(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 458 295**

(51) Int. CI.:

H04L 12/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.03.2005 E 05716144 (0)**

(97) Fecha y número de publicación de la concesión europea: **12.03.2014 EP 1810474**

(54) Título: **Disposición, nodos y método en relación con acceso a servicios sobre un sistema de comunicación**

(30) Prioridad:

10.11.2004 US 626691 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 STOCKHOLM, SE

(72) Inventor/es:

BOMAN, KRISTER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Disposición, nodos y método en relación con acceso a servicios sobre un sistema de comunicación

Campo de la invención

La presente invención se refiere a una disposición en un sistema de comunicaciones que participa en procedimientos de acceso a, o solicitud de, servicios de estación de usuario y comprende una serie de nodos de soporte de datos en paquetes, una serie de nodos de gestión de facturación y/o de políticas y una serie de funciones de aplicación que administran la gestión de movilidad y el control de llamadas de estaciones de usuario móviles que solicitan servicios o acceden a los mismos. La invención se refiere asimismo a un nodo en un sistema de comunicaciones que soporta datos en paquetes, que está dispuesto para comunicar con una función de aplicación y un nodo de soporte de datos en paquetes.

La invención se refiere además a un método involucrado en la solicitud de/el acceso a servicios, en un sistema de comunicaciones que soporta comunicación de datos en paquetes y que comprende una serie de nodos de datos en paquetes, una serie de nodos de gestión de facturación y/o de políticas y una serie de funciones de aplicación que administran la gestión de movilidad y el control de llamadas de estaciones de usuario móviles que solicitan/acceden a servicios.

Estado de la técnica

Los denominados servicios IM (Internet IP Multimedia, multimedia IP por internet) son cada vez más atractivos y se utilizan ya ampliamente. Los subsistemas IMS (IP Multimedia Subsystems, subsistemas multimedia IP) 3GPP proporcionan una capacidad de control de sesión basada en IP que se basa en el protocolo SIP (Session based Initiation Protocol, protocolo de inicio basado en sesiones). IMS puede utilizarse por ejemplo para la prestación de servicios tales como pulsar para hablar, mensajería instantánea, presencia y conferencia. IMS en UMTS (Universal Mobile Telecommunication System, sistema universal de telecomunicaciones móviles) soportará aplicaciones multimedia IP tales como video, audio y conferencias multimedia. Tal como se ha mencionado anteriormente, 3GPP utilizará SIP, protocolo de inicio de sesiones, como el protocolo de señalización para crear y finalizar sesiones multimedia, véase por ejemplo el documento IETF RFC (Request For Comments) 3261, que trata sobre cómo se protege la señalización SIP entre el abonado y el IMS, cómo se autentica el abonado y cómo el abonado autentica el IMS.

La arquitectura de seguridad actual para IMS está especificada en 3GPP TS 33.203. Sin embargo, existe un problema en el hecho de que existirán implementaciones de los servicios mencionados anteriormente que no sean totalmente compatibles con IMS 3GPP. IMS 3GPP, por ejemplo, utiliza exclusivamente IPv6 (Internet Protocol version 6, protocolo de internet versión 6) aunque pueden seguir existiendo implementaciones IMS basadas en IPv4. Sin embargo, la utilización de IPv4 en lugar de IPv6 es solamente una de las diferencias entre las implementaciones IMS "precoces" y las implementaciones plenamente compatibles con IMS 3GPP. Se ha reconocido que la no compatibilidad con características de seguridad 3GPP TS 33.203 producirá principalmente problemas en el equipo de usuario (UE) debido a la ausencia potencial de soporte de la interfaz USIM/ISIM, en particular para estaciones de usuario compatibles solamente con 2G. Por lo tanto, se ha comprendido que para dichas implementaciones IMS "precoces", se requieren mecanismos de protección contra las amenazas de seguridad más significativas.

Una solución temporal de este tipo para las implementaciones IMS "precoces" se propone en 3GPP TR 33.878. El enfoque de este documento es que el GGSN (Gateway GPRS Support Node, nodo de soporte de pasarela GPRS) deberá enviar MSISDN y la dirección IP de una estación de usuario (UE equipo de usuario) hacia un servidor Radius sobre la interfaz Gi. El servidor Radius transfiere a continuación la MSISDN y la dirección IP al HSS (Home Subscriber Server, servidor propio de abonado). Cuando la estación de usuario, o el UE, envía una solicitud de registro SIP hacia una función de control de sesión/llamada de servicio (S-CSCF, Serving-Call/Session Control Function), que incluye la identidad privada IM (IP Multimedia, multimedia IP), la S-CSCF consultará al HSS el cual, basándose en la identidad IMS puede identificar la MSISDN y la dirección IP coincidentes del UE y devolver la dirección IP a la S-CSCF. La S-CSCF comprobará la dirección IP almacenada en la S-CSCF para ver si coincide con la dirección IP recibida desde el UE. Si las dos direcciones IP son iguales, la S-CSCF puede avanzar al procedimiento de registro, pero si no son iguales, presumiblemente debido a un ataque en curso, se finaliza la sesión. Esto proporciona la posibilidad de evitar ciertos ataques, tales como por ejemplo un atacante que utiliza identidades IMS de una víctima, lo que puede tener como consecuencia que el usuario atacado tenga que pagar el servicio al que ha accedido el atacante.

Un operador corre asimismo el riesgo de que el atacante no pague por el portador, por ejemplo un portador conversacional, debido al hecho de que, por ejemplo, está implementada FBC (Flow Based Charging, facturación basada en flujo) y la facturación al portador es cero. Esto significa que en algunos casos de utilización, un atacante podría utilizar ciertos servicios gratis.

El documento 3GPP TR 33.878 asume que durante una solicitud de contexto-PDP hacia el IMS, el GGSN deberá enviar un mensaje de "Radius Accounting-Request-Start" (iniciar solicitud de contabilización Radius) a un servidor Radius acoplado al HSS. Esto puede llevar a suponer que un operador utiliza un APN (Access Point Name, nombre

de punto de acceso) IMS específico o que el UE utiliza un contexto PDP de señalización. Sin embargo, se considera que la hipótesis relativa a la utilización de un APN IMS específico es demasiado restrictiva desde el punto de vista del diseño. El documento 3GPP TS 23.228 estipula que "cuando el UE utiliza acceso GPRS para servicios IMS, deberá ser capaz de establecer un contexto PDP de señalización dedicado para la señalización relacionada con el subsistema IM o utilizar un contexto PDP de propósito general para el tráfico de señalización del subsistema IM". Por lo tanto, no existe ninguna garantía de que el UE utilice un contexto PDP de señalización para IMS, lo que puede conducir a la conclusión de que el GGSN debería enviar entonces la dirección IP de un UE hacia un servidor Radius para todos los servicios. Además, un UE puede tener varias direcciones IP hacia un mismo GGSN y parece necesario que, en tal caso, el GGSN tenga que enviar todas estas direcciones IP hacia el servidor Radius. Además, en el caso general un UE puede estar acoplado a más de un GGSN o puede tener activada más de una conexión de red IP. Dichos escenarios no se discuten en el documento 3GPP TR 33.878.

Además, la solución descrita en este documento sugiere la introducción de un denominado "temporizador de reposo" en GGSN. Esto tiene un impacto sobre cómo son asignadas o liberadas las direcciones IP hacia un UE, y cómo una dirección IP puede ser reutilizada para un usuario cuando se produce el restablecimiento de un contexto PDP en una etapa posterior. Aparentemente, la razón para la introducción del temporizador de reposo es reducir la carga sobre la HSS y, cuando no existe contexto PDP disponible entre el GGSN y el UE, el GGSN almacena o reserva la dirección IP asignada para un UE específico durante un tiempo que es igual al periodo del tiempo establecido en el temporizador de reposo. Esto significa que el GGSN, tras la terminación de todos los portadores, no envía una detención de solicitud de contabilización hasta que ha expirado el temporizador de reposo. Por lo tanto, el temporizador de reposo no se ha introducido por razones de seguridad si no para reducir la comunicación hacia el HSS que es responsable de la creación de los vectores de autenticación, y por lo tanto la intención es reducir la comunicación con el HSS, o para no permitir más comunicación con el HSS que la necesaria a efectos de evitar que resulte sobrecargado, lo cual puede tener la consecuencia de que se verían perjudicados otros servicios, por ejemplo voz. La utilización del temporizador de reposo es inconveniente, por ejemplo, debido a que existirá un mayor riesgo de conflictos entre direcciones IP asignadas dinámicamente. Además, se mantienen más recursos de los necesarios.

La solución propuesta es asimismo inconveniente porque se envía cada vez más información desde el GGSN sobre la interfaz Gi, la cual está cada vez más sobrecargada. Es asimismo una desventaja que se requiera un servidor Radius para verificar las direcciones IP y, tal como se ha mencionado anteriormente, no se tengan en cuenta diseños generales tales como cuando, por ejemplo, un UE está acoplado a más de un GGSN y/o ha activado más de una conexión de red IP, etc.

El documento WO 191446 da a conocer un método para unificar facturación basada en servicios y facturación basada en recursos, mediante la utilización del identificador común.

Compendio de la invención

Por lo tanto, tal como se ha mencionado inicialmente, es necesaria una disposición mediante la cual pueda proporcionarse seguridad IMS de manera directa y sencilla. En particular, se necesita una disposición mediante la cual pueda proporcionarse la denominada seguridad IMS "precoz", es decir, en redes que aún no son "completamente" compatibles con la Versión 5 del 3GPP TS 33.203. En particular, se requiere una disposición mediante la cual puedan detectarse e impedirse ataques y, en particular, mediante la cual pueda aumentarse la seguridad para usuarios finales así como para operadores, por ejemplo, de tal modo que se impida que un atacante utilice estos servicios gratis o haciendo que los pague otra persona, y que un ataque pueda detectarse lo antes posible, lo cual es extremadamente importante para el usuario final así como para el operador.

En particular, se necesita una disposición que sea flexible y que pueda adaptarse a diferentes entornos de red, tal como por ejemplo los denominados entornos de red consciente ("aware network"). Además, se requiere una disposición que tenga en cuenta y aproveche el desarrollo dentro de sistemas, por ejemplo, 3GPP o similares. Asimismo, se requiere una disposición mediante la cual la cantidad de información enviada sobre una denominada interfaz Gi desde nodos de soporte pasarela GPRS o similares pueda reducirse en lugar de aumentarse. Más específicamente, se requiere una disposición mediante la cual no se requiera la introducción de nodos adicionales y, más en general, mediante la cual el número de nodos implicados y afectados pueda mantenerse lo más bajo posible. Se requiere asimismo una disposición que reduzca o incluso elimine los inconvenientes e impactos sobre la asignación o liberación de direcciones IP hacia un UE, que surgen mediante la introducción de un denominado temporizador de reposo en un GGSN.

Se requiere asimismo una disposición que pueda utilizarse en un diseño general y que tenga en cuenta situaciones, tales como por ejemplo cuando un equipo de usuario está acoplado a más de un GGSN (o CGSNs en otras pasarelas) y/o cuando un equipo de usuario ha activado más de una conexión de red IP. Adicionalmente, se requiere un nodo que ayude a la consecución de uno o varios de los objetivos mencionados anteriormente. Se requiere asimismo un método mediante el cual puedan conseguirse uno o varios de los objetivos mencionados anteriormente.

Por lo tanto, tal como se ha mencionado inicialmente, se da a conocer una disposición en la que uno o varios nodos de soporte de datos en paquetes comprenden medios adaptados para enviar una primera información relativa a la identidad de estación de usuario móvil sobre una primera interfaz (Gx, Gy; Gx/Gy) a un nodo de gestión de

facturación y/o de políticas, a la recepción de una solicitud para servicios de portador desde una estación de usuario móvil, la función o funciones de aplicación comprenden medios para, a la recepción de una solicitud para una sesión de servicio (SIP) desde una estación de usuario móvil (UE), enviar una segunda información relativa a la identidad de estación de usuario móvil al nodo de gestión de facturación y/o de políticas, sobre una segunda interfaz (Rx, Rx/Gq), y en la que el nodo de gestión de políticas y/o facturación comprende medios de verificación adaptados para determinar si la solicitud para un servicio de portador al nodo de soporte de datos en paquetes y la solicitud para una sesión de servicio a la función de aplicación (AF; P/S/I-CSCF) están originadas en una única estación de usuario móvil (UE). En particular, la primera información relativa a la identidad de la estación de usuario móvil comprende uno o varios de la MSISDN, la IMSI y dirección IP de la estación de usuario móvil, y la segunda información relativa a la identidad de la estación de usuario móvil comprende la identidad privada IMS (IMPI) y/o la identidad pública IMS (IMPU), o la IMSI y/o la MSISDN, por ejemplo obtenidas de una identidad privada o pública IMS (IMPI, IMPU), o estando adaptada cada función de aplicación para obtener dicha información externamente, por ejemplo de un HSS.

En particular, las direcciones IP se reciben en, o se obtienen a partir de, la primera información relativa a la estación de usuario móvil y la segunda información relativa a la identidad de la estación de usuario móvil, y los medios de verificación están adaptados para comparar la dirección IP obtenida de la función de aplicación (AF) con la dirección IP obtenida del nodo de soporte de datos en paquetes. En una realización, los medios de verificación están adaptados para, si se requiere, establecer y, utilizando la IMSI y/o la MSISDN de dichas primera y segunda informaciones relativas a la identidad de las estaciones de usuario móviles respectivamente, comparar las direcciones IP asociadas. El nodo de gestión de facturación y/o de políticas puede estar adaptado asimismo para deducir la IMSI y/o la MSISDN a partir de una identidad de usuario privada y/o pública IMS (IMPI/IMPU).

En una realización ventajosa, el nodo de gestión de facturación y/o de políticas está adaptado para construir una identidad de usuario privada utilizando la IMSI de una estación de usuario móvil, por ejemplo, cuando no está implementada ninguna aplicación ISIM, y además está adaptado particularmente para identificar e instalar normas de facturación a aplicar a la recepción de una solicitud de las mismas desde un nodo de soporte de datos en paquetes.

Según la invención, si la primera y la segunda informaciones relativas a la identidad están originadas en una única estación de usuario móvil, el nodo de gestión de facturación y/o de políticas se adapta en particular para implementar las normas de facturación proporcionadas. Por otra parte, si la primera y la segunda informaciones relativas a la identidad no están originadas en una única estación de usuario móvil, el nodo de gestión de facturación y/o de políticas puede adaptarse para rechazar las normas de facturación y/o desactivar normas de facturación implementadas y desechar el tráfico de flujo de IP relacionado, y además para informar a la función de aplicación (AF) de que no está disponible un contexto PDP.

Alternativamente, si la primera y la segunda informaciones relativas a la identidad no están originadas en una única estación de usuario móvil, el nodo de gestión de facturación y/o de políticas puede ser adaptado para seleccionar si desactiva las normas de facturación en el nodo de soporte de datos en paquetes, o las mantiene activas (o las activa). En una realización particular, el nodo de soporte de datos en paquetes comprende un nodo que gestiona funciones para el plano del tráfico (TPF, Traffic Plane Functions), por ejemplo un GGSN que implementa TPF o un CGSN que implementa TPF. Alternativamente, puede comprender un nodo independiente o un nodo de pasarela que gestione TPF, o TPF y ejecución de políticas (PEP).

De acuerdo con diferentes realizaciones, el nodo de gestión de facturación y/o de políticas comprende una CRF, una PDF o un PCCN. En particular, la primera interfaz es Gx o Go/Gx fusionada con Gy si el nodo de gestión de facturación y/o de políticas está fusionado con un OCS, y la segunda interfaz comprende Rx o Rx fusionada con Gq.

Se da a conocer asimismo un nodo (funcional, lógico o físico) en un sistema de comunicación, tal como se ha mencionado inicialmente, que está adaptado para recibir la primera información relativa a la identidad de la estación de usuario móvil desde un nodo de soporte de datos en paquetes, en relación con una solicitud de servicio de portador para una estación de usuario móvil, o a la recepción de una solicitud para un servicio de portador procedente de una estación de usuario móvil (UE) en el nodo de soporte de datos en paquetes, para recibir la segunda información relativa a la identidad de la estación de usuario móvil desde una función de aplicación en relación con una sesión de servicio o a la recepción de una solicitud de una sesión de servicio en el mismo, y comprende medios de verificación para determinar si la solicitud para un servicio de portador (al nodo de soporte de datos en paquetes) y la solicitud para una sesión de servicio (a la función de aplicación) están originadas en la misma estación de usuario móvil. En particular, la primera información relativa a la identidad de la estación de usuario móvil comprende uno o varios de la MSISDN, la IMSI y la dirección IP de la estación de usuario móvil. En mayor detalle, la segunda información relativa a la identidad de la estación de usuario móvil comprende la identidad privada IMS (IMPI) y/o la identidad pública IMS (IMPU) de la estación de usuario móvil o la IMSI, y/o el nodo de gestión está adaptado para obtener la IMSI y/o la MSISDN a partir de la IMPI y/o la IMPU, y/o está adaptado para solicitar dichas IMSI y/o MSISDN a la función de aplicación.

Preferentemente, los medios de verificación están adaptados para comparar la dirección IP correspondiente a, o incluida en la primera información relativa a la identidad de la estación de usuario móvil, y la dirección IP correspondiente a, o incluida en la segunda información relativa a la identidad de la estación de usuario móvil, y en

particular, si se requiere establecer y utilizar la IMSI y/o la MSISDN de dichas primera y segunda informaciones relativas a la identidad de las estaciones de usuario móviles, para comparar las direcciones IP asociadas. Alternativamente, éstos están adaptados para derivar la IMSI y/o la MSISDN a partir de una identidad de usuario pública y/o privada IMS (IMPI/IMPU) recibida. En particular, el nodo de gestión de facturación y/o de políticas está adaptado para construir una identidad de usuario privada utilizando la IMSI de una estación de usuario móvil, por ejemplo cuando no está implementada ninguna aplicación IMSI.

Éste puede estar adaptado asimismo para identificar e instalar normas de facturación a aplicar a la recepción de una solicitud de las mismas desde un nodo de soporte de datos en paquetes. En particular, está adaptado para identificar e instalar normas de facturación a aplicar a la recepción de una solicitud de las mismas desde un nodo de soporte de datos en paquetes, y si la primera y la segunda informaciones relativas a la identidad están originadas en una única estación de usuario móvil, para implementar las normas de facturación proporcionadas, y si la información relativa a la identidad del primer y el segundo usuario no están originadas en una única estación de usuario móvil, para rechazar las normas de facturación y/o desactivar las normas de facturación implementadas y desechar el tráfico de flujo de IP relacionado, para informar a la función de aplicación (AF) de que no está disponible un contexto PDP, o para seleccionar si desactiva las normas de facturación en el nodo de soporte de datos en paquetes, o las mantiene activas, si ya lo estaban. En particular, éste comprende una CRF, una PDF o un PCCN o un nodo con una funcionalidad similar.

Además, se da a conocer un método, tal como se ha mencionado inicialmente, que comprende las etapas de recibir una solicitud de servicios de portador desde una estación de usuario móvil en un nodo de soporte de datos en paquetes; enviar, desde el nodo de soporte de datos en paquetes, la primera información relativa a la identidad de estación de usuario móvil, de la estación de usuario móvil, a un nodo de gestión de facturación y/o de políticas; recibir a continuación, antes o sustancialmente al mismo tiempo, una solicitud de una sesión de servicio procedente de la estación de usuario móvil en una función de aplicación; enviar, desde la función de aplicación, la segunda información relativa a la identidad de la estación de usuario móvil al nodo de gestión de facturación y/o de políticas; y establecer, en el nodo de gestión de facturación y/o de políticas, si la solicitud para un servicio de portador al nodo de soporte de datos en paquetes y la solicitud para un servicio de sesión a la función de aplicación están originadas en una única estación de usuario móvil.

Tal como se ha mencionado anteriormente, en particular la primera información relativa a la identidad de la estación de usuario móvil comprende una o varias de la MSISDN, la IMSI y la dirección IP de la estación de usuario móvil, y la segunda información relativa a la identidad de la estación de usuario móvil comprende la identidad privada IMS (IMPI) y/o la identidad pública IMS (IMPU), o la segunda información relativa a la identidad de usuario comprende la IMSI y/o la MSISDN, por ejemplo obtenidas a partir de la identidad privada o pública IMS (IMPI, IMPU), o la función de aplicación está adaptada para extraer dicha información de un HSS. En particular, el método comprende además las etapas de: establecer o encontrar la IMSI y/o la MSISDN de dichas primera y segunda informaciones relativas a la identidad de las estaciones de usuario móviles, comparar por lo menos parte de dichas primera y segunda informaciones relativas a la identidad de las estaciones de usuario móviles entre sí, y más específicamente comparar las direcciones IP de dichas primera y segunda informaciones relativas a la identidad de las estaciones de usuario móviles y/u obtener la IMSI y/o la MSISDN a partir de las identidades de usuario pública y/o privada IMS (IMPI/IMPU) recibidas, y/o construir, en el nodo de gestión de facturación y/o de políticas, una identidad de usuario privada utilizando la IMSI de la estación de usuario móvil, por ejemplo cuando no está implementada ninguna aplicación ISIM.

Ventajosamente, comprende asimismo la etapa de: identificar e instalar normas de facturación y/o de políticas aplicables, a la recepción de una solicitud procedente de un nodo de soporte de datos en paquetes. De manera más concreta, el método comprende además las etapas de: si la primera y la segunda informaciones relativas a la identidad de las estaciones de usuario móviles están originadas en una única estación de usuario móvil, implementar las normas de facturación y/o las normas de políticas proporcionadas, en el nodo de gestión de facturación y/o de políticas, de lo contrario, desechar el tráfico de flujo de IP relacionado; o seleccionar si mantener activas o desactivar las normas de facturación. En implementaciones preferidas, el nodo de soporte de datos en paquetes comprende un nodo que gestiona funciones en el plano de tráfico, y es un nodo independiente, o un GGSN o un CGSN o un nodo pasarela que gestiona la TPF y la ejecución de políticas (PEP), y el nodo de gestión de facturación y/o de políticas comprende una CRF, una PDF o un PCCN, o un nodo con una funcionalidad similar.

Breve descripción de los dibujos

A continuación se describirá en mayor medida la invención, de manera no limitativa, y haciendo referencia a los dibujos adjuntos, en los cuales:

la figura 1 muestra una solución del "estado de la técnica",

la figura 2 es un diagrama de bloques esquemático que muestra una disposición según la presente invención,

la figura 3 es un diagrama secuencial simplificado que muestra la disposición de la primera información relativa a la identidad de estación de usuario móvil a un nodo de gestión de facturación y/o de

políticas,

la figura 4 es un diagrama secuencial simplificado que incluye el procedimiento en el que se proporciona la segunda información relativa a la identidad de estación de usuario móvil al nodo de gestión de facturación y/o de políticas,

la figura 5 es un diagrama secuencial que muestra un procedimiento a modo de ejemplo, de la prestación de la segunda información relativa a la identidad de estación de usuario móvil y la verificación de la misma,

la figura 6A es un diagrama secuencial que describe una implementación a modo de ejemplo, y en el que el resultado de la verificación es positivo,

la figura 6B es un diagrama secuencial que describe la primera implementación a modo de ejemplo de la figura 6A, pero en el que el resultado de la verificación es negativo,

la figura 7 es un diagrama de bloques esquemático que muestra el concepto inventivo implementado en un diseño general,

la figura 8A muestra otro diseño general en el que puede ser implementado el concepto inventivo,

la figura 8B muestra otro diseño en el que puede ser implementado el concepto inventivo, y

la figura 9 es un diagrama de flujo que describe el procedimiento acorde con una realización de la presente invención.

Descripción detallada de la invención

La figura 1 muestra la solución del estado actual de la técnica, descrita anteriormente, en la aplicación para proporcionar seguridad para accesos IMS, en particular para implementaciones precoces de IMS no compatibles aún con los requisitos de 3GPP TS 33.203. Dicha solución se describe entre otras en el documento 3GPP TR 33.878. Se supone que un UE 10 solicita un portador al GGSN 10_0. Se establecen los contextos PDP de manera convencional, dependiendo principal o secundariamente de cuál sea el procedimiento relevante. El equipo de usuario UE 10 puede tener varias direcciones IP, una dirección IP por cada conexión de red IP. El GGSN comprende un temporizador de reposo 11_0 mediante cuya utilización puede reutilizarse una dirección IP para un usuario cuando se reestablece un contexto PDP en una etapa posterior. No existe APN (nombre de punto de acceso) de IMS específico y el GGSN no puede asumir la utilización de un contexto PDP de señalización. Conociendo de la manera convencional la MSISDN y la dirección IP del UE 10, el GGSN 10_0 envía la MSISDN y la dirección IP sobre la interfaz Gi hacia el servidor Radius 30_0, es decir se envían todas las direcciones IP y MSISDN del UE. El temporizador de reposo utilizado en el GGSN 10_0 está destinado aparentemente, principalmente a reducir la carga sobre el HSS. Se propone que esté trabajando del orden de horas, de manera que cuando no existe un contexto PDP disponible entre el GGSN y UE, el GGSN almacena o reserva la dirección IP asignada para un UE específico durante un período de tiempo que corresponde al tiempo establecido en el temporizador de reposo. Esto significa que el GGSN, tras la terminación de todos los portadores, no envía ninguna detención de solicitud de contabilización hasta que haya terminado realmente el temporizador de reposo. Este temporizador de reposo influye sobre cómo son asignadas o liberadas las direcciones IP hacia el UE.

El servidor Radius 30_0 transmite la información, es decir la MSISDN y la dirección IP, al HSS 40_0. Todas las direcciones IP del UE y la MSISDN se envían según el temporizador de reposo 11_0 en el GGSN 10_0, es decir, generalmente el envío se ralentizará, o retardará, hasta que expire el temporizador de reposo.

A continuación, se envía una solicitud de un registro SIP (SIP REGISTER) desde el UE 10 a la S-CSCF, y la S-CSCF envía la identidad IMS sobre el HSS 40_0. El HSS 40_0 devuelve una respuesta a la S-CSCF con la dirección IP registrada de vuelta a la S-CSCF 20_0. La S-CSCF 20_0 comprende un medio de verificación 21_0 o una funcionalidad para llevar a cabo una verificación mediante verificar que la dirección IP procedente del HSS 40_0 es la misma que la dirección IP almacenada en la S-CSCF. Si no son iguales, la sesión se finaliza debido a que se asume que se está produciendo un ataque.

Los inconvenientes de dicha solución se han descrito anteriormente en la solicitud.

La figura 2 muestra una disposición acorde con una implementación del concepto inventivo según el cual se utiliza un diseño FBC (facturación basada en flujo). El problema que se resuelve mediante la disposición consiste en la provisión de un mecanismo que asegura que la red está capacitada para verificar que la dirección IP de un equipo de usuario UE 1 y la identidad IMS del UE 1 en el servidor SIP corresponden al mismo usuario al nivel de portador. De acuerdo con la invención, los nodos involucrados o funciones son el GGSN 10 que gestiona la función para el plano de tráfico TPF, (según el concepto inventivo, ésta es la función para el plano de tráfico que se utiliza, y puede obtenerse como un nodo independiente, dispuesto en un GGSN o en un CGSN o en cualquier nodo que incluya por lo menos la funcionalidad TPF), un nodo 30 de gestión de facturación y/o de políticas que en esta realización está

implementada como una CRF (Charging Rules Functionality, funcionalidad de normas de facturación) y una función de aplicación AF 20 que puede estar implementada como una S-CSCF, una P-CSCF o similar, y el equipo de usuario UE 1 relacionado. La CRF 30 comprende medios de almacenamiento, por ejemplo, una tabla para almacenar la primera información relativa a la identidad del equipo de usuario tal como se explica a continuación, y medios de verificación 32 para verificar si por lo menos una parte dada de una primera información relativa a la identidad del UE corresponde a la segunda información relativa a la identidad del UE, por ejemplo, mediante comparar por lo menos partes de dichas primera y segunda informaciones relativas a la identidad, respectivamente. "Por lo menos parte de" significa que puede no ser necesario comparar toda la información en función de las implementaciones, tal como se describirá asimismo a continuación. Sin embargo, en la figura 2 se supone que el UE 1 envía una solicitud para un establecimiento de servicios de portador (I) a la TPF 10, que puede estar implementada en un GGSN. A continuación la TPF 10, por ejemplo una implementación basada en CRF, tal como en la figura 2, solicita normas de facturación (II) CRF 30. La primera información relativa a la identidad del UE acompaña la solicitud. La primera información relativa a la identidad del UE puede ser proporcionada por el UE o por la TPF 10 (por ejemplo, si se refiere a una solicitud de contexto PDP secundaria). Cómo se realice o consiga esto, no tiene importancia para el funcionamiento de la presente invención, siendo la cuestión principal que la primera información relativa a la identidad del UE esté disponible en la TPF 10. La primera información relativa a la identidad del UE que acompaña las normas solicitud de normas de facturación se almacena a continuación en la tabla 31 de la CRF 30, utilizando la CRF 30 entre otras la primera información relativa a la identidad del UE y posiblemente otra información, por ejemplo información de QoS acerca de la función de aplicación, etc., identifica cuáles son las normas de facturación pertinentes a instalar, y a continuación proporciona las normas de facturación a la TPF 10 (III). La TPF 10 lleva a cabo las acciones de las normas de facturación pertinentes o proporciona la implementación de las normas de facturación suministradas, y envía un mensaje de aceptación en relación con el establecimiento de la solicitud de servicio del portador (IV) al UE 1.

Una vez que se ha establecido un portador, el UE 1 envía una solicitud para una sesión de servicio utilizando SIP, (V) a la AF 20. En los sistemas GPRS, y desde el punto de vista de una FBC, la CFCS intermediaria y/o una CFCS de servicio y/o una CSCF de interrogación pueden, en función de la configuración del operador, actuar como una AF que maneja la interfaz Rx y/o la interfaz Gq. En la solicitud que utiliza el protocolo SIP, está incluida la segunda información relativa a la identidad de usuario, de la solicitud. La AF 20 envía a continuación información de facturación del flujo de la aplicación/del servicio, que incluye la segunda información relativa a la identidad del UE, a la CRF 30 (VI). Por ejemplo, si una S-CSCF actúa como una AF, puede, antes de proceder a una sesión de registro, transferir de manera no solicitada la identidad de usuario privada junto con la dirección IP del UE sobre Rx, hacia la CRF 30. En la activación del contexto PDP, la FBC asume que la dirección IP del UE y la IMSI (o MSISDN) se envían hacia la CRF 30 sobre la interfaz Gx. Basándose en las hipótesis anteriores, la CRF 30 está entonces en conocimiento de las IMSI procedentes tanto de la AF 20, en particular de la S-CSCF, como de la TPF 10, en particular del GGSN, y de las direcciones IP correspondientes y por lo tanto está capacitada, en el medio de verificación 32, para comprobar si las direcciones IP coinciden con, o están originadas en un único usuario (en la figura 1, de hecho ambas están originadas en el mismo UE, a saber el UE 1). Si no se corresponden, o no están originadas en un único usuario final, es decir, si no existe coincidencia entre las direcciones IP, la CRF 30 (en este caso, debería estar claro que para la gestión de políticas el nodo podría ser una PDF, pero puede ser asimismo un PCCN para gestionar políticas y/o facturación) notifica a la AF 20, en particular a la S-CSCF, a efectos de proporcionar una terminación de la sesión SIP, y la CRF 30 debería desactivar cualesquiera norma o normas correspondientes en la TPF 10.

Por supuesto, debería asimismo ser opcional si la sesión debe o no finalizarse, y opcionalmente esto puede ser controlado por el operador, de manera que bajo ciertas circunstancias, por ejemplo, un operador puede desear localizar o realizar el seguimiento del atacante y, por lo tanto, permitiría que continúe la sesión. También por otras razones, un operador puede permitir la sesión bajo ciertas condiciones, etc. La invención no se limita a la adopción de ningunas medidas particulares, sino que es fundamental que se proporcione una vigilancia en relación con la correspondencia entre direcciones y posibles ataques o similares.

La segunda información relativa a la identidad de usuario enviada desde la AF 20 a la CRF 30 puede contener, por ejemplo, la IMPI (identidad privada IMS), la IMPU (identidad pública IMS) y la dirección IP. Alternativamente, la AF 20 puede enviar la IMSI o la MSISDN directamente. Esto puede obtenerse a partir de la identidad privada o bien alternativamente a partir de la AF, por ejemplo, la S-CSCF puede contactar con el HSS para identificar la IMSI con la MSISDN.

Por ejemplo, si el UE no contiene un ISIM (pero sí, por ejemplo, un USIM) la IMPI se puede obtener y la identidad de usuario privada debería adoptar la forma de un NAI y deberá tener la forma de username@realm, tal como se especifica en IETF RFC 2486, cláusula 3.

Puede contenerse una representación de la IMSI dentro del NAI, para la identidad privada.

Si no existe una aplicación ISIM, la identidad de usuario privada no se conoce y puede entonces obtenerse de la IMSI. La identidad de usuario privada puede considerarse exterior a la IMSI mediante utilizar las cadenas completas de dígitos como parte del nombre de usuario de la identidad de usuario privada, y mediante transformar los dígitos principales de la IMSI, es decir MNC y MCC, en un nombre de dominio.

El resultado será una identidad de usuario privada, de la forma:

"<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org". Por ejemplo: si la IMSI es 234150999999999 (MCC=234, MNC=15), la identidad de usuario privada adoptará la forma 234150999999999@ims.mnc015.mcc234.3gppnetwork.org.

Por lo tanto, la CRF/PDF (PCCN) está capacitada, en base a la recepción de la IMPI, es decir, la identidad privada IMS, o incluso de la IMPU, la identidad de usuario pública, y de la dirección IP procedente de una AF, por ejemplo una CSCF tal como P-CSCF, S-CSCF, o I-CSCF, sobre Rx o Gq o Rx fusionadas con Gq, para obtener la IMSI (o la MSISDN) del UE. Debe observarse que una AF puede, alternativamente, enviar la MSISDN y/o la IMSI directamente sobre Rx/Gq, tal como se ha indicado anteriormente.

Además, dado que la TPF, en este caso la TPF implementada en un GGSN, deberá tener la capacidad de enviar la IMSI o la MSISDN a la CRF/PDF/PPCN (sobre Gx o Gx/Gy si están fusionadas), la CRF/PDF puede comparar las IMSI (o las MSISDN) procedentes de la CRF y de la TPF (en este caso, el GGSN) con las direcciones IP respectivas, es decir, la CRF 30 es capaz de encontrar la IMSI (MSISDN), en este caso, a partir del GGSN y la AF y comprueba si se trata de la misma dirección IP asociada. Si existe una coincidencia, la CRF implementa preferentemente, en este caso, normas de facturación tal como se especifica en el documento 3GPP TS 23.125. Por otra parte, si la dirección IP no está originada en un único UE, la CRF puede decir no implementar las normas de facturación, o desactivar normas de facturación ya implementadas, tal como se ha mencionado anteriormente, y por lo tanto puede desecharse el tráfico para el flujo IP afectado. La CRF informa a continuación a la AF, por ejemplo una P-CSCF/S-CSCF, de que no existe un contexto PDP disponible.

Alternativamente, en ciertas situaciones, mencionadas asimismo anteriormente, un operador puede desear permitir el tráfico, por ejemplo para rastrear a un atacante. Por lo tanto, puede existir una opción para que el nodo de gestión de facturación y/o de políticas 30 mantenga las normas en la TPF 10 activas, o para desactivarlas.

En algunas implementaciones, la TPF está implementada en un GGSN (o CGSN), pero, tal como se ha mencionado anteriormente, la TPF puede estar implementada en un nodo independiente o función, o asignada a cualquier otro elemento diferente a un GGSN/CGSN, siendo la cuestión principal que la función para el plano del tráfico TPF es la que está involucrada, de acuerdo con el concepto inventivo, dado que es la TPF la que hace funcionar la Gx hacía la CRF/PDF (o el PCCN) (o Gx/Gy cuando están fusionadas).

La invención funciona para identidades de usuario públicas de manera similar a como lo hace para identidades de usuario privadas. El documento GPP TS 23.003 especifica que cuando no se utiliza ISIM, la identidad de usuario pública temporal debería adoptar la forma de "user@domain", y por lo tanto debería ser igual a la identidad de usuario privada. Por lo tanto, es posible utilizar una identidad de usuario pública en lugar de la identidad privada en la capa SIP. Entonces la AF, por ejemplo la S-CSCF, puede solicitar, por ejemplo, una IMSI al HSS en base a la identidad de usuario pública, obtener la IMSI a partir de la identidad de usuario pública o enviar la identidad de usuario pública hacia la CRF/PDF/PCCN que obtiene la IMSI, o enviar una solicitud a un repositorio de perfiles de suscripción, si está implementado, ver la figura 5, para obtener la IMSI o la MSISDN.

La figura 3 es un diagrama secuencial esquemático que muestra la mensajería entre un UE, una TPF y, en este caso, una CRF. Debería estar claro que, tal como se ha mencionado anteriormente, la TPF puede disponerse como un nodo independiente, en un GGSN, en un CGSN o en cualquier otro nodo o medio de funcionamiento que proporcione por lo menos la funcionalidad TPF. Debería estar claro asimismo que, en lugar de que una CRF gestione normas de facturación, podría ser asimismo una PDF que gestione normas de políticas o un nodo combinado o funcionalidad que gestione, por ejemplo, políticas y facturación. Por lo tanto, se supone que el UE, de manera convencional, envía una solicitud para establecimiento de un servicio de portador, 1, por ejemplo, a un GGSN que proporciona la funcionalidad TPF. En una activación de contexto PDP, primera o principal, el GGSN, en este caso, enviará identidades de terminal, tales como una o varias de las dirección IP, la MSISDN y la IMSI hacia la CRF sobre la interfaz Gx en una solicitud de normas de facturación, 2, es decir, la primera información relativa a la identidad de equipo de usuario acompaña la solicitud de normas de facturación. La CRF almacena la primera información relativa a la identidad del UE recibida, 3, e identifica cuáles son las normas de facturación que son aplicables y deberían ser instaladas, 4. A continuación, se proporcionan las normas de facturación a la TPF, 5. La TPF, a la recepción de las normas de facturación, lleva a cabo la acción o acciones de las normas de facturación, 6, y envía al UE un mensaje de aceptación del establecimiento del servicio de portador, 7.

Debería resultar evidente que, tal como se mencionó anteriormente, la CRF puede estar fusionada con una PDF. De manera más específica, la CRF (y/o la PDF o el PCCN) puede estar fusionada con un sistema de facturación en línea OCS, en cuyo caso la Gx puede estar fusionada con la Gy. Estas interfaces están definidas en el documento TS 23.125, y, por ejemplo, en una realización pueden basarse ambas en control de crédito Diameter (Diameter Credit Control).

La figura 4 es un diagrama secuencial esquemático que muestra el procedimiento mediante el cual se proporciona a la CRF (por ejemplo) la segunda información relativa a la identidad del UE, de manera que puede llevarse a cabo una verificación según el concepto inventivo.

En este caso, se supone que cuando el UE envía una solicitud para una sesión de servicio utilizando el protocolo SIP, 8, a la AF que puede comprender, por ejemplo, una P-CSCF o una S-CSCF o una I-CSCF actuando como una AF, aquella incluye enviar identidades de usuario a la CRF sobre la Rx, lo que se describe el documento 3GPP TS 23.228, que se incorpora al presente documento como referencia. En otras palabras, el UE establece un registro SIP hacia la red IMS. Por lo tanto, cuando se envía una solicitud de sesión de servicio, registro SIP, 8, a la AF, la AF proporciona a la CRF información de facturación del flujo de datos de aplicación/servicio que incluye la segunda información relativa a la identidad del UE, por ejemplo, la IMPI, la IMPU, la dirección IP, 9. La CRF, habiendo almacenado la primera información relativa a la identidad del UE en un medio de almacenamiento, extrae dicha primera información relativa a la identidad del UE y la compara con la segunda información relativa a la identidad del UE recibida de la AF, 10. En este caso, se supone que la primera y la segunda informaciones relativas a la identidad del UE se originan respectivamente en un único UE, y por lo tanto se envía un acuse de recibo, 11, a la AF y el servicio se establece implementando las normas de facturación pertinentes, o similares.

Debería estar claro que la interfaz Rx puede estar fusionada con Gq, y la AF puede funcionar por lo tanto sobre Rx/Gq. En realizaciones particulares, Rx y Gq pueden estar ambas basadas en Diameter Nasreq.

Debería resultar evidente que, como una alternativa para enviar la IMPI y la IMPU, es decir, la identidad privada y la pública del IMS, respectivamente, tal como se describe en los documentos TS 23.228 y TS 23.003, la AF, o cualquier CSCF, pueden enviar la IMSI o la MSISDN directamente a la CRF. La IMSI o la MSISDN se pueden obtener a partir de la identidad privada, o puede ser necesaria una comunicación con el HSS para la identificación de la IMSI o la MSISDN. Esto se ha descrito anteriormente haciendo referencia a la figura 2.

La CRF comprende particularmente una tabla de traducción entre la IMPI y la IMSI.

La figura 5 es un diagrama secuencial que muestra el procedimiento en el que se proporciona la segunda información relativa a la identidad del UE, por ejemplo, a una CRF o a un PCCN, etc., donde, en este caso, se realiza una verificación satisfactoria. En este caso, se supone que se establece un contexto PDP, y que la primera información relativa a la identidad del UE está disponible en la CRF, el PCCN, etc. Se supone que el UE está en una red visitada y envía un registro SIP, 80, con la ID de usuario pública, la ID de usuario privada y la dirección IP del UE a la P-CSCF. El registro SIP se envía desde la P-CSCF a la I-CSCF de la red propia del UE, 81. La I-CSCF envía un mensaje Cx-Query/Cx-Select-Pull Diameter (en esta realización particular), 82, al HSS, que devuelve la respuesta correspondiente, 83, relativa a identidades IMS. A continuación, el registro SIP con la ID de usuario pública, la ID de usuario privada, la dirección IP del UE, se envía desde la I-CSCF a la S-CSCF, 84. En esta realización específica, se supone que la S-CSCF actúa como una AF. En realizaciones alternativas, una P-CSCF o una I-CSCF pueden actuar como una AF. Deberá estar claro que en este caso, la TPF y el repositorio de información de suscripciones no son visibles.

Las etapas 85, 86 se refieren a la disposición de parámetros de seguridad, dirección IP de aplicación, etc., lo cual, no obstante, no tiene relevancia para el concepto inventivo.

A continuación, se supone que la segunda información relativa a la identidad del UE, la ID de usuario pública, la ID de usuario privada, y la dirección IP del UE se proporcionan a la CRF (PCCN, etc.), 87, y después de la verificación (que, en este caso, se supone afirmativa) con la primera información relativa a la identidad del UE (que no se muestra en este caso), se envía un acuse de recibo a la S-CSCF, 88. La S-CSCF envía un mensaje de verificación positivo 2XX OK a la I-CSCF, 89, la cual lo transfiere a la P-CSCF, 90, la cual a su vez lo transfiere al UE, 91.

La figura 6A muestra un ejemplo de la implementación en la que se supone que la primera y la segunda informaciones relativas a la identidad del UE pueden ser verificadas positivamente (es decir, existe correspondencia) y en la que se utiliza el protocolo Diameter.

Por lo tanto, el primer UE envía (en este caso) una solicitud de activar contexto PDP (en este caso) a un SGSN, 1_1. De la manera convencional, el SGSN envía una solicitud de crear contexto PDP al GGSN, 2_1, que en este caso utiliza un cliente Radius para obtener direcciones IP de UEs.

En esta realización, se supone que se utiliza el protocolo Diameter (ver el documento 3GPP TS 29.210), y el GGSN envía una solicitud de normas, en este caso una Diameter CCR (Credit Control Request, solicitud de control de crédito) con IMSI, MSISDN, dirección IP, sobre Gx a la CRF (o al PCCN, etc.), 3_1. La CRF responde con una Diameter CCA (Credit Control Answer, respuesta de control de crédito) con normas de facturación sobre la Gx, 4_1, al GGSN, el cual envía una respuesta de crear contexto PDP al SGSN, 5_1. El SGSN envía aceptar activar contexto PDP al UE 6_1, con la dirección PDP (dirección IP) asignada. Tal como se ha descrito anteriormente, se supone que el UE envía un registro SIP al GGSN, 7_1, el cual comprueba si hay suplantación de dirección IP (es decir, comprueba que el UE no ha cambiado la dirección IP que se le ha proporcionado, es decir, que no utiliza otra diferente). Cuando se comprueba que el UE utiliza la dirección IP "correcta", se envía un registro SIP a la P-CSCF, 8_1, que lo envía a la I-CSCF, 9_1. A continuación, la I-CSCF envía el registro SIP a la C-CSCF (que, en este caso, actúa como AF), 10_1.

En esta realización, se supone que la S-CSCF envía un mensaje Diameter (aplicación Nasreg) AAR a la CRF, 11_1, sobre la Rx y que contiene la ID de usuario pública del UE, y la ID de usuario privada y la dirección IP del UE. La CRF mapea la identidad de usuario pública y/o privada a la MSISDN y/o a la IMSI para recuperar la dirección IP

asociada. A continuación, la CRF lleva a cabo la verificación, es decir comprueba si la información recibida desde el GGSN (ver la etapa 31) es la misma, y acusa recibo de que la verificación ha sido (en este caso) satisfactoria sobre Rx a la S-CSCF en una respuesta AAA, 12_1.

Finalmente, se envía un mensaje SIP 2XX OK desde la S-CSCF al UE, 13_1.

La figura 6B es similar a la figura 6A con la diferencia de que el mapeo en la CRF no es satisfactorio. Por lo tanto las etapas 1_1-1_{11} son similares a las etapas 1_1-1_{11} de la figura 6A, y por ello mantienen los mismos numerales de referencia.

Tras establecerse en la CRF que el mapeo no es satisfactorio, es decir, que la primera y la segunda informaciones relativas a la identidad de UE no son iguales, se envía un mensaje de error sobre la Rx (Diameter) a la S-CSCF, 12_2. Finalmente, la CRF puede enviar a continuación un mensaje Diameter CCA sobre la Gx al GGSN, 13_2, indicando que las normas de facturación pertinentes deberían eliminarse. El GGSN confirma a continuación a la CRF la eliminación, 14_2 y (en cualquier caso, independientemente de si se implementan o no las etapas 13_2, 14_2) se envía un mensaje de error desde la S-CSCF o UE, por ejemplo, un SIP 4XX Forbidden, 15_2.

Debería resultar evidente que el concepto inventivo no se limita la utilización de Diameter. Puede utilizarse asimismo Radius o cualquier otro protocolo adecuado. Tal como se ha mencionado anteriormente, el flujo será asimismo diferente si se utiliza un CGGN, en lugar de un GGSN y un SGSN lo cual, no obstante, no se muestra explícitamente dado que en las variaciones serían obvias.

Tal como se ha mencionado también anteriormente, no tienen por qué actuar la S-CSCF como una AF, y en lugar de la CRF puede ser, por ejemplo, un PDF, PCCN, etc.

La figura 7 muestra una realización particular en la que el nodo de gestión de facturación y/o de políticas comprende un PCCN 30A (nodo de control de políticas y facturación). El PCCN 30A comunica con el control 36A de crédito basado en flujo de datos de servicio o, de forma más general, con el OCS. Si, por ejemplo, el PCCN 30A recibe una identidad IMS, por ejemplo la IMPI, desde una AF (no mostrada), éste puede solicitar la IMSI al repositorio de perfiles de suscripción 35 sobre el punto de referencia Sp (o, en particular, la interfaz Sp). De manera más general, si el PCCN 30A recibe una identidad IMS, puede consultar el repositorio de perfiles de suscripción 35 a efectos de obtener una conexión entre la identidad IMS (IMPI o IMPU) y la MSISDN o la IMSI recibida de la TPF, por ejemplo, en el GGSN. Esto es ventajoso porque cubre asimismo casos en que los usuarios utilizan un ISIM que puede tener otra estructura para la IMPI, que por ejemplo no esté basada en la IMSI o la MSISDN. En otra realización (no mostrada) el PCCN (o la PDF 33A o la CRF 34A en el PCCN, como alternativa a un PCCN), puede solicitar el control de crédito 36A basado en flujo de datos de servicio, a efectos de obtener una conexión entre la identidad IMS y la MSISDN/IMSI recibida desde la TPF.

La figura 8A muestra esquemáticamente otra arquitectura en la que es aplicable el concepto inventivo. Dicho diseño se da a conocer, por ejemplo, en el documento TR 23.803. En este caso, el nodo de gestión de facturación y/o de políticas comprende un PCCN 30B con una PDF 33B y una CRF 34B en comunicación con una AF 20B sobre una interfaz Rx/Gq fusionada. En este caso, el nodo de soporte de datos en paquetes que incluye la funcionalidad TPF 11 comprende una pasarela 10B que, además de la funcionalidad TPF 11, incluye asimismo una funcionalidad PEP (Policy Enforcement Point, punto de ejecución de políticas), 12. La comunicación entre el PCCN 30B y la pasarela GW 10B tiene lugar sobre la interfaz fusionada Go/Gx. El PCCN 30B comunica con el OCS (Online Charging System, sistema de facturación en línea) 36B con un Camel SCP 37B y con medios 38B de control de crédito basados en flujo de datos de servicio, sobre la interfaz Ry. La GW 10B comunica con el OSC 36B sobre la interfaz Gy. La GW 10B comunica asimismo con una función $15B_1$ de pasarela de facturación y una función $15B_2$ de cobro de facturación, sobre la interfaz Gz.

La figura 8B muestra otra realización similar a la de la figura 8A, pero con la diferencia de que el OSC y la PCCN están fusionados en un nodo 30C, que comunica con la GW 10C sobre una interfaz fusionada que comprende las interfaces Gy/Go/Gx fusionadas entre ellas. En otros aspectos, la figura 8B es similar a la figura 8A y el OCS/PCCN 30C comunica sobre una interfaz fusionada Gq/Rx con la AF 20C, y la GW 10C comunica sobre la Gz con la función $15C_1$ de pasarela de facturación y la función $15C_2$ de cobro de facturación.

Debería estar claro que estas figuras se muestran solamente para presentar algunos ejemplos adicionales sobre diseños en los que puede aplicarse el concepto inventivo.

Por lo tanto, según la invención, mediante solamente una leve adición a los diseños FBC existentes o similares, puede proporcionarse seguridad para IMS precoz. Los operadores que utilizan FBC para servicios no basados en IMS que migran a IMS reciben la oportunidad de simplemente actualizar la FBC en lugar de HSS y un servidor Radius, lo cual es muy ventajoso. El concepto inventivo no implica limitaciones, por ejemplo, sobre un diseño GGSN, por ejemplo asignación o liberación de direcciones IP, tal como es el caso con la propuesta proporcionada en el documento TR 33.878, y tampoco existe la necesidad de introducir un temporizador de reposo en el GGSN. Según la invención, las identidades del IMS pueden estar en conexión, por ejemplo, con identidades basadas en GPRS mediante la utilización de las interfaces Rx y Gx.

La figura 9 es un diagrama de flujo que describe una implementación del concepto inventivo. En este caso, se supone que un UE solicita a la TPF un establecimiento de servicio de portador, 100. En la solicitud, el UE incluye la primera información relativa a la identidad del UE, o si se trata de una solicitud de contexto PDP secundario, la primera información relativa a la identidad del UE está ya almacenada en el nodo que gestiona la TPF. No obstante, esto es conocido en la técnica.

La TPF envía a continuación una solicitud de normas de facturación y/o de políticas a la CRF o la PDF, o a un PCCN, en función de la implementación aplicable, que incluye dicha primera información relativa a la identidad del UE, 101. La CRF/PDF (o el PCCN) almacena la primera información relativa a la identidad del UE en medios de almacenamiento, por ejemplo una tabla, 102. A continuación, la CRF/PDF (o el PCCN) identifica e instala, utilizando dicha primera información relativa a la identidad del UE y posiblemente otra información tal como se ha mencionado anteriormente, las normas pertinentes de facturación y/o de políticas, 103. A continuación la CRF/PDF (o el PCCN) proporciona las normas de facturación y/o de políticas a la TPF, 104. A continuación se envía un mensaje de aceptación de establecimiento de servicio de portador desde la TPF al UE, 105. Una vez que se ha establecido un servicio de portador, se supone que el UE envía un mensaje SIP o una solicitud SIP, por ejemplo una invitación SIP, a una función de aplicación AF, 106. A continuación, puede comprobarse si la identidad de usuario privada se conoce a partir del mensaje SIP, 107. Si no, ésta puede obtenerse de alguna manera en la AF o bien en comunicación con algún otro nodo o función, tal como se ha descrito anteriormente, 107A. A continuación, así como si la identidad de usuario privada se conocía de hecho a partir del mensaje SIP o de la solicitud SIP, se envía la segunda información relativa a la identidad del UE a la CRF/PDF o al PCCN, 108. De esta manera, en la CRF/PDF o el PCCN se examina a continuación si la primera información relativa a la identidad del UE y la segunda información relativa a la identidad del UE se han originado en un único UE, 109. Si no, se comprueba si las normas de gestión de facturación y/o de políticas han de ser desactivadas, 109A, y si es así, se desactivan y/o se desecha el tráfico pertinente, 109B. Sin embargo, si en la etapa 109A se selecciona la opción de que las normas no han de ser desactivadas, así como si la primera y la segunda informaciones relativas a la identidad del UE están originadas respectivamente en un único UE, se implementan las normas de facturación y/o de políticas, 110.

Debería resultar evidente que la invención no se limita a las realizaciones mostradas específicamente, sino que puede variarse de muchas formas dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Una disposición en un sistema de comunicaciones que participa en procedimientos de solicitud de y/o de acceso a servicios de estación de usuario, y que comprende una serie de nodos de soporte de datos en paquetes (GGSN; CGSN; TPF; 10; 10B; 10C), una serie de nodos de gestión de facturación y/o de políticas (CRF; TPF; PCCN; 30; 30A; 30B; 30C) y una serie de funciones de aplicación (AF; P, S, ICSCF; 20; 20B; 20C) que administran la gestión de movilidad y el control de llamadas de estaciones de usuario móviles (UE; 1) que solicitan y/o acceden a servicios,

caracterizada

por que el nodo o nodos de soporte de datos en paquetes (10; 10B; 10C) comprenden medios adoptados para enviar una primera información relativa a la identidad de la estación de usuario móvil (UE; 1) sobre una primera interfaz (Gx, Gy; Gx/Gy) a un nodo de gestión de facturación y/o de políticas (CRF; PDF; PCCN; 30; 30A; 30B; 30C), a la recepción de una solicitud de servicios de portador procedente de una estación de usuario móvil (UE; 1)

por que la función o funciones de aplicación (AF; P, S, ICSCF; 20; 20B; 20C) comprenden medios para, a la recepción de una solicitud de una sesión de servicio SIP procedente de una estación de usuario móvil (UE; 1), enviar una segunda información relativa a la identidad de la estación de usuario móvil al nodo de gestión de facturación y/o de políticas (CRF; PDF; PCCN; 30; 30A; 30B; 30C), sobre una segunda interfaz (Rx, Rx/Gq),

y **por que** el nodo (CRF; PDF; PCCN; 30; 30A; 30B; 30C) de gestión de políticas y/o de facturación comprende medios de verificación (32, 32A) adaptados para determinar si la solicitud de un servicio de portador al nodo de soporte de datos en paquetes (10; 10B; 10C) y la solicitud de un servicio de sesión a la función de aplicación (AF; P/S/I-CSCF; 20; 20B; 20C) están originadas en una única estación de usuario móvil (UE; 1).

2. Una disposición según la reivindicación 1,

caracterizada

por que la primera información relativa a la identidad de la estación de usuario móvil comprende una o varias de la MSISDN, la IMSI y la dirección IP de la estación de usuario móvil (UE; 1).

3. Una disposición según la reivindicación 1 ó 2,

caracterizada

por que la segunda información relativa a la identidad de la estación de usuario móvil comprende la identidad privada IMS (IMPI) y/o la identidad pública IMS (IMPU).

4. Una disposición según la reivindicación 1 ó 2,

caracterizada

por que la segunda información relativa a la identidad de la estación de usuario móvil comprende la IMSI y/o la MSISDN, por ejemplo, obtenida a partir de la identidad privada o pública IMS (IMPI, IMPU), o **por que** la función de aplicación (20; 20B; 20C) está adaptada para extraer dicha información externamente, por ejemplo, de un HSS.

5. Una disposición según cualquiera de las reivindicaciones anteriores,

caracterizada

por que las direcciones IP se reciben, o se obtienen a partir de la primera información relativa a la estación de usuario móvil y de la segunda información relativa a la identidad de la estación de usuario móvil, y **por que** los medios de verificación (32, 32A) están adaptados para comparar la dirección IP obtenida a partir de la función de aplicación (20; 20B; 20C) con la dirección IP obtenida a partir del nodo de soporte de datos en paquetes.

6. Una disposición según la reivindicación 4,

caracterizada

por que el nodo de gestión de facturación y/o de políticas (30; 30A; 30B; 30C) está adaptado para deducir la IMSI y/o la MSISDN a partir de la identidad de usuario privada y/o pública IMS (IMPI/IMPU).

7. Una disposición según cualquiera de las reivindicaciones anteriores,

caracterizada

por que el nodo de gestión de facturación y/o de políticas (30; 30A; 30B; 30C) está adaptado para identificar e instalar normas de facturación a aplicar a la recepción de la solicitud de las mismas desde un nodo de soporte de datos en paquetes (10; 10B; $15B_1$, $15B_2$; 10C).

8. Un usuario según cualquiera de las reivindicaciones anteriores,

caracterizado

por que el nodo de soporte de datos en paquetes comprende un GGSN (10) o un CGSN que gestiona opciones para el plano de tráfico.

9. Una disposición según cualquiera de las reivindicaciones anteriores,

caracterizada

por que el nodo de soporte de datos en paquetes comprende un nodo independiente o un nodo de pasarela (10B; 10C) que gestiona funciones para el plano de tráfico, o funciones para el plano de tráfico y ejecución de políticas (PEP).

10. Una disposición según cualquiera de las reivindicaciones anteriores,

caracterizada

por que la segunda interfaz comprende Rx o Rx fusionadas con Gq.

11. Un nodo de gestión de facturación y/o de políticas (30; 30A; 30B; 30C) en un sistema de comunicaciones que soporta comunicación de datos en paquetes y está dispuesto para comunicar con una función de aplicación (20; 20B; 20C) y un nodo de soporte de datos en paquetes (10; 10B; 10C),

caracterizado

por que está adaptado para recibir una primera información relativa a la identidad de la estación de usuario móvil procedente del nodo de soporte de datos en paquetes (10; 10B; 10C) a la recepción de una solicitud de un servicio de portador procedente de una estación de usuario móvil (UE; 1) en el nodo de soporte de datos en paquetes (10; 10B; 10C), para recibir una segunda información relativa a la identidad de la estación de usuario móvil procedente de la función de aplicación a la recepción de una solicitud de una sesión de servicio en la misma, y **por que** comprende medios de verificación (32, 32A) para determinar si la solicitud de un servicio de portador al nodo de soporte de datos en paquetes (10; 10B; 10C) y la solicitud de un servicio de sesión a la función de aplicación (20; 20B; 20C) están originadas en una única estación de usuario móvil (UE; 1).

12. Un nodo de gestión de facturación y/o de políticas según la reivindicación 11,

caracterizado

por que la primera información relativa a la identidad de la estación de usuario móvil comprende uno o varios de la MSISDN, la IMSI y la dirección IP de la estación de usuario móvil.

13. Un nodo de gestión de facturación y/o de políticas según cualquiera de las reivindicaciones 11 a 12,

caracterizado

por que los medios de verificación (32, 32A) están adaptados para comparar la dirección IP correspondiente a, o incluida en la primera información relativa a la identidad de la estación de usuario móvil, y la dirección IP correspondiente a, o incluida en la segunda información relativa a la identidad de la estación de usuario móvil.

14. Un nodo de gestión de facturación y/o de políticas según cualquiera de las reivindicaciones 11 a 13,

caracterizado

por que está adaptado para identificar e instalar normas de facturación a aplicar, a la recepción de una solicitud de las mismas desde un nodo de soporte de datos en paquetes (10; 10B; 10C), y si la primera y la segunda informaciones relativas a la identidad de usuarios están originadas en una única estación de usuario móvil (1), está adaptado para implementar las normas de facturación proporcionadas, y si la primera y la segunda informaciones relativas a la identidad de usuario no están originadas en una única estación de usuario móvil,

está adaptado para rechazar las normas de facturación y/o para desactivar normas de facturación implementadas y desechar el tráfico de flujo IP correspondiente, informar a la función de aplicación (20; 20B; 20C) de que no está disponible un contexto PDP, o seleccionar si desactivar las normas de facturación en el nodo de soporte de datos en paquetes (10; 10B; 10C) o mantenerlas activas.

15. Un método de control de acceso a servicios, en un sistema de comunicación que soporta comunicación de datos en paquetes y comprende una serie de nodos de datos en paquetes, una serie de nodos de gestión de facturación y/o de políticas y una serie de funciones de aplicación que administran gestión de movilidad y control de llamadas de servicios de solicitud/acceso de estaciones de usuario móviles, que comprende las etapas de:

- recibir una solicitud de servicios de portador desde una estación de usuario móvil en un nodo de soporte de datos en paquetes,

- enviar, desde el nodo de soporte de datos en paquetes, una primera información relativa a la identidad de estación de usuario móvil, de la estación de usuario móvil, a un nodo de gestión de facturación y/o de políticas,

- recibir, a continuación, antes o sustancialmente al mismo tiempo, una solicitud de una sesión de servicio procedente de la estación de usuario móvil en una función de aplicación,

- enviar, desde la función de aplicación, una segunda información relativa a la identidad de la estación de usuario móvil al nodo de gestión de facturación y/o de políticas,

- establecer, en el nodo de gestión de facturación y/o de políticas, si la solicitud de un servicio de portador al nodo de soporte de datos en paquetes y la solicitud de una sesión de servicio a la función de aplicación se originan en una única estación de usuario móvil.

16. Un método según la reivindicación 15,

en el que la primera información relativa a la identidad de la estación de usuario móvil comprende una o varias de la MSISDN, la IMSI y la dirección IP de la estación de usuario móvil, y en el que la segunda información relativa a la identidad de la estación de usuario móvil comprende la identidad privada IMS (IMPI) y/o la identidad pública IMS (IMPU), o la segunda información relativa a la identidad de usuario comprende la IMSI y/o la MSISDN, por ejemplo obtenidas a partir de la identidad privada o pública IMS (IMPI, IMPU), o la función de aplicación está adaptada para extraer dicha información de un HSS.

17. Un método según la reivindicación 15 ó 16,

que comprende además las etapas de:

- establecer o encontrar la IMSI y/o la MSISDN de dichas primera y segunda informaciones relativas a la identidad de la estación de usuario móvil,

- comparar entre sí por lo menos parte de dichas primera y segunda informaciones relativas a la identidad de la estación de usuario móvil.

18. Un método según la reivindicación 15, 16 ó 17,

que comprende la etapa de:

- comparar las direcciones IP de dichas primera y segunda informaciones relativas a la identidad de la estación de usuario móvil.

19. Un método según cualquiera de las reivindicaciones 15 a 18,

que comprende la etapa de:

- obtener la IMSI y/o la MSISDN a partir de identidades de usuario públicas y/o privadas IMS (IMPI/IMPU) recibidas.

20. Un método según cualquiera de las reivindicaciones 15 a 19,

que comprende la etapa de:

- construir, en el nodo de gestión de facturación y/o de políticas, una identidad de usuario privada utilizando la IMSI de la estación de usuario móvil.

21. Un método según cualquiera de las reivindicaciones 15 a 20

que comprende la etapa de:

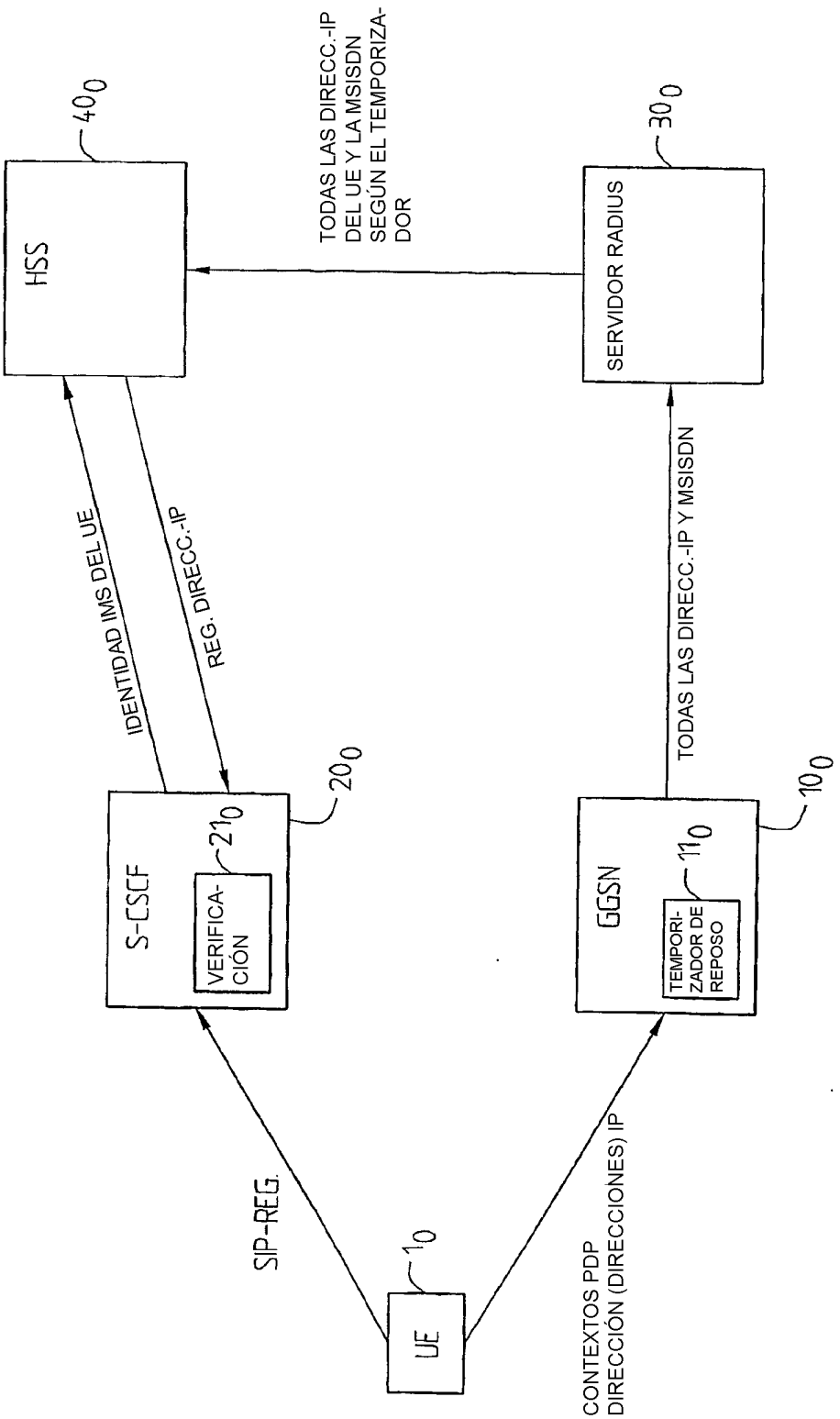
- identificar e instalar normas aplicables de facturación y/o de políticas, a la recepción de una solicitud procedente de un nodo de soporte de datos en paquetes,

- si la primera y la segunda informaciones relativas a la identidad de la estación de usuario móvil se originan en una única estación de usuario móvil,

- implementar las normas de facturación y/o de políticas proporcionadas aplicables, en el nodo de gestión de facturación y/o de políticas, o bien,

- desechar el tráfico de flujo IP correspondiente, o

- seleccionar si activar o desactivar las normas de facturación.



ESTADO DE LA TÉCNICA

Fig. 1

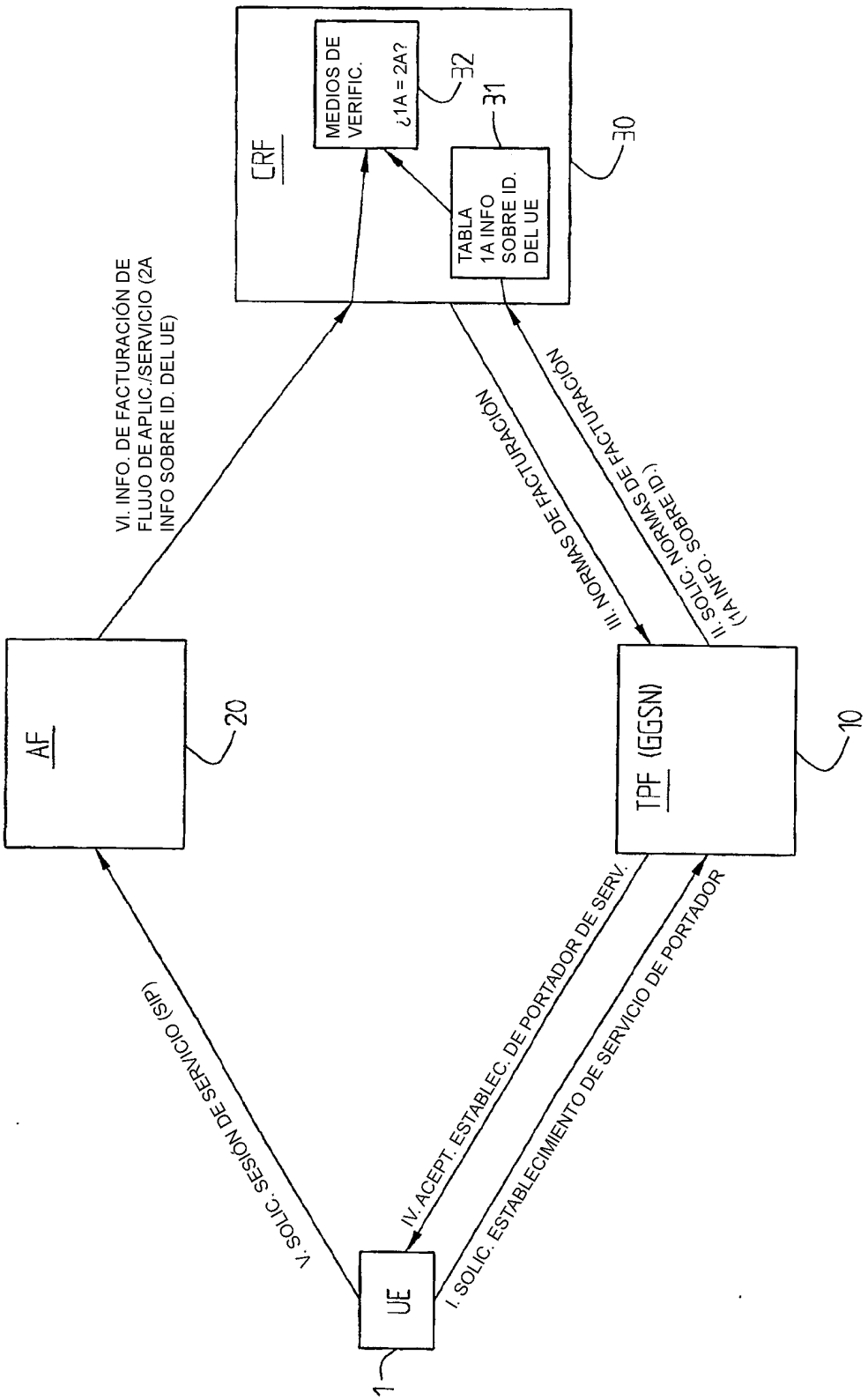

CRF
MEDIOS DE VERIFIC.
¿1A = 2A?
32
31
TABLA 1A INFO SOBRE ID. DEL UE
30
VI. INFO. DE FACTURACIÓN DE FLUJO DE APLIC./SERVICIO (2A INFO SOBRE ID. DEL UE)
III. NORMAS DE FACTURACIÓN
II. SOLIC. NORMAS DE FACTURACIÓN (1A INFO SOBRE ID.)
AF
20
TPF (GGSN)
10
V. SOLIC. SESIÓN DE SERVICIO (SIP)
IV. ACEPT. ESTABLEC. DE PORTADOR DE SERV.
I. SOLIC. ESTABLECIMIENTO DE SERVICIO DE PORTADOR
UE
1

Fig. 2

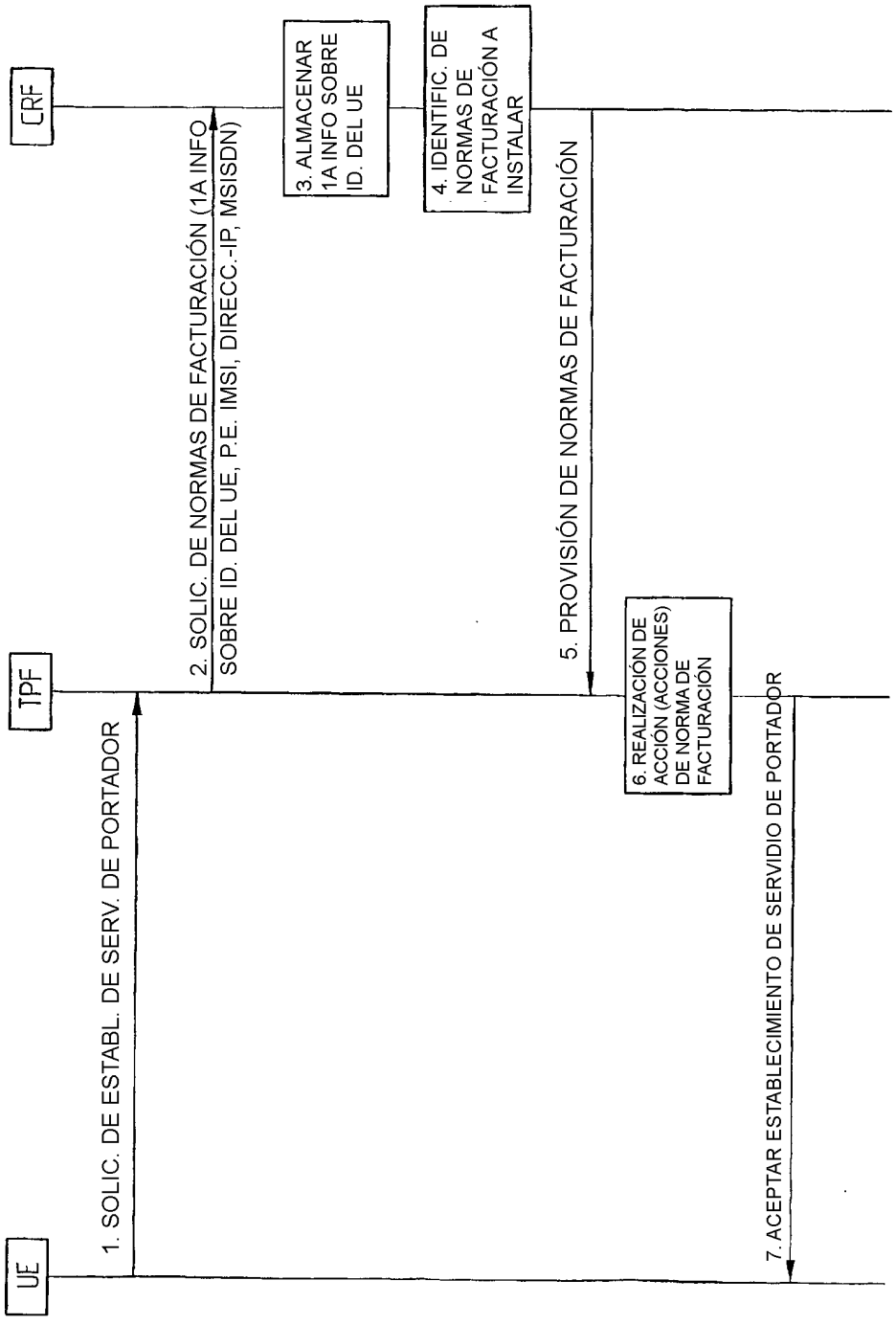

UE
TPF
CRF
1. SOLIC. DE ESTABL. DE SERV. DE PORTADOR
2. SOLIC. DE NORMAS DE FACTURACIÓN (1A INFO SOBRE ID. DEL UE, P.E. IMSI, DIRECC.-IP, MSISDN)
3. ALMACENAR 1A INFO SOBRE ID. DEL UE
4. IDENTIFIC. DE NORMAS DE FACTURACIÓN A INSTALAR
5. PROVISIÓN DE NORMAS DE FACTURACIÓN
6. REALIZACIÓN DE ACCIÓN (ACCIONES) DE NORMA DE FACTURACIÓN
7. ACEPTAR ESTABLECIMIENTO DE SERVIDIO DE PORTADOR

Fig. 3

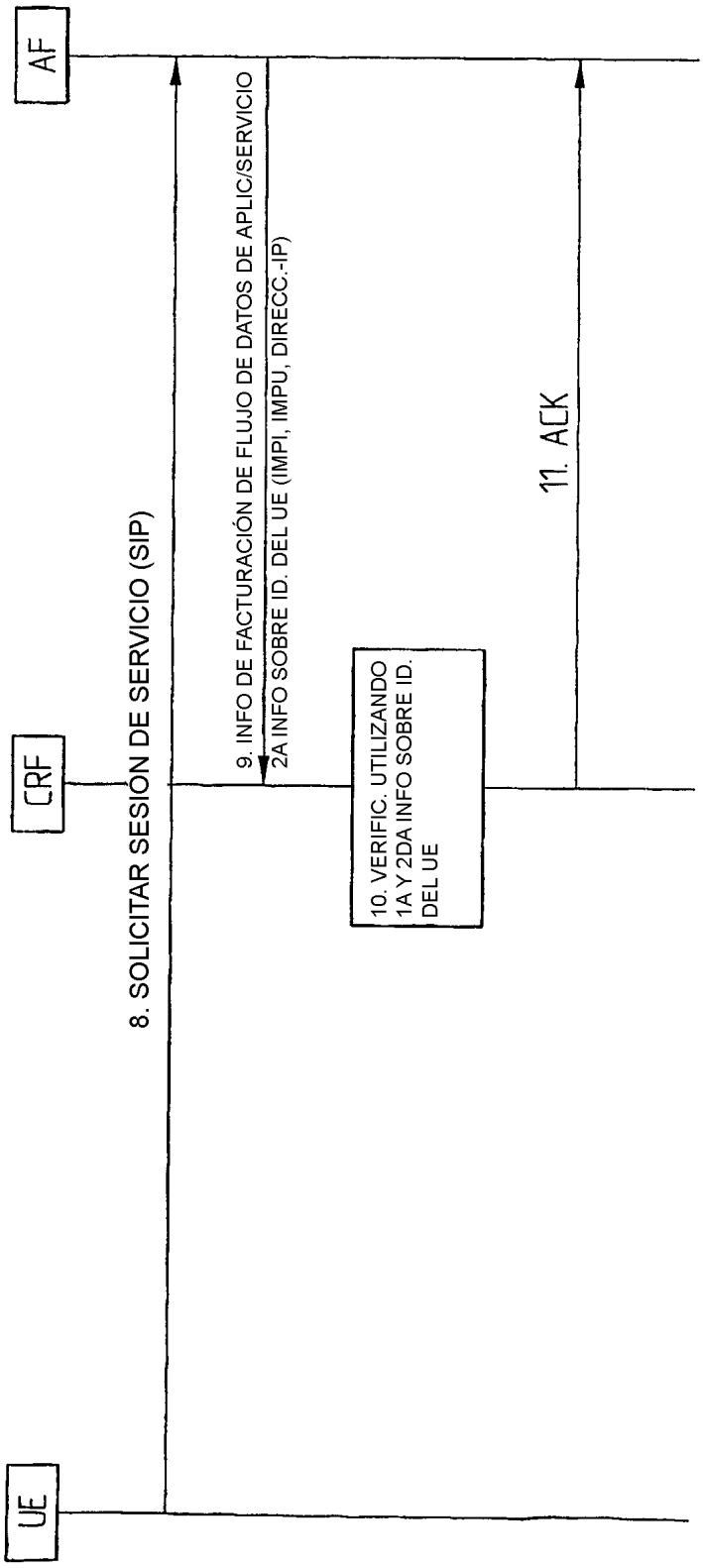

AF
CRF
UE
8. SOLICITAR SESIÓN DE SERVICIO (SIP)
9. INFO DE FACTURACIÓN DE FLUJO DE DATOS DE APLIC/SERVICIO
2A INFO SOBRE ID. DEL UE (IMPI, IMPU, DIRECC.-IP)
10. VERIFIC. UTILIZANDO 1A Y 2DA INFO SOBRE ID. DEL UE
11. ACK

Fig. 4

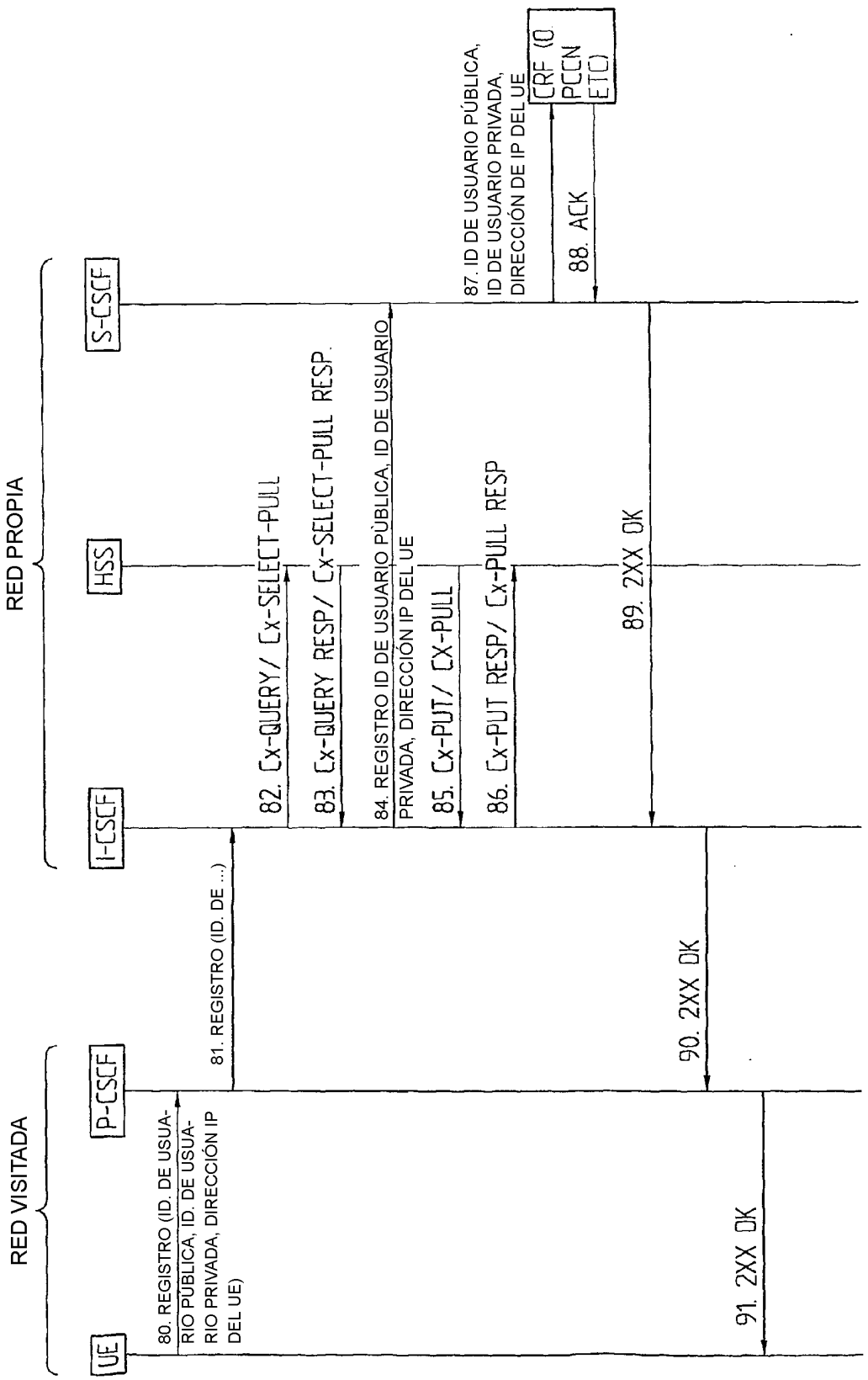

RED VISITADA
RED PROPIA
UE
P-CSCF
I-CSCF
HSS
S-CSCF
80. REGISTRO (ID. DE USUARIO PÚBLICA, ID. DE USUARIO PRIVADA, DIRECCIÓN IP DEL UE)
81. REGISTRO (ID. DE ...)
82. Cx-QUERY/ Cx-SELECT-PULL
83. Cx-QUERY RESP/ Cx-SELECT-PULL RESP
84. REGISTRO ID DE USUARIO PÚBLICA, ID DE USUARIO PRIVADA, DIRECCIÓN IP DEL UE
85. Cx-PUT/ CX-PULL
86. Cx-PUT RESP/ Cx-PULL RESP
87. ID DE USUARIO PÚBLICA, ID DE USUARIO PRIVADA, DIRECCIÓN DE IP DEL UE
CRF (O PCCN ETC)
88. ACK
89. 2XX OK
90. 2XX OK
91. 2XX OK

Fig. 5

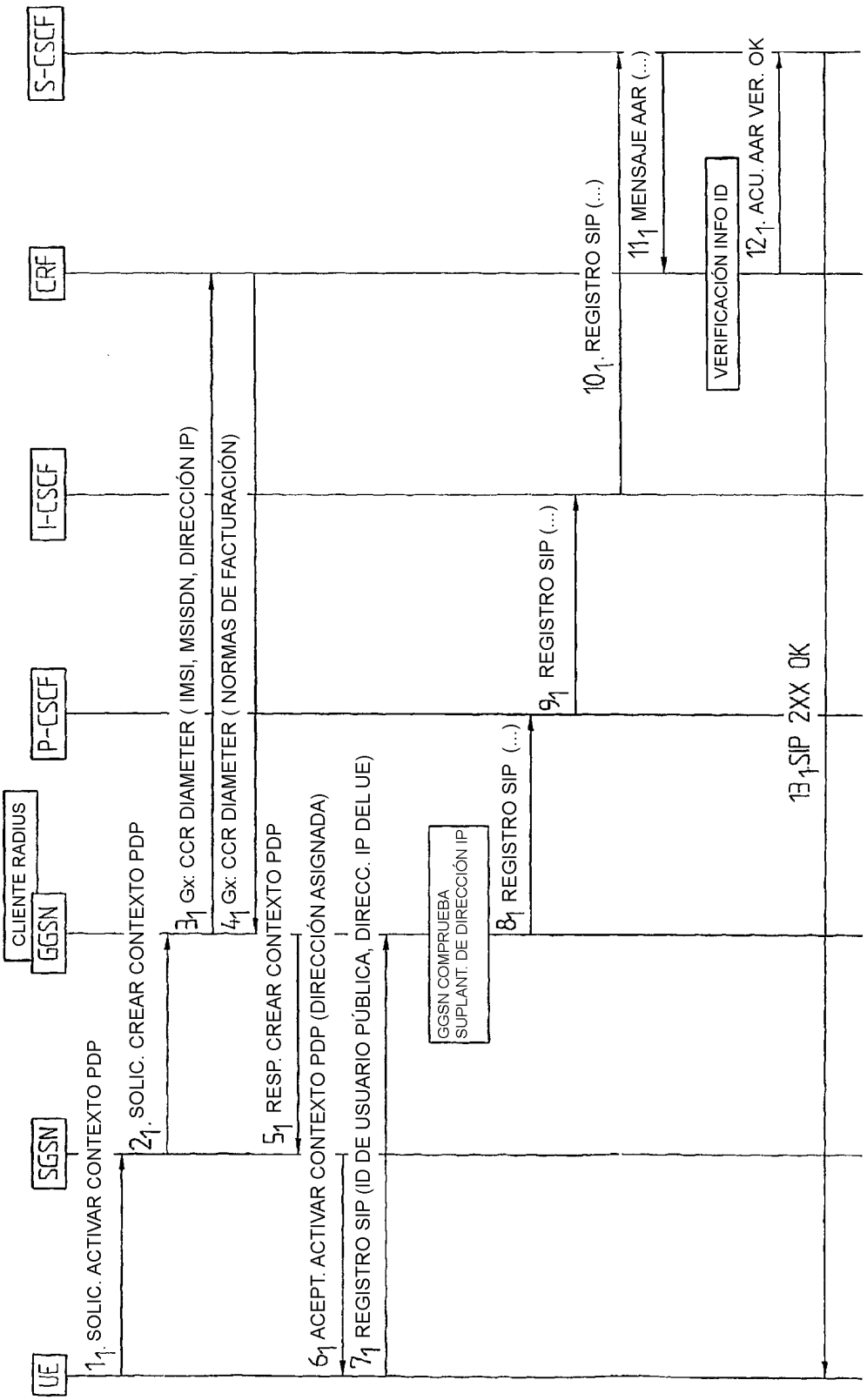

UE
SGSN
CLIENTE RADIUS
GGSN
P-CSCF
I-CSCF
CRF
S-CSCF
1. SOLIC. ACTIVAR CONTEXTO PDP
2. SOLIC. CREAR CONTEXTO PDP
3 Gx: CCR DIAMETER (IMSI, MSISDN, DIRECCIÓN IP)
4 Gx: CCR DIAMETER (NORMAS DE FACTURACIÓN)
5 RESP. CREAR CONTEXTO PDP
6 ACEPT. ACTIVAR CONTEXTO PDP (DIRECCIÓN ASIGNADA)
7 REGISTRO SIP (ID DE USUARIO PÚBLICA, DIRECC. IP DEL UE)
GGSN COMPRUEBA SUPLANT. DE DIRECCIÓN IP
8 REGISTRO SIP (...)
9 REGISTRO SIP (...)
10. REGISTRO SIP (...)
11 MENSAJE AAR (...)
VERIFICACIÓN INFO ID
12. ACU. AAR VER. OK
13 SIP 2XX OK

Fig. 6A

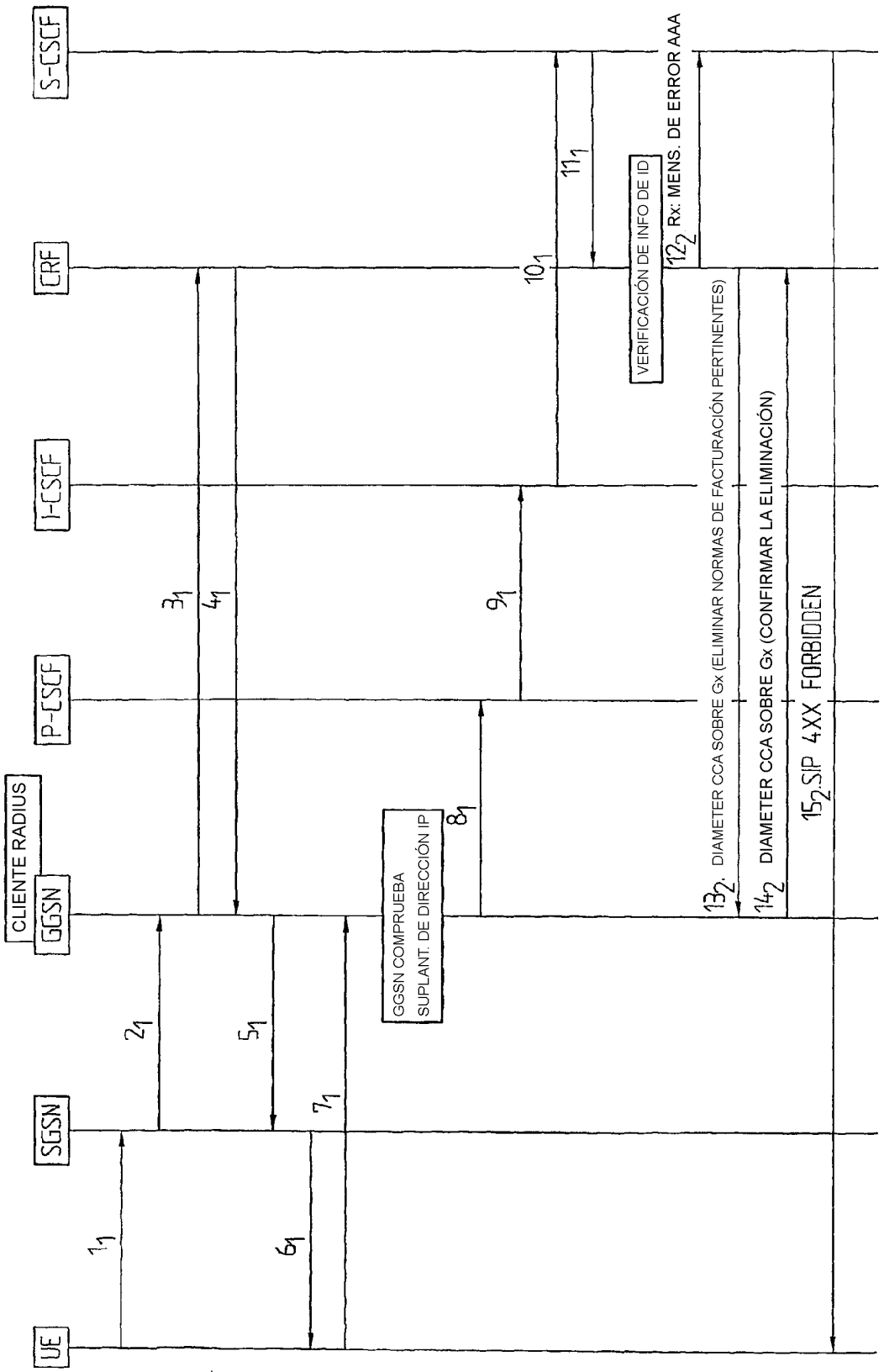

UE
SGSN
CLIENTE RADIUS
GGSN
P-CSCF
I-CSCF
CRF
S-CSCF
1₁
2₁
3₁
4₁
5₁
6₁
7₁
GGSN COMPRUEBA SUPLANT. DE DIRECCIÓN IP
8₁
9₁
10₁
11₁
VERIFICACIÓN DE INFO DE ID
12₂ Rx: MENS. DE ERROR AAA
13₂. DIAMETER CCA SOBRE Gx (ELIMINAR NORMAS DE FACTURACIÓN PERTINENTES)
14₂ DIAMETER CCA SOBRE Gx (CONFIRMAR LA ELIMINACIÓN)
15₂.SIP 4XX FORBIDDEN

Fig. 6B

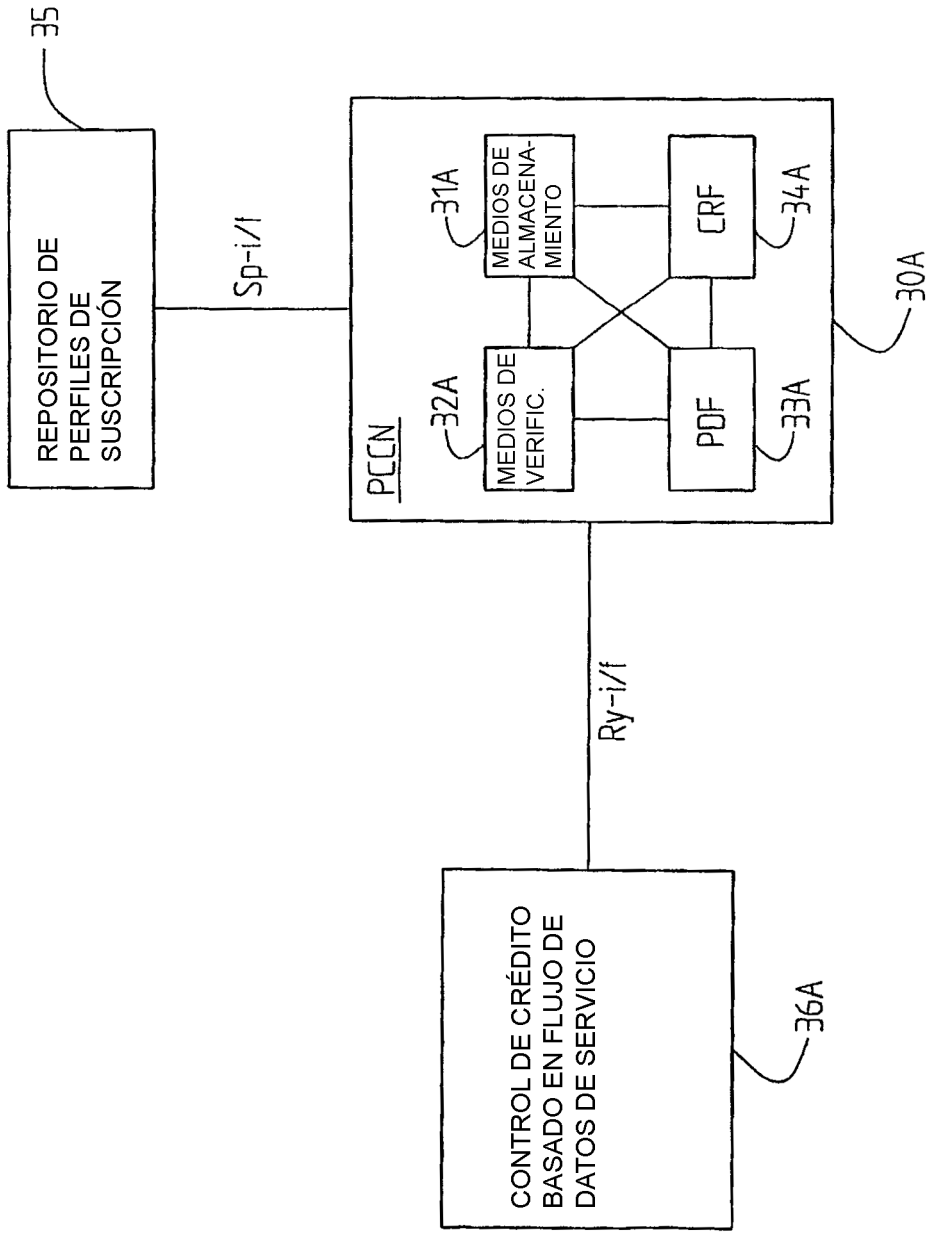

35
REPOSITORIO DE PERFILES DE SUSCRIPCIÓN
Sp-i/f
PCCN
31A
MEDIOS DE ALMACENA-MIENTO
32A
MEDIOS DE VERIFIC.
CRF
34A
PDF
33A
30A
Ry-i/f
CONTROL DE CRÉDITO BASADO EN FLUJO DE DATOS DE SERVICIO
36A

Fig. 7

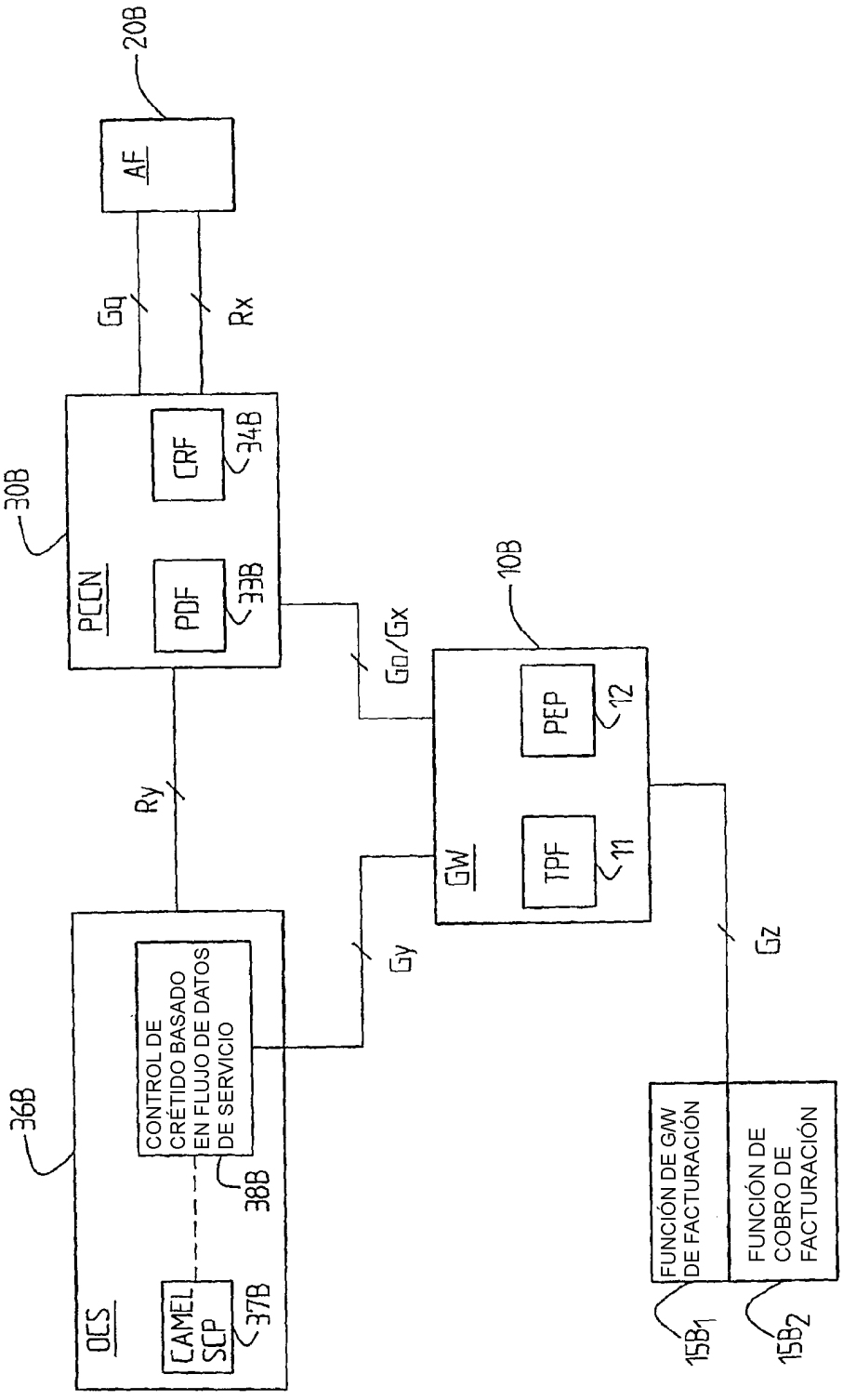

20B
AF
Gq
Rx
30B
PCCN
CRF
34B
PDF
33B
Go/Gx
10B
PEP
12
GW
TPF
11
Ry
Gy
Gz
36B
CONTROL DE CRÉTIDO BASADO EN FLUJO DE DATOS DE SERVICIO
38B
OCS
CAMEL SCP
37B
FUNCIÓN DE GW DE FACTURACIÓN
FUNCIÓN DE COBRO DE FACTURACIÓN
15B1
15B2

Fig. 8A

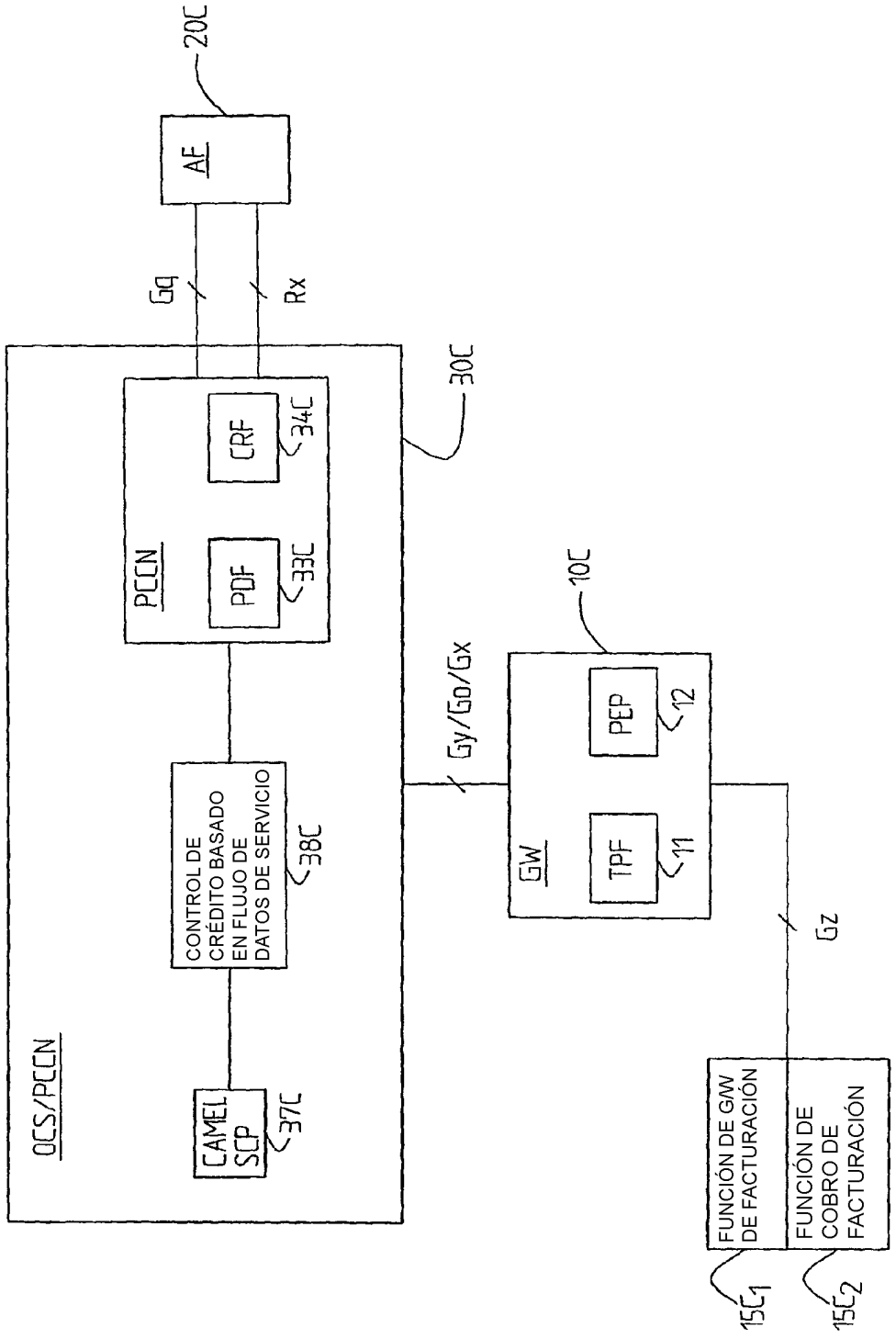

20C
AF
Gq
Rx
30C
PCCN
CRF
34C
PDF
33C
CONTROL DE CRÉDITO BASADO EN FLUJO DE DATOS DE SERVICIO
38C
CAMEL SCP
37C
OCS/PCCN
Gy/Go/Gx
10C
GW
PEP
12
TPF
11
Gz
FUNCIÓN DE GW DE FACTURACIÓN
FUNCIÓN DE COBRO DE FACTURACIÓN
15C1
15C2

Fig. 8B

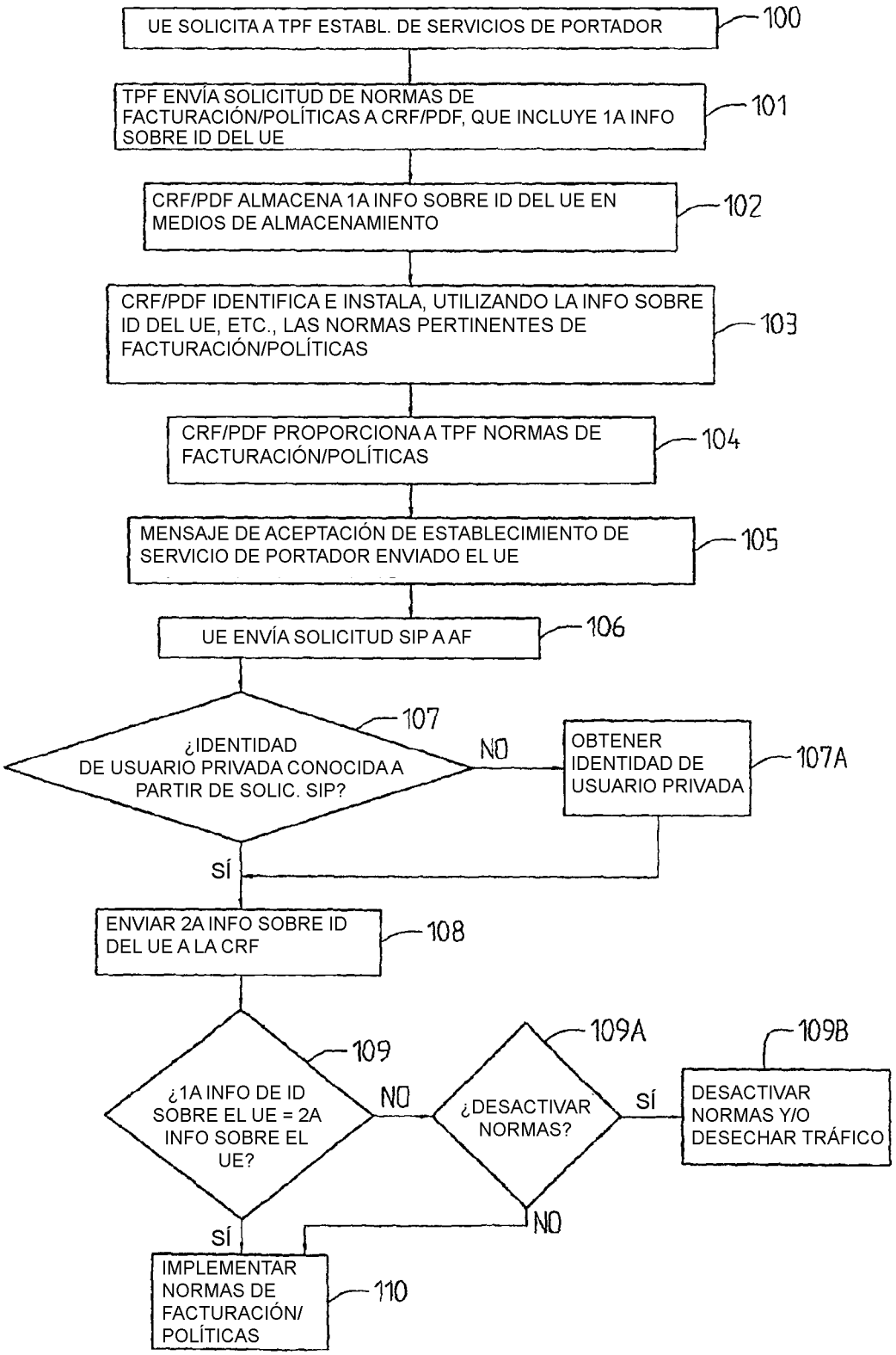

UE SOLICITA A TPF ESTABL. DE SERVICIOS DE PORTADOR
100
TPF ENVÍA SOLICITUD DE NORMAS DE FACTURACIÓN/POLÍTICAS A CRF/PDF, QUE INCLUYE 1A INFO SOBRE ID DEL UE
101
CRF/PDF ALMACENA 1A INFO SOBRE ID DEL UE EN MEDIOS DE ALMACENAMIENTO
102
CRF/PDF IDENTIFICA E INSTALA, UTILIZANDO LA INFO SOBRE ID DEL UE, ETC., LAS NORMAS PERTINENTES DE FACTURACIÓN/POLÍTICAS
103
CRF/PDF PROPORCIONA A TPF NORMAS DE FACTURACIÓN/POLÍTICAS
104
MENSAJE DE ACEPTACIÓN DE ESTABLECIMIENTO DE SERVICIO DE PORTADOR ENVIADO EL UE
105
UE ENVÍA SOLICITUD SIP A AF
106
¿IDENTIDAD DE USUARIO PRIVADA CONOCIDA A PARTIR DE SOLIC. SIP?
107
NO
OBTENER IDENTIDAD DE USUARIO PRIVADA
107A
SÍ
ENVIAR 2A INFO SOBRE ID DEL UE A LA CRF
108
¿1A INFO DE ID SOBRE EL UE = 2A INFO SOBRE EL UE?
109
NO
¿DESACTIVAR NORMAS?
109A
SÍ
DESACTIVAR NORMAS Y/O DESECHAR TRÁFICO
109B
NO
SÍ
IMPLEMENTAR NORMAS DE FACTURACIÓN/ POLÍTICAS
110

Fig. 9