicional de registro de ubicación, estando dicho punto de agregación y dicha entidad de red en comunicación mutua. Ejemplos de funcionalidad adicional del registro de ubicación incluyen el almacenamiento temporal de números IMSI.

Ejemplos de gestión de servicio llevada a cabo por el componente de monitorización de red incluyen: gestión de sesiones; verificar la autenticación de la sesión; y/o la aplicación de la directriz de la empresa explotadora de la red (tal como un uso legítimo).

Según otro aspecto de la presente invención, se proporciona un método para facilitar conexiones de comunicación entre terminales que tienen módulos de identificación por testigo y una red celular de telecomunicaciones, incluyendo la red celular un registro de ubicación, un registro de testigos, un componente de pasarela de red, un componente de monitorización de red, un servidor y una pasarela de interconexión de redes, incluyendo el método:

en el registro de ubicación, recibir de un terminal una solicitud de acceso a la red, determinar si la solicitud está asociada con un módulo de identificación por testigo y redirigir la solicitud al registro de testigos;
en el registro de testigos, recibir la solicitud redirigida, generar datos de identificación de conexión por testigo y transmitir los datos de identificación de conexión al registro de ubicación, identificando con ello al terminal ante el registro de ubicación;
establecer una comunicación entre la red y el terminal según los datos de identificación de conexión por testigo; y
efectuar una verificación de autenticación de la sesión.

La etapa de verificación de autenticación de la sesión puede incluir determinar si los datos de identificación de conexión por testigo están asociados con una sesión válida, y el método, además, puede incluir: servir al terminal una página electrónica de diálogos de usuario según los datos de identificación de conexión por testigo, presentando la página electrónica al usuario al menos una opción de acciones de usuario; dirigir al terminal a la página electrónica de diálogos de usuario cuando el componente de monitorización de red determina que no hay ninguna sesión asociada válida; y permitir el acceso desde la red celular a la interconexión de redes dependiendo de la indicación de la opción de acciones de usuario desde el terminal.

Alternativamente, el método puede incluir, además: dirigir al terminal al servidor M2M cuando el componente de monitorización de red determina que los datos de identificación de conexión por testigo están asociados con una sesión M2M válida, cuando la pasarela de interconexión de redes gobierna el acceso desde la red celular a un servidor M2M mediante una interconexión de redes y la etapa de verificación de autenticación de la sesión incluye determinar si los datos de identificación de conexión por testigo están asociados con una sesión M2M válida.

Para una mejor comprensión de la presente invención, ahora se hará referencia, únicamente a título de ejemplo, de los dibujos adjuntos, en los que:

la Figura 1 ilustra elementos clave de una red celular de telecomunicaciones y su operación;
la Figura 2A ilustra elementos clave de una red celular de telecomunicaciones según la invención, teniendo la red tanto un registro de ubicación en origen y un registro de testigos;
la Figura 2B ilustra elementos clave de una red celular alternativa de telecomunicaciones según la invención, no teniendo la red ningún registro de ubicación en origen y dependiendo en su lugar de un registro de ubicación de visitantes;
la Figura 2C ilustra elementos clave de una red celular alternativa adicional de telecomunicaciones según la invención, dependiendo la red de la funcionalidad de un registro de ubicación de un componente de pasarela de red en lugar de en un registro de ubicación en origen;
la Figura 2D ilustra elementos clave de redes celulares alternativas adicionales de telecomunicaciones según la invención en las que se usa un punto de agregación SS7 para facilitar las arquitecturas de las Figuras 2A, 2B y 2C;
la Figura 3 ilustra el flujo de acciones al proporcionar sesiones de datos a un PC portátil con un módulo embebido de identificación según la invención; y
la Figura 4 ilustra el flujo de acciones al proporcionar sesiones de datos a un dispositivo para su uso en un entorno máquina-máquina según la invención.

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

Cada estación base (BS) corresponde a una respectiva célula de la red de telecomunicaciones y recibe llamadas de un terminal móvil en esa célula y transmite llamadas al mismo mediante comunicación inalámbrica por radio en uno o ambos de los dominios conmutados por circuitos o conmutados por paquetes. En 1 se muestra tal terminal móvil de abonado. El terminal móvil puede ser un teléfono móvil portátil, una agenda electrónica (PDA) o un ordenador portátil equipado con una tarjeta de datos.

Cada estación base comprende una estación transceptora base (BTS) y un controlador de estaciones base (BSC). Un BSC puede controlar más de una BTS. Las BTS y los BSC comprenden la red de acceso de radio.

Convencionalmente, las estaciones base son dispuestas en grupos y cada grupo de estaciones base es controlado por un centro de conmutación móvil (MSC), tal como el MSC 2 para las estaciones base 3, 4 y 5. Según 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 MSC y estaciones base que los mostrados en la Figura 1.

Cada abonado de la red está dotado de al menos una tarjeta inteligente o tarjeta de módulo de identidad de abonado (SIM) (hablando estrictamente, una UICC) que, cuando es asociada con el terminal móvil del usuario identifica al abonado ante la red. El terminal normalmente tiene un identificador propio (la “identidad internacional del equipo móvil”, IMEI), que puede ser obtenido en ciertas redes; sin embargo, esta ID del terminal no es esencial para identificar al abonado ante la red. La tarjeta SIM está preprogramada con un número de identificación único, la “identidad internacional del abonado móvil” (IMSI) a la que se puede acceder en la tarjeta, pero que generalmente no es conocida para el abonado (ni usada directamente por él). Impreso en el exterior de cada SIM, hay un número de identificación único adicional, el ICCID / número de serie SIM (SSN), que no está relacionado con el número IMSI. Al abonado se le facilita un número adicional, conocido de manera pública; es decir, el número de teléfono del abonado, por medio del cual los llamantes inician llamadas al abonado. Este número es el número ISDN de abonado móvil (MSISDN).

La red central incluye un registro 10 de ubicación en origen (HLR) que, para cada abonado de la red, almacena el IMSI y el correspondiente MSISDN junto con otros datos de abonado, tales como la ubicación actual o la última conocida del terminal móvil de abonado. Se usa un segundo registro, el registro 14 de ubicación de visitantes (VLR), para almacenar el IMSI y el correspondiente MSISDN para abonados que estén activos en la red temporalmente. En toda la presente descripción, debería entenderse que la expresión “registro de ubicación” está relacionada con una entidad de red que realiza la funcionalidad de un HLR, un VLR y/o un componente de pasarela de red, tal como un nodo servidor de soporte GPRS (SGSN).

Cuando el abonado desea activar su terminal móvil en la red (para que, subsiguientemente, pueda hacer o recibir llamadas), el abonado pone su tarjeta SIM en un lector de tarjetas asociado con el terminal móvil (el terminal 1 en este ejemplo).

Cuando el terminal móvil 1 se enciende, busca una red móvil a la que conectarse. Una vez que el terminal móvil identifica la red deseada, envía un mensaje a la red (a través de la estación base 3 asociada con la célula particular de esa red en la que está situado el terminal 1) para indicar que ha entrado en un “estado de inactividad”. Este mensaje incluye el IMSI (leído en la tarjeta). En una red convencional, la estación base 3 transmite entonces el IMSI al MSC 2 en el que está registrada la BS 3.

El MSC 2 pasa el IMSI al VLR 14, que, a su vez, comprueba su base de datos para determinar si existe algún registro del abonado particular.

Si no se encuentra ningún registro, el VLR 14 indica esto al MSC 2 y el MSC 2 accede a la ubicación apropiada del HLR 10 presente en la red central 12. El MSC 2 extrae entonces el correspondiente MSISDN de abonado y otros datos de abonado de la ubicación apropiada de almacenamiento y los almacena temporalmente en una ubicación del VLR 14. A continuación, se envía un mensaje de acuse al terminal móvil. Así, por lo tanto, el abonado nuevamente activo queda registrado efectivamente en un MSC (MSC 2) particular, y la información del abonado se almacena temporalmente en el VLR (VLR 14) asociado con ese MSC.

Cuando el HLR 10 es interrogado por el MSC 2 de la manera descrita anteriormente, el HLR 10 lleva a cabo, además, un procedimiento de autenticación para el terminal móvil 1. El HLR 10 transmite datos de autenticación al MSC 2 en formularios de “pregunta” y “respuesta”. Usando estos datos, el MSC 2 pasa una “pregunta” al terminal móvil 1 a través de la estación base 3. Tras la recepción de estos datos, el terminal móvil 1 pasa estos datos a su SIM y produce una “respuesta”. Se genera esta respuesta usando un algoritmo de cifrado del SIM y una clave única, Ki, del SIM. La respuesta se vuelve a transmitir al MSC 2, que la comprueba con información que ha obtenido del abonado en el HLR 10 para completar el procedimiento de autenticación. Si la respuesta del terminal móvil 1 es la esperada, se considera que el terminal móvil 1 está autenticado. En este punto el MSC 2 solicita datos de abono del HLR 10. El HLR 10 pasa entonces los datos de abono al VLR 14.

El procedimiento de autenticación se repetirá a intervalos regulares mientras el terminal móvil 1 permanezca activado y también puede repetirse cada vez que el terminal móvil haga o reciba una llamada, si se requiere (este procedimiento se denomina “notificación”).

Cada uno de los MSC de la red (MSC 2 y MSC 6) tiene un respectivo VLR (14 y 11) asociado consigo y opera de la misma forma que ya se ha descrito cuando un abonado activa un terminal móvil en una de las células correspondientes a una de las estaciones base controladas por ese MSC.

Cuando el abonado que usa el terminal móvil 1 desea hacer una llamada de voz, habiendo insertado ya la tarjeta SIM en el lector asociado con este terminal móvil y habiéndose autenticado la SIM de la manera descrita, puede hacerse una llamada introduciendo de la forma habitual el número de teléfono (MSISDN) del abonado al que se llama. Esta información es recibida por la estación base 3 y luego es encaminada por el MSC 2 al abonado llamado. Por medio de la información mantenida en el VLR 14, el MSC 6 puede asociar la llamada con un abonado particular y, así, registrar información con fines de facturación.

Los MSC 2 y 6 soportan las comunicaciones en el dominio conmutado por circuitos, normalmente llamadas de voz. Se proporcionan correspondientes SGSN 16 y 18 para soportar las comunicaciones en el dominio conmutado por paquetes, tal como las transmisiones de datos GPRS. Los SGSN 16 y 18 funcionan de forma análoga a los MSC 2 y 6. Los SGSN 16, 18 están equipados con un equivalente al VLR para el dominio conmutado por paquetes.

Las Figuras 2A, 2B, 2C y 2D muestran varias disposiciones de redes celulares alternativas adecuadas para permitir la comunicación de datos entre un terminal móvil y la red según la invención. Cuando los componentes son sustancialmente idénticos a los componentes mostrados en la Figura 1, en las Figuras 2A, 2B, 2C y 2D se adoptan los mismos números de referencia.

En la invención, los módulos de identificación son tratados como testigos únicos que aún no han sido asociados con un abonado particular: en consecuencia, se los denomina módulos de identificación por testigo, o TIM. Normalmente, una tarjeta TIM tiene el mismo factor de forma que una tarjeta SIM y es intercambiable con la misma. Como las tarjetas SIM, los TIM están preprogramados con al menos un número de identificación único, la “identidad internacional del 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, se considera que el TIM es un SIM “no suministrado”.

Dado que los TIM no tienen ningún MSISDN asociado con ellos, pueden ser usados en entornos en los que es incierto cuándo se usará cualquier TIM dado o, ciertamente, si ese TIM será usado en lo más mínimo. Esto es comercialmente importante en las redes celulares típicas, en las que hay un coste asociado con la dotación a un SIM de un MSISDN válido y un coste adicional asociado con la puesta en cuarentena y, en último término, la reasignación de ese número MSISDN cuando no es utilizado durante un periodo predeterminado (normalmente, del orden de seis a nueve meses).

Para gestionar las solicitudes iniciales para una conexión con la red, la red de la Figura 2A incluye tanto un registro 10 de ubicación en origen (HLR) (idéntico al de la red de la Figura 1) como un HLR global (G-HLR) 210.

En una implementación alternativa, ilustrada en la Figura 2B, las estaciones base 3, 4, 5, 7, 8 y 9; los MSC 2, 6; los VLR 11, 14; y los SGSN de la Figura 1 están ligados a un HLR global (G-HLR) 210; sin embargo, no se requiere ningún HLR 10.

Cuando el usuario del terminal móvil 1′ desea activar su terminal móvil en la red (para que subsiguientemente pueda abrir una conexión de datos), el usuario coloca una tarjeta TIM en un lector de tarjeta asociado con el terminal móvil (terminal 1′ en las Figuras 2A, 2B, 2C y 2D). El terminal móvil 1′ se conecta entonces con la red de radio (etapa 201).

Como para la Figura 1, la conexión con la red de radio de la Figura 2A equivale a una solicitud procedente del TIM para acceder a la ubicación apropiada en el HLR 10 para el número IMSI transmitido desde la ubicación apropiada de almacenamiento. El HLR 10 determina que el número IMSI proporcionado por el TIM pertenece a otro registro. La solicitud de conexión es remitida entonces al G-HLR 210 (etapa 202). El G-HLR 210 extrae entonces de esta solicitud el número IMSI y, suponiendo que el número IMSI esté en un intervalo mantenido por el G-HLR 210, transmite una señal testigo al HLR 10 (etapa 203) de que el lMSI ha sido reconocido por el G-HLR 210 (esta señal testigo puede ser, simplemente, una señal de confirmación (“OK”), pero puede incluir información de perfil adicional).

La conexión a la red de radio de la Figura 2B, en cambio, equivale a una solicitud de acceso a la ubicación en origen apropiada en el VLR 14 para el número IMSI transmitido desde la ubicación de almacenamiento apropiada. El VLR 14 determina, mediante análisis del número IMSI, que el TIM pertenece a otro registro. La solicitud de conexión es entonces remitida al G-HLR 210 (etapa 202B). El G-HLR 210 extrae entonces de esta solicitud el número IMSI y, suponiendo que el número IMSI esté en un intervalo mantenido por el G-HLR 210, transmite una señal testigo al VLR 14 (etapa 203B) de que el IMSI ha sido reconocido por el G-HLR 210 (esta señal testigo puede ser, simplemente, una señal de confirmación (“OK”), pero puede incluir información de perfil adicional).

Asimismo, la conexión a la red de radio de la Figura 2C, equivale a una solicitud de acceso a la ubicación en origen apropiada en el SGSN para el número IMSI transmitido desde la ubicación de almacenamiento apropiada. El SGSN determina, mediante análisis del número IMSI, que el TIM pertenece a otro registro. La solicitud de conexión es entonces remitida al G-HLR 210 (etapa 202C). El G-HLR 210 extrae entonces de esta solicitud el número IMSI y, suponiendo que el número IMSI esté en un intervalo mantenido por el G-HLR 210, transmite una señal testigo al SGSN (etapa 203C) de que el IMSI ha sido reconocido por el G-HLR 210 (esta señal testigo puede ser, simplemente, una señal de confirmación (“OK”), pero puede incluir información de perfil adicional).

La Figura 2D ilustra un mecanismo diferente para gestionar tales solicitudes de conexión a la red de radio en el que se usa un punto 290 de agregación SS7 (tal como una retransmisión de la parte de control de la conexión de señalización (SCCP) SS7 o un punto de transferencia de señalización (STP)) para agregar la funcionalidad SS7. En particular, el punto de agregación SS7 puede llevar a cabo un análisis del IMSI (por ejemplo, prestaciones de conversión de título global (GTT) para el tipo de direccionamiento IMSI), eliminando la necesidad de gestionar continuamente las tablas de encaminamiento en los MSC (centros de conmutación móvil) y/o del SGSN 220.

El HLR 10, tras la recepción de la señal testigo, almacena el IMSI temporalmente en una ubicación del registro 14 de ubicación de visitantes (VLR). En la alternativa de la Figura 2B, el VLR 14 almacena el IMSI temporalmente en una memoria del registro de ubicación VLR. Así, por lo tanto, el usuario del terminal 1′ es registrado de manera efectiva en un MSC particular (MSC 2), y cualquier información de perfil asociada con el TIM es almacenada temporalmente en el VLR (VLR 14) asociado con ese MSC.

En la alternativa de la Figura 2C, el SGSN almacena el IMSI temporalmente en una memoria del registro de ubicación del SGSN. El usuario del terminal 1′ es registrado entonces de manera efectiva en un SGSN particular (saltándose el VLR por completo), y cualquier información de perfil asociada con el TIM es almacenada temporalmente en la memoria del registro de ubicación del SGSN.

Una vez que se han completado las etapas anteriores, se realiza a continuación un procedimiento de autenticación para el terminal móvil 1′. Para las Figuras 2A y 2B, el G-HLR 210 transmite datos de autenticación al MSC 2 en formularios de “pregunta” y “respuesta”. Usando estos datos, el MSC 2 pasa una “pregunta” al terminal móvil 1′ a través de la estación base 3. Tras la recepción de estos datos, el terminal móvil 1′ pasa estos datos a su TIM y produce una “respuesta”. Se genera esta respuesta usando un algoritmo de cifrado del TIM y una clave única, Ki′, del TIM. La respuesta se vuelve a transmitir al MSC 2, que la comprueba con información que ha obtenido para ese testigo en el G-HLR 210 para completar el procedimiento de autenticación. Si la respuesta del terminal móvil 1′ es la esperada, se considera que el terminal móvil 1′ está autenticado.

También para la Figura 2C, el G-HLR 210 transmite datos de autenticación al SGSN 220 en formularios de “pregunta” y “respuesta”. Aquí, el SGSN 220 usa estos datos para pasar una “pregunta” al terminal móvil 1′ a través de la estación base 3. Tras la recepción de estos datos, el terminal móvil 1′ pasa estos datos a su TIM y produce una “respuesta”. Se genera esta respuesta usando un algoritmo de cifrado del TIM y una clave única, Ki′, del TIM. La respuesta se vuelve a transmitir al SGSN 220, que la comprueba con información que ha obtenido para ese testigo

en el G-HLR 210 para completar el procedimiento de autenticación. Si la respuesta del terminal móvil 1′ es la esperada, se considera que el terminal móvil 1′ está autenticado.

Como apreciará de inmediato el lector, el uso de un punto 290 de agregación SS7 para agregar funcionalidad SS7 (según se ilustra en la Figura 2D) puede combinarse con los mecanismos para llevar a cabo la autenticación descritos más arriba, con independencia de que la autenticación se realice a través del MSC 2 o del SGSN 220.

El procedimiento de autenticación se repetirá a intervalos regulares mientras el terminal móvil 1′ permanezca activado y también puede repetirse cada vez que el terminal móvil haga o reciba una llamada, si se requiere.

Cuando el usuario del terminal móvil 1′ desea establecer una conexión de datos, habiendo insertado ya la tarjeta TIM en el lector asociado con este terminal móvil y habiendo confirmado el G-HLR 210 la validez del TIM de la manera descrita, se pasa la solicitud de conexión de datos a un componente 220 de pasarela de red (es decir, el SGSN 16) y se establece una sesión de pasarela.

El componente 220 de pasarela de red recibe del G-HLR 210 una clave correspondiente al IMSI. Esta clave es usada, a su vez, para interrogar a un componente 230 de monitorización de red (por ejemplo, NGME, o GGSN) que determina si los datos clave están asociados con una sesión válida existente (normalmente una sesión RADIUS y/o DIAMETER nativa). Preferentemente, la señalización entre el componente 220 de pasarela de red y el componente 230 de monitorización de red tiene una tarificación de cero para que no se facture al usuario el establecimiento de la sesión.

Si realmente existe ya una sesión válida para estos datos clave, se establece la conexión de datos (etapa 209). El terminal móvil 1′ tiene acceso a una interconexión 246 de redes solicitada, normalmente Internet o una intranet de empresa.

Sin embargo, si no puede encontrarse ninguna sesión válida que corresponda a la clave, el terminal móvil 1′ puede ser redirigido, en su lugar, a una página electrónica generada por un servidor 240 de Web. La página electrónica presentada está personalizada para el terminal móvil 1′ según los datos clave y ofrece al usuario al menos una opción de acciones de usuario.

El componente 230 de monitorización de red actúa entonces como una pasarela de interconexión de redes: denegando o permitiendo el acceso desde la red celular 100 a la interconexión 246 de redes solicitada, dependiendo de la información introducida por el usuario en relación con la opción de acciones de usuario seleccionada. En un escenario típico, la página electrónica ofrece la opción de una sesión limitada en el tiempo por un precio predeterminado. La selección de esa opción lleva al usuario a un diálogo de usuario que solicita información de facturación al usuario, incluyendo, por ejemplo, nombre, dirección, detalles de una tarjeta de crédito/débito, información de vales/cupones, nº existente de teléfono al que facturar/enviar un SMS, etc.

Un servidor de control de la sesión (preferentemente un servidor DIAMETER nativo) proporciona el control de la sesión. El servidor de control de la sesión emite informes regulares sobre las sesiones que gestiona (denominados “fichas de eventos”). En una sesión basada en DIAMETER nativo, el componente 230 de monitorización de red puede usar las fichas de eventos DIAMETER para cada sesión válida para monitorizar el uso de la sesión de cada usuario. Este, a su vez, puede ser presentado al usuario a través de una aplicación en el terminal móvil 1′, para que el usuario pueda ver, por ejemplo, que el uso ha superado un valor umbral dispuesto con antelación. Alternativamente, el uso de la sesión, a su vez, puede ser presentado al usuario a través de un mensaje emergente en una aplicación de páginas electrónicas (por ejemplo, un navegador) en el terminal móvil 1′.

Dado que la presentación de informes proviene directamente del servidor DIAMETER y no de una aplicación contadora basada en el cliente (e imprecisa), al usuario se le presenta de inmediato una información actualizada del uso de la sesión. Como apreciará el lector, esto quiere decir que el usuario puede evitar el fenómeno del “susto por facturación” (cuando se recibe (tras cierta demora) la tarifa para una sesión particular y el usuario se da cuenta de que la factura es mucho más alta de lo que entendía que sería).

Hay muchos beneficios adicionales con respecto a cuando se usa una aplicación cliente en el terminal para presentar la información de uso. Por ejemplo, se podría proporcionar al usuario una prestación de grabar historiales detalladas de su utilización o de solicitar un nivel específico de calidad de servicio (para lo cual podría imponerse una tarifa diferente, y que esa tarifa, a su vez, fuera monitorizada por el usuario). La empresa explotadora de una red celular también podría tener mayor latitud en sus servicios: ofrecer, por ejemplo, una facturación dinámica, en función de la congestión, en la que el coste por unidad de datos pueda variar según el grado de utilización de datos en la red en ese instante (que el usuario podría monitorizar, a su vez, a través de su aplicación cliente).

Está claro que el componente 230 de monitorización de red también puede usar las fichas de eventos DIAMETER para cada sesión válida para monitorizar el uso de la sesión de grupos de usuarios (como se podría requerir al proporcionar servicios a un negocio o “empresa”). Esta disposición facilita lo que ha dado en llamarse “facturación mediada” para que una empresa pueda agregar las facturaras para grupos de usuarios de la empresa. La

facturación mediada puede efectuarse presentando información sobre sesiones monitorizadas a un administrador o agente de la empresa a través de una aplicación de monitorización empresarial y de facturación central.

La operación de la invención puede ser comprendida adicionalmente considerando dos realizaciones específicas más. La primera realización, ilustrada en la Figura 3, está relacionada con el procesamiento de una solicitud de una sesión de datos desde un ordenador portátil con un TIM embebido. La segunda realización, ilustrada en la Figura 4, se refiere al procesamiento de una solicitud de una sesión de datos máquina-máquina desde un cliente máquina-máquina con un TIM embebido.

En la Figura 3, la red incluye un SCP 302 y un HLR global (G-HLR) 310. El terminal móvil 301 en este caso es un ordenador portátil con un TIM embebido. El SCP 302 puede subsumir la funcionalidad del HLR 10 de la red de la Figura 1 (garantizando que la conexión a la red de radio sigue el mecanismo expuesto con más detalle en la Figura 2A). Alternativamente, el SCP 302 puede subsumir la funcionalidad de un VLR 14 (facilitando el mecanismo de la Figura 2B) y/o la funcionalidad de un SGSN 220 (facilitando el mecanismo de la Figura 2C). Está claro que el SCP 302 también puede incorporar un agregador SS7 290 (tal como un retransmisor de SCCP) para agregar las funcionalidades SS7 que, si no, se requerirían del HLR 10, el VLR 14 y/o el SGSN 220, facilitando con ello uno cualquiera de los mecanismos representados en la Figura 2D.

Cuando el usuario desea activar su ordenador portátil en la red celular (para que este pueda abrir subsiguientemente una conexión de datos), el usuario “inicia” una aplicación de conexión a datos que se ejecuta en el sistema operativo del ordenador portátil. El ordenador portátil 301 se conecta entonces a la red de radio (etapa 351).

Como para la Figura 1, la conexión con la red de radio de la Figura 3 equivale a una solicitud de acceso a la ubicación apropiada en el SCP 302 para el número IMSI transmitido desde la ubicación apropiada de almacenamiento: no se ha asociado ningún MSISDN con el número IMSI proporcionado por el TIM. El SCP 302 determina que el número IMSI proporcionado por el TIM pertenece a otro registro. La solicitud de conexión es redirigida entonces al G-HLR 310 (etapa 352). El G-HLR 310 extrae entonces de esta solicitud el número IMSI y, suponiendo que el número IMSI esté en un intervalo mantenido por el G-HLR 310, transmite una señal testigo al SCP 302 (etapa 354) de que el IMSI ha sido reconocido por el G-HLR 310 (esta señal testigo puede ser, simplemente, una señal de confirmación (“OK”), pero puede incluir información de perfil adicional).

El SCP 302, tras la recepción de la señal testigo, almacena el IMSI temporalmente (por ejemplo, en una memoria del registro de ubicación VLR o una memoria del registro de ubicación del SGSN). Así, por lo tanto, el usuario del ordenador portátil 301 es registrado de manera efectiva en un MSC o un SGSN particulares, y cualquier información de perfil asociada con el TIM es almacenada temporalmente en el VLR 14 asociado con ese MSC 2 o ese SGSN 220.

El SCP 302 pasa la solicitud de conexión de datos a un componente 320 de pasarela de red (es decir, el SGSN 16). El componente 320 de pasarela de red recibe del G-HLR 310 una clave correspondiente al IMSI (etapa 356). Tomando la clave, junto con la solicitud remitida de conexión de datos, el componente 320 de pasarela de red establece una sesión de pasarela. Esta clave es usada, a su vez, para interrogar a un componente 330 de monitorización de red (por ejemplo, NGME, o GGSN) que determina si los datos clave están asociados con una sesión válida existente (normalmente una sesión DIAMETER nativa). Preferentemente, la señalización (etapa 358) entre el componente 320 de pasarela de red y el componente 330 de monitorización de red tiene una tarificación de cero para que no se facture al usuario el establecimiento de la sesión.

Si ya existe una sesión válida para estos datos clave, se establece la conexión de datos (etapa 362). El ordenador portátil 301 tiene acceso a una interconexión 346 de redes solicitada, normalmente Internet o una intranet de empresa.

Sin embargo, si no puede encontrarse ninguna sesión válida que corresponda a la clave, el ordenador portátil 301 puede ser redirigido, en su lugar, a una página electrónica generada por un servidor 340 de Web (etapa 364). La página electrónica presentada está personalizada para el ordenador portátil 301 según los datos clave y ofrece al usuario al menos una opción de acciones de usuario.

En este caso, el servidor de Web ofrece una “página de aterrizaje” con acceso a un portal de pago que permite al usuario comprar ya sea un paquete de sesiones limitadas en el tiempo o la cantidad de datos, o iniciar una aplicación para una relación de pago de contrato con la empresa explotadora de la red.

Se indica al usuario que proporcione detalles personales, incluyendo los detalles de su tarjeta de crédito para facilitar el establecimiento de una sesión de datos por un precio predeterminado (etapa 366).

Los datos del usuario son enviados a un servidor 350 de aplicaciones. Este servidor, a su vez, procesa los detalles de la tarjeta de crédito del usuario para su autenticación en un servidor 360 de tarjetas de crédito. Suponiendo que los detalles de la tarjeta de crédito sean autenticados, el servidor 360 de tarjetas de crédito señala ese hecho (etapa 372) en su respuesta al servidor 350 de aplicaciones.

El servidor 350 de aplicaciones, ahora que tiene los detalles autenticados de la tarjeta de crédito para el usuario, indica a un servidor DIAMETER 370 que debe iniciarse una sesión DIAMETER para este usuario (etapa 374). El SERVIDOR DIAMETER, a su vez, indica al componente 330 de monitorización de red que debe abrirse una sesión (etapa 376).

El componente 330 de monitorización de red redirige entonces al usuario a Internet (etapa 378) y, simultáneamente, cambia el estado de facturación del usuario de una tarificación igual a cero a una tarificación de datos.

Dado que el servidor DIAMETER 370 proporciona “fichas” que muestran el uso de la sesión, esta información es enviada a un servidor 380 de notificaciones (etapa 382). El servidor de notificaciones puede o bien enviar actualizaciones dispuestas de antemano en cuanto al uso porcentual (o absoluto) o puede responder a consultas del usuario (o de la aplicación cliente) en cuanto al estado de uso actual. En una implementación preferente, el servidor de notificaciones crea un canal RSS para cada sesión, permitiendo con ello que el ordenador portátil del usuario monitorice el estado usando un puerto HTTP convencional (puerto 80) y evitando cualquier necesidad de personalización del soporte lógico de cortafuegos del usuario.

Al final de una sesión dispuesta de antemano, el servidor DIAMETER 370 indica al componente 330 de monitorización de red que suspenda la sesión (y aplica una tarifa de cero a la sesión). También envía una alerta de uso al usuario por medio del servidor 380 de notificaciones.

Si la sesión terminó porque había expirado el crédito, el usuario solo precisa repetir el procedimiento de solicitud de una sesión adicional de la página de aterrizaje.

En una implementación preferente, la página electrónica presentada al ordenador portátil 301 ofrece al usuario una opción adicional de acciones de solicitar que la actual relación a base de sesiones mediada por el TIM se convierta en una relación basada en un contrato (es decir, lo que se denomina contrato de pospago). Para satisfacer esta solicitud, la empresa explotadora de la red puede simplemente encargar y enviar al usuario una tarjeta SIM convencional “suministrada” para que el usuario pueda intercambiar físicamente el TIM, sacándolo del lector de tarjeta del ordenador portátil (e introduciendo la nueva tarjeta SIM en el mismo). Posteriormente, el acceso a las sesiones de datos iría a través del flujo convencional de eventos, esbozado en relación con la Figura 1.

Como apreciará el lector, hay mecanismos alternativos para facilitar un intercambio entre las sesiones habilitadas por TIM y el acceso convencional de sesiones de datos por contrato. El IMSI que lleva el TIM podría, por ejemplo, ser suministrado en la red dada de una empresa explotadora de la red (es decir, puede haber un número MSISDN asociado con el IMSI). De hecho, podrían suministrarse varios números MSISDN al TIM, según fuera necesario para plasmar el escenario de SIM “preinstalado” de la técnica anterior mencionado más arriba.

En este caso, el servidor de Web ofrece una “página de aterrizaje” con acceso a un portal de pago que permite al usuario comprar ya sea un paquete de sesiones limitadas en el tiempo o la cantidad de datos, o iniciar una aplicación para una relación de pago de contrato con la empresa explotadora de la red.

La segunda realización, ilustrada en la Figura 4, está relacionada con una implementación máquina-máquina de la invención. La red ilustrada incluye un SCP 402 y un HLR global (G-HLR) 410. El terminal 401 en este caso es un cliente máquina-máquina (M2M) (obsérvese que este terminal no es estrictamente “móvil” en muchos casos, estando instalado el terminal en una única ubicación geográfica de la que normalmente no se mueve) con un TIM embebido.

El SCP 402 puede subsumir la funcionalidad del HLR 10 de la red de la Figura 1 (garantizando que la conexión a la red de radio siga el mecanismo expuesto con más detalle en la Figura 2A). Alternativamente, el SCP 402 puede subsumir la funcionalidad de un VLR 14 (facilitando el mecanismo de la Figura 2B) y/o la funcionalidad de un SGSN 220 (facilitando el mecanismo de la Figura 2C). Está claro que el SCP 402 también puede incorporar un agregador SS7 290 (tal como un retransmisor de SCCP) para agregar las funcionalidades SS7 que, si no, se requerirían del HLR 10, el VLR 14 y/o el SGSN 220, facilitando con ello uno cualquiera de los mecanismos representados en la Figura 2D.

Cuando el cliente M2M 401 requiere ser activado en la red celular (para que pueda abrir subsiguientemente una conexión de datos), el cliente “inicia” una aplicación de conexión a datos que se ejecuta en el sistema operativo, normalmente en respuesta a un evento desencadenante. El cliente M2M 401 se conecta entonces a la red de radio (etapa 450).

Como para la Figura 1, la conexión con la red de radio de la Figura 4 equivale a una solicitud de acceso a la ubicación apropiada en el SCP 402 para el número IMSI transmitido y para extraer el correspondiente MSISDN de abonado desde la ubicación apropiada de almacenamiento. Dado que no se ha asociado ningún MSISDN con el número IMSI proporcionado por el TIM, el SCP 402 determina que el número IMSI proporcionado por el TIM pertenece a otro registro. La solicitud de conexión es redirigida entonces al G-HLR 410 (etapa 452). El G-HLR 410 extrae entonces de esta solicitud el número IMSI y, suponiendo que el número IMSI esté en un intervalo mantenido por el G-HLR 410, transmite una señal testigo al SCP 402 (etapa 454) de que el IMSI ha sido reconocido por el G-

HLR 410 (esta señal testigo puede ser, simplemente, una señal de confirmación (“OK”), pero puede incluir información de perfil adicional).

El SCP 402, tras la recepción de la señal testigo, almacena el IMSI temporalmente en una ubicación del registro de ubicación de visitantes (VLR) (no mostrado). Así, por lo tanto, el cliente M2M 401 es registrado de manera efectiva en un MSC particular (no mostrado), y cualquier información de perfil asociada con el TIM es almacenada temporalmente en el VLR asociado con ese MSC.

El SCP 402 pasa la solicitud de conexión de datos a un 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 remitida para una conexión de datos, el componente 320 de pasarela de red establece una sesión de pasarela. Esta clave es usada, a su vez, para interrogar a un componente 430 de monitorización de red (por ejemplo, NGME, o GGSN) que determina si los datos clave están asociados con una sesión válida existente (normalmente una sesión DIAMETER nativa). Preferentemente, la señalización (etapa 458) entre el componente 420 de pasarela de red y el componente 430 de monitorización de red tiene una tarificación de cero para que no se facture al dispositivo cliente 401 el establecimiento de la sesión.

Suponiendo que no exista ninguna sesión válida correspondiente a esa clave, el componente 430 de monitorización de red se comunica con un servidor DIAMETER 440 para autenticar una nueva sesión de datos M2M (etapa 462) para el cliente M2M 401.

El servidor DIAMETER 440, a su vez, indica al componente 430 de monitorización de red que debe abrirse una sesión (etapa 464).

El componente 430 de monitorización de red redirige entonces al usuario a un servidor M2M 450 solicitado por medio de una red de línea fija tal como Internet 470 (etapa 466) y simultáneamente cambia el estado de facturación de la sesión del cliente M2M de una tarificación igual a cero a una tarificación de datos.

Al final de una sesión dispuesta de antemano, el servidor DIAMETER 440 indica al componente 430 de monitorización de red que suspenda la sesión (y aplica una tarifa de cero a la sesión).

El servidor DIAMETER 440 también envía una alerta de uso de uso (usando fichas DIAMETER, etapa 468) a un motor 480 de mediación de facturación, que genera un evento de facturación correspondiente al uso documentado de la sesión.

Según se describe con detalle adicional en la solicitud de patente del Reino Unido GB 0815200.1, en tramitación como la presente, el cliente M2M envía y recibe mensajes de texto cortos (SMS) a una plataforma SMS M2M 495 dedicada. Estos mensajes SMS son transportados de manera convencional a través de una pasarela SMS 490 y luego a través de una conexión 470 de Internet a la plataforma SMS M2M 495.

La pasarela SMS 490 también pasa datos relativos a los mensajes SMS transferidos al motor 480 de mediación para permitir la facturación de estos mensajes.

Aunque en la exposición precedente a menudo se dice que los terminales son “móviles”, no debería interpretarse que el término “móvil” requiera que un terminal *siempre* sea móvil; meramente que tiene la capacidad de estar en comunicación con una red de telecomunicaciones inalámbricas que permite la movilidad. Por ejemplo, un terminal de PC o un cliente M2M que nunca se muevan de una ubicación geográfica particular pueden en este sentido seguir considerándose móviles, porque *podrían* ser movidos a una ubicación diferente y, no obstante, seguir accediendo a la misma red. Cuando se usa la expresión “terminal móvil” en la presente exposición, ha de entenderse que incluye la posibilidad de un terminal que es “semipermanente” o incluso “fijo” cuando el contexto no contradiga tal interpretación.

REIVINDICACIONES

1. Una red celular de telecomunicaciones para facilitar conexiones de comunicación para terminales que tienen módulos de identificación por testigo, incluyendo la red:

un registro (10; 2, 6; 11, 14; 16; 302; 402) de ubicación adaptado para recibir de los terminales solicitudes de acceso a la red y, si las solicitudes están asociadas con un módulo de identificación por testigo, adaptado para redirigir las solicitudes;
un registro (210; 310; 410) de testigos adaptado para recibir dichas solicitudes redirigidas, para generar datos de identificación de conexión por testigo y para transmitir los datos de identificación de conexión por testigo al registro de ubicación para identificar el terminal ante el registro de ubicación;
un componente (220; 320; 420) de pasarela de red adaptado para establecer una comunicación entre la red y el terminal según los datos de identificación de conexión por testigo; y
un componente (230; 330; 430) de monitorización de red adaptado para realizar una gestión del servicio.

2. Una red según se reivindica en la reivindicación 1 en la que las conexiones de comunicación son conexiones de comunicación solo de datos.

3. Una red según se reivindica en las reivindicaciones 1 o 2 en la que cada solicitud de acceso a la red procedente de un terminal que tiene un módulo de identificación por testigo incluye un número IMSI que identifica de forma única al módulo de identificación por testigo.

4. Una red según se reivindica en las reivindicaciones 2 o 3 en la que la red, además, incluye:

un servidor (340) que está adaptado para servir páginas electrónicas de diálogos de usuario a terminales móviles según los datos de identificación de conexión por testigo, presentando cada página electrónica al usuario al menos una opción de acciones de usuario; y
una pasarela de interconexión de redes que está adaptada para gobernar el acceso de la red celular a una interconexión (346) de redes;
incluyendo la verificación de autenticación de la sesión llevada a cabo por el componente de monitorización de red determinar si los datos de identificación de conexión por testigo están asociados con una sesión válida;
estando adaptado el componente (320) de pasarela de red para dirigir al terminal a una página electrónica de diálogos de usuario servida por un servidor de Web cuando el componente de monitorización de red determina que no hay ninguna sesión asociada válida, y
dándosele acceso al terminal a la interconexión de redes dependiendo de la indicación de la opción de acciones de usuario desde el terminal.

5. Una red según se reivindica en las reivindicaciones 2 o 3 en la que la red, además, incluye:

una pasarela de interconexión de redes que está adaptada para gobernar el acceso de la red celular a un servidor M2M (450) por medio de una interconexión (470) de redes;
incluyendo la verificación de autenticación de la sesión llevada a cabo por el componente de monitorización de red determinar si los datos de identificación de conexión por testigo están asociados con una sesión M2M válida; y
estando adaptado el componente de monitorización de red para dirigir al terminal al servidor M2M cuando el componente de monitorización de red determina que los datos de identificación de conexión por testigo están asociados con una sesión M2M válida.

6. Una red según se reivindica en las reivindicaciones 4 o 5 en la que la interconexión de redes es Internet.

7. Una red según se reivindica en las reivindicaciones 4 o 5 en la que la interconexión de redes es una intranet.

8. Una red según se reivindica en una cualquiera de las reivindicaciones precedentes en la que el registro de ubicación está distribuido, teniendo un punto de agregación para agregar funcionalidad de señalización y una entidad de red adaptada para realizar una funcionalidad adicional de registro de ubicación, estando dicho punto de agregación y dicha entidad de red en comunicación mutua.

9. Un método para facilitar conexiones de comunicación entre terminales que tienen módulos de identificación por testigo y una red celular de telecomunicaciones, incluyendo la red celular un registro de ubicación, un registro de testigos, un componente de pasarela de red, un componente de monitorización de red, un servidor y una pasarela de interconexión de redes, incluyendo el método:

en el registro de ubicación, recibir de un terminal una solicitud de acceso a la red, determinar si la solicitud está asociada con un módulo de identificación por testigo y redirigir la solicitud al registro de testigos;
en el registro de testigos, recibir la solicitud redirigida, generar datos de identificación de conexión por testigo y transmitir los datos de identificación de conexión al registro de ubicación, identificando con ello al terminal ante el registro de ubicación;

establecer una comunicación entre la red y el terminal según los datos de identificación de conexión por testigo; y
efectuar una verificación de autenticación de la sesión.

10. Un método según se reivindica en la reivindicación 8 en el que las conexiones de comunicación son conexiones de comunicación solo de datos.

11. Un método según se reivindica en las reivindicaciones 8 o 9 en el que la etapa de verificación de autenticación de la sesión incluye determinar si los datos de identificación de conexión por testigo están asociados con una sesión válida, e incluyendo el método, además:

servir al terminal una página electrónica de diálogos de usuario según los datos de identificación de conexión por testigo, presentando la página electrónica al usuario al menos una opción de acciones de usuario;
dirigir al terminal a la página electrónica de diálogos de usuario cuando el componente de monitorización de red determina que no hay ninguna sesión asociada válida; y
permitir el acceso desde la red celular a la interconexión de redes dependiendo de la indicación de la opción de acciones de usuario desde el terminal.

12. Un método según se reivindica en las reivindicaciones 8 o 9 en el que la pasarela de interconexión de redes gobierna el acceso desde la red celular a un servidor M2M mediante una interconexión de redes; en el que la etapa de verificación de autenticación de la sesión incluye determinar si los datos de identificación de conexión por testigo están asociados con una sesión M2M válida; e incluyendo el método, además:

dirigir al terminal al servidor M2M cuando el componente de monitorización de red determina que los datos de identificación de conexión por testigo están asociados con una sesión M2M válida.

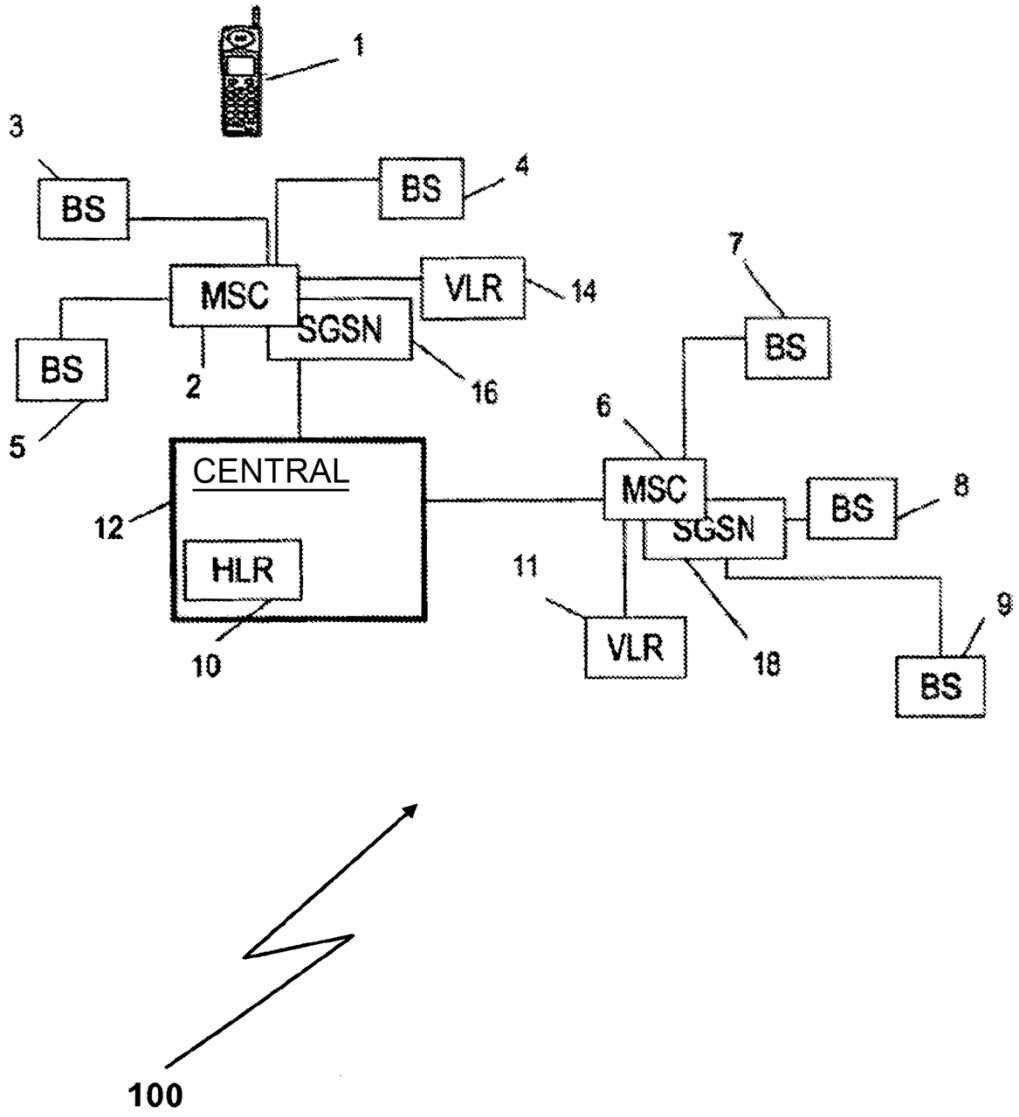

1
3
BS
4
BS
MSC
VLR
14
SGSN
7
BS
BS
2
16
5
6
CENTRAL
MSC
BS
8
12
SGSN
HLR
11
9
VLR
18
10
BS
100

Fig 1

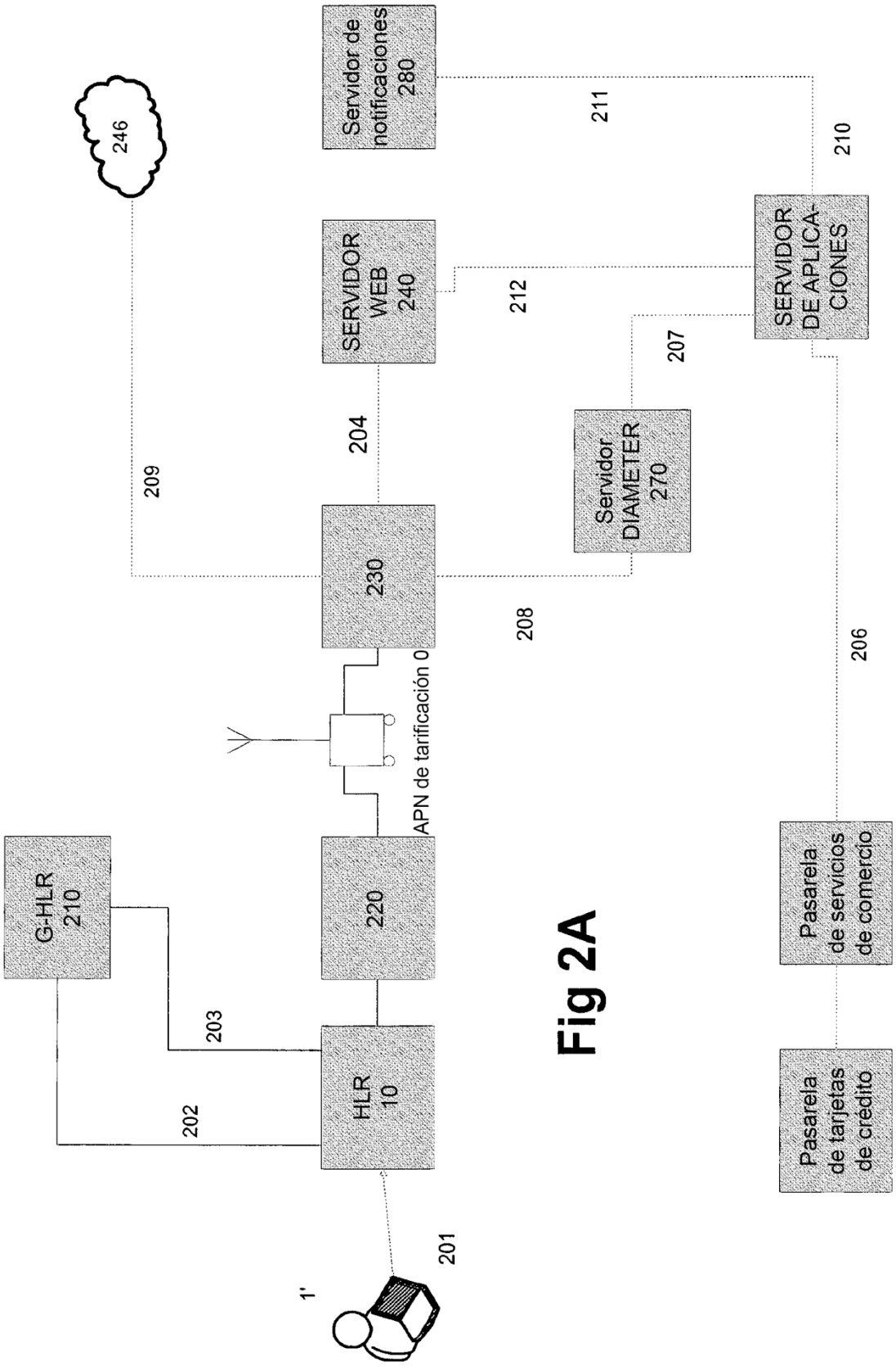

246
Servidor de notificaciones 280
211
210
SERVIDOR WEB 240
SERVIDOR DE APLICACIONES
212
207
204
209
Servidor DIAMETER 270
230
208
206
APN de tarificación 0
G-HLR 210
220
Pasarela de servicios de comercio
203
202
HLR 10
Pasarela de tarjetas de crédito
1'
201

Fig 2A

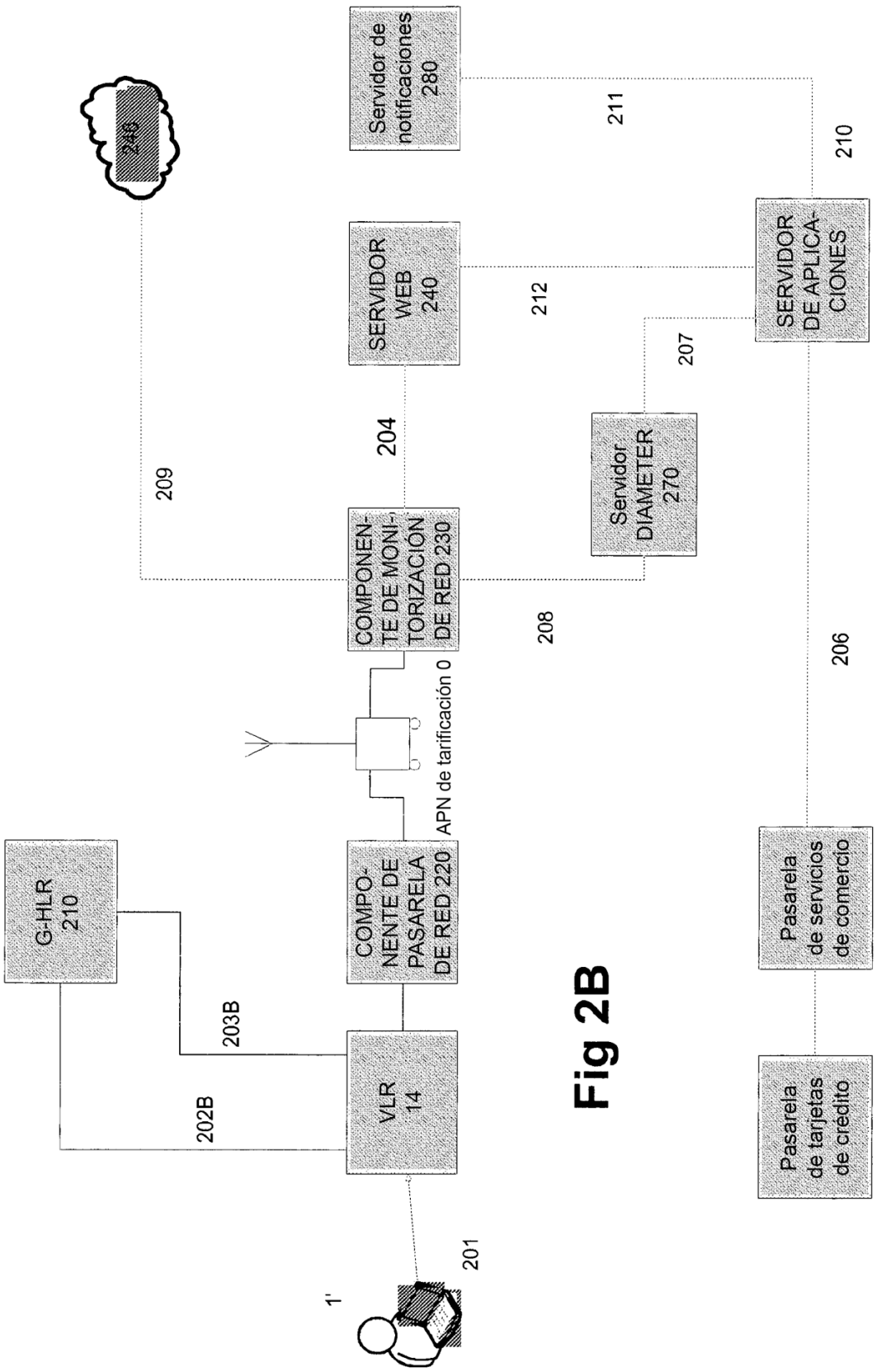

Servidor de notificaciones 280
211
210
248
SERVIDOR WEB 240
212
SERVIDOR DE APLICACIONES
207
209
204
Servidor DIAMETER 270
COMPONENTE DE MONITORIZACIÓN DE RED 230
208
206
APN de tarificación 0
G-HLR 210
COMPONENTE DE PASARELA DE RED 220
Pasarela de servicios de comercio
203B
202B
VLR 14
Pasarela de tarjetas de crédito
201
1'

Fig 2B

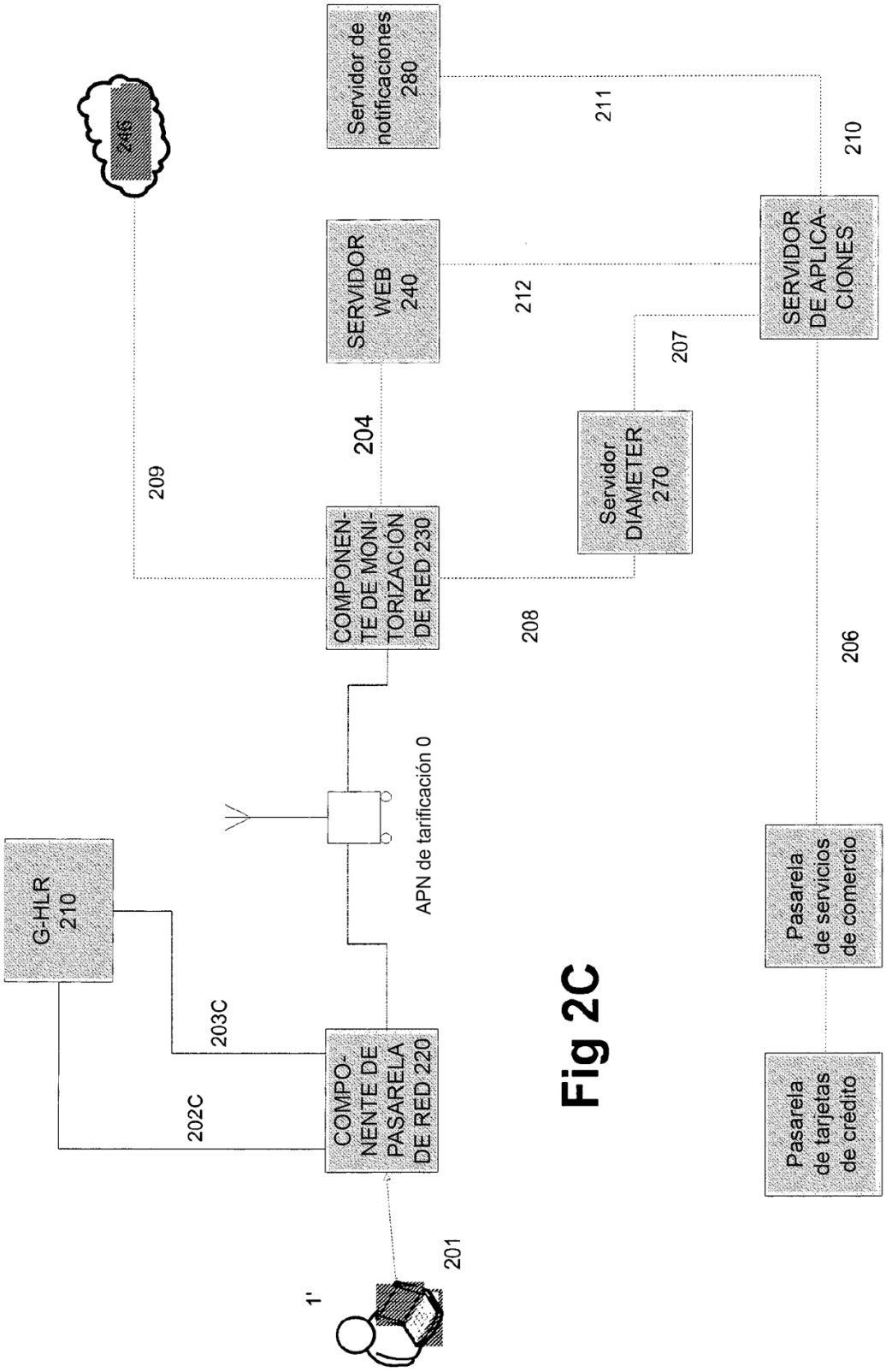
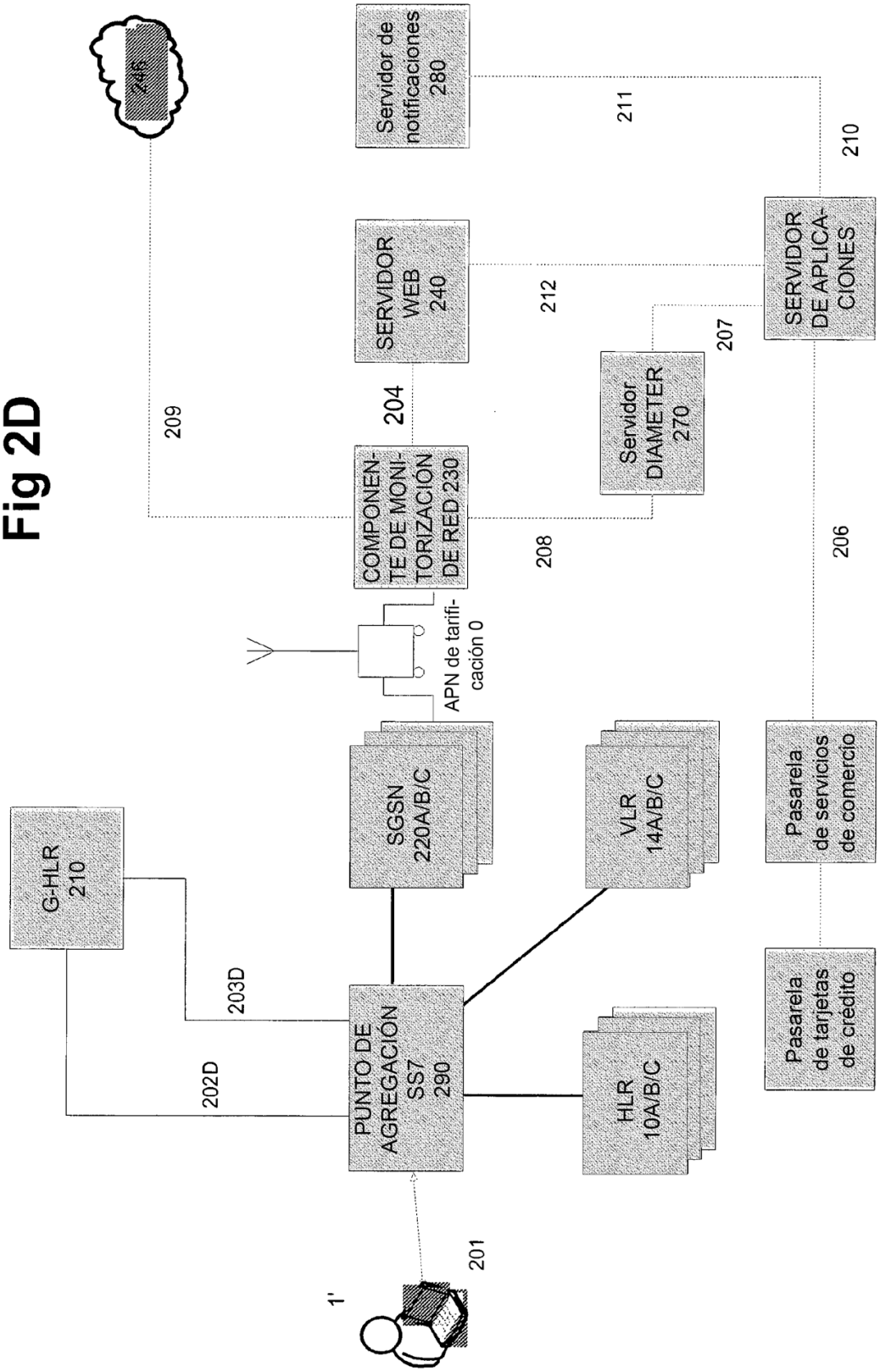

246
Servidor de notificaciones 280
211
210
SERVIDOR WEB 240
212
SERVIDOR DE APLICACIONES
207
Servidor DIAMETER 270
209
204
COMPONENTE DE MONITORIZACIÓN DE RED 230
208
206
APN de tarificación 0
G-HLR 210
203C
202C
COMPONENTE DE PASARELA DE RED 220
Pasarela de servicios de comercio
Pasarela de tarjetas de crédito
201
1'

Fig 2C

Fig 2D


246
Servidor de notificaciones 280
211
210
SERVIDOR WEB 240
212
SERVIDOR DE APLICACIONES
207
Servidor DIAMETER 270
209
204
COMPONENTE DE MONITORIZACIÓN DE RED 230
208
206
APN de tarificación 0
SGSN 220A/B/C
VLR 14A/B/C
Pasarela de servicios de comercio
G-HLR 210
203D
202D
PUNTO DE AGREGACIÓN SS7 290
HLR 10A/B/C
Pasarela de tarjetas de crédito
201
1'

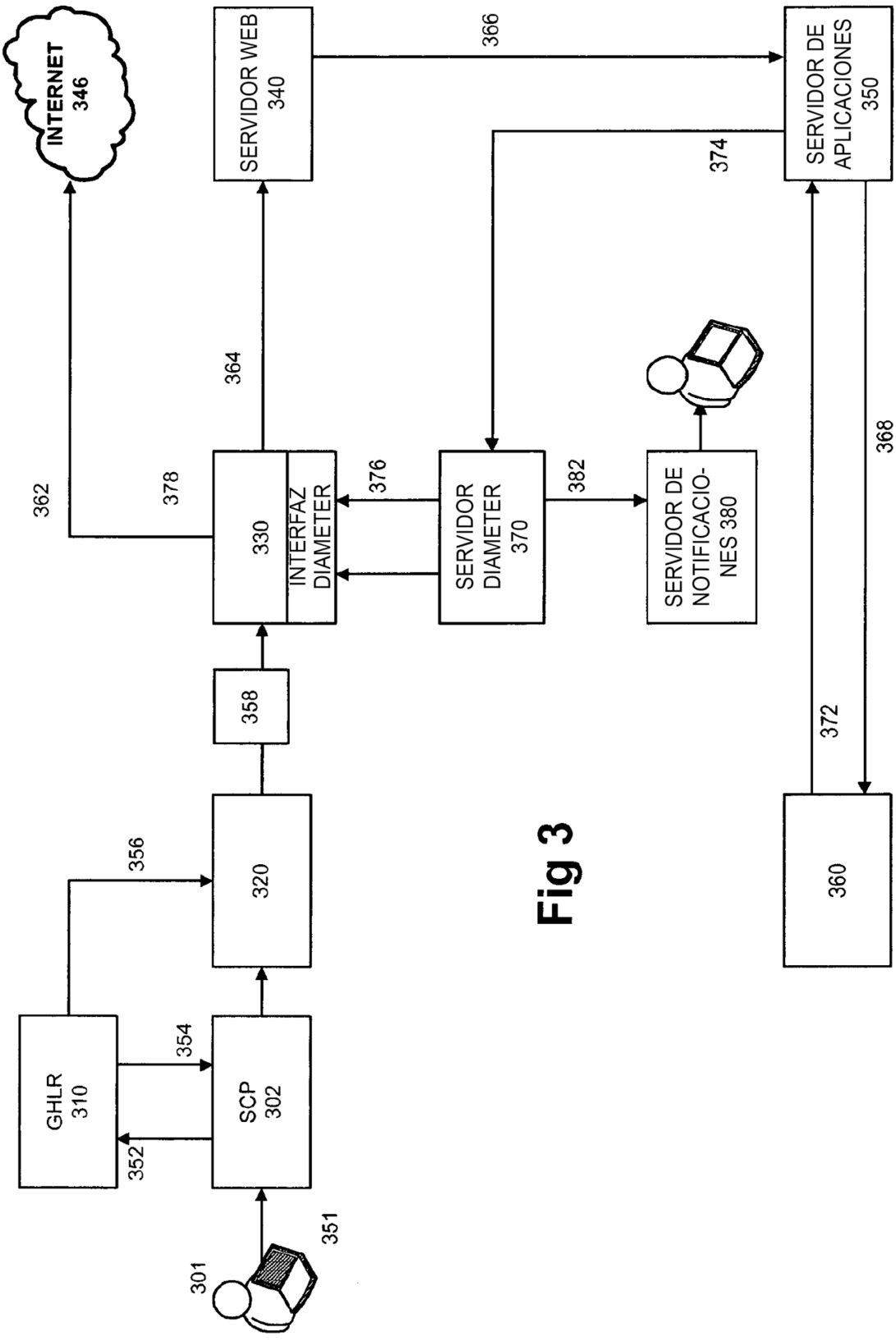

INTERNET
346
SERVIDOR WEB
340
366
SERVIDOR DE
APLICACIONES
350
374
364
362
378
330
INTERFAZ
DIAMETER
376
SERVIDOR
DIAMETER
370
382
SERVIDOR DE
NOTIFICACIO-
NES 380
368
358
372
356
320
360
GHLR
310
354
SCP
302
352
351
301

Fig 3

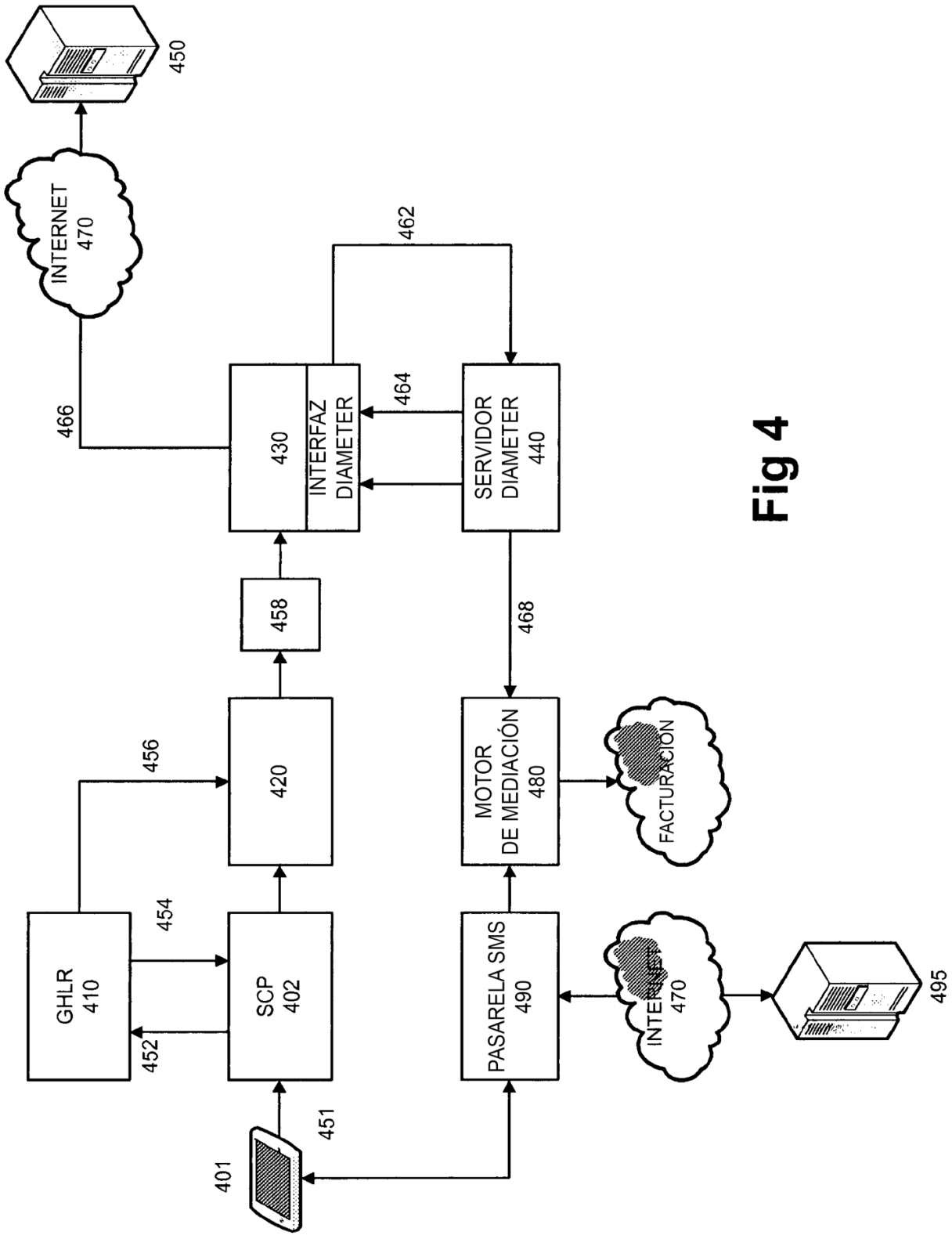

450
INTERNET
470
462
466
430
INTERFAZ
DIAMETER
464
SERVIDOR
DIAMETER
440
458
468
456
420
MOTOR
DE MEDIACIÓN
480
FACTURACIÓN
GHLR
410
454
SCP
402
PASARELA SMS
490
INTERNET
470
495
452
451
401

Fig 4