

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 711 340**

51 Int. Cl.:

H04L 29/06 (2006.01)

H04W 12/02 (2009.01)

H04M 3/22 (2006.01)

H04M 7/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **24.07.2008 PCT/EP2008/059727**

87 Fecha y número de publicación internacional: **28.01.2010 WO10009765**

96 Fecha de presentación y número de la solicitud europea: **24.07.2008 E 08775337 (2)**

97 Fecha y número de publicación de la concesión europea: **14.11.2018 EP 2332309**

54 Título: **Interceptación legal para objetivos en una red de protocolo de Internet móvil proxy**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
03.05.2019

73 Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
(100.0%)
164 83 Stockholm, SE

72 Inventor/es:
IOVIENO, MAURIZIO

74 Agente/Representante:
ELZABURU, S.L.P

ES 2 711 340 T3

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

DESCRIPCIÓN

Intercepción legal para objetivos en una red de protocolo de Internet móvil proxy

5 Campo técnico

La presente invención se refiere a métodos y disposiciones en un sistema de telecomunicaciones para proporcionar datos de retención o intercepción a entidades solicitantes de intercepción legal. Particularmente, la invención se refiere a la intercepción legal de un objetivo cuando se utilizan arquitecturas y protocolos basados en el Protocolo de Internet Móvil Proxy en la red de telecomunicaciones.

10

Antecedentes

En muchos países, los operadores y los proveedores de servicios de Internet están obligados por los requisitos legales a proporcionar datos de tráfico, incluidos los datos almacenados, y el contenido de las comunicaciones generadas por los servicios públicos de telecomunicaciones e Internet para abonados objetivo específicos a solicitud de las Autoridades (Agencias de Cumplimiento de la Ley) con el fin de detectar, investigar y perseguir crímenes y delitos, incluido el terrorismo.

15

Estos requisitos ya se han cumplido mediante métodos y sistemas que permiten la intercepción legal de un objetivo en una variedad de redes de telecomunicaciones 3GPP, es decir, redes de telecomunicaciones cubiertas por los estándares 3GPP.

20

Las iniciativas dentro de la Unión Europea (UE) regulan la base legal para la Retención de Datos. Por ejemplo, el Parlamento de la UE adoptó un conjunto de enmiendas que aprobaron la Directiva del Consejo propuesta sobre la Retención de Datos (Directiva 2006/24/EC). En esta directiva, se describen los requisitos iniciales y cómo se manejará una extensión de la directiva. En consecuencia, una parte esencial del esfuerzo del operador por cumplir con la legislación vigente es garantizar que los procesos y las herramientas se puedan adaptar para manejar una expansión del alcance de la Retención de Datos.

25

La especificación técnica ETSI DTS/LI-00039 proporciona una guía para la entrega y los problemas asociados de los datos retenidos de telecomunicaciones y abonados. En particular, dicha especificación proporciona un conjunto de requisitos relacionados con las Interfaces de Traspaso para los datos de tráfico retenidos y los datos del abonado por cumplimiento de la ley y otras autoridades autorizadas que lo solicitan. La Especificación técnica ETSI DTS/LI-00033 contiene requisitos de traspaso y una especificación de traspaso para los datos que se identifican en la Directiva 2006/24/EC de la UE sobre los datos retenidos.

30

35

En el proceso continuo de integración de redes y protocolos de comunicaciones heterogéneos, 3GPP ahora está especificando un Evolved Packet System (EPS) (Sistema de Paquetes Evolucionado), que permite utilizar algunos protocolos IETF para movilidad, tal como Protocolo de Internet Móvil Proxy v6, cuya arquitectura funcional y protocolos relacionados se definen en el proyecto de IETF "Proxy Mobile IPv6". Para este propósito, 3GPP especifica en TS 23.402 "Mejoras en la arquitectura para accesos que no son 3GPP (Versión 8)" una arquitectura que permite el uso de protocolos PMIPv6 y terminales no 3GPP para usar una red 3GPP para obtener servicios de los operadores.

40

Claramente, cada operador que usa una red basada en 3GPP aún debe cumplir con los requisitos legales y reglamentarios para objetivos que pueden incluir terminales que no sean 3GPP, de acuerdo con la arquitectura de Intercepción Legal estándar del 3GPP definida en 3GPP TS 33.107 "Seguridad 3G; Arquitectura y Funciones de Intercepción Legal (Versión 8)".

45

Desafortunadamente, las soluciones de Intercepción Legal existentes para arquitecturas de red 3GPP no cubren el caso en el que la movilidad del terminal se maneja mediante el uso de protocolos IETF tales como el Protocolo de Internet Móvil Proxy v6 (PMIPv6).

50

El caso en el que se usa un acceso no 3GPP para obtener servicios de telecomunicación desde una red 3GPP tampoco está cubierto.

55

Compendio

El objetivo de la presente invención es superar los inconvenientes mencionados anteriormente.

Dentro de este objetivo, un objeto de la invención es proporcionar métodos y sistemas que puedan permitir que se apliquen funcionalidades de Intercepción Legal con respecto a terminales que no sean 3GPP y, en particular, en objetivos para los cuales la arquitectura del Protocolo de Internet Móvil Proxy y las funciones se utilizan en la red.

60

Este objetivo y otros objetos que se harán más evidentes en lo sucesivo se lograrán mediante un método para proporcionar a las Agencias de Cumplimiento de la Ley en una red de telecomunicaciones los resultados de retención o Intercepción relacionados con un nodo móvil objetivo en un dominio de Protocolo de Internet Móvil Proxy y conectados a la red de telecomunicaciones a través de una Pasarela de Acceso Móvil (Mobile Access

65

Gateway), que comprende los pasos para configurar al menos uno entre dicha Pasarela de Acceso Móvil y un Anclaje de Movilidad Local (Local Mobility Anchor) para que funcionen como Elementos de Control de Interceptación.

5 El objetivo y los objetos anteriores también se logran mediante un sistema de Interceptación Legal para la Retención de Datos de tráfico o la interceptación de datos de tráfico y contenido de comunicación relacionado con un nodo móvil objetivo en un dominio de Protocolo de Internet Móvil Proxy, conectado a una red de telecomunicaciones a través de una Pasarela de Acceso Móvil, en donde al menos uno entre un Anclaje de Movilidad Local y dicha Pasarela de Acceso Móvil están configurados para operar como Elementos de Control de Interceptación.

10 La presente invención también se refiere a programas informáticos que comprenden partes de códigos de software para implementar el método descrito anteriormente cuando se opera en un procesador de un Elemento de Control de Interceptación o una fuente de Retención de Datos. En particular, un programa informático puede cargarse en al menos uno de entre una Pasarela de Acceso Móvil o un Anclaje de Movilidad Local para configurar dicha Pasarela de Acceso Móvil o Anclaje de Movilidad Local como Elemento de Control de Interceptación o fuente de Retención de Datos operable en una Interceptación Legal o sistema de Retención de Datos según la invención. Dicho programa informático puede almacenarse en un medio legible por ordenador, que puede ser una memoria permanente o regrabable dentro del Elemento de Control de Interceptación o la fuente de Retención de Datos o puede ubicarse externamente. El programa informático respectivo también puede transferirse al Elemento de Control de Interceptación o a la fuente de Retención de Datos, por ejemplo, a través de un enlace por cable o un enlace inalámbrico como una secuencia de señales.

Breve descripción de los dibujos

25 Otras características y ventajas de la invención se harán más evidentes a partir de la descripción detallada de realizaciones particulares, pero no exclusivas, ilustradas a modo de ejemplos no limitativos en los dibujos adjuntos, en los que:

30 La Figura 1 muestra una arquitectura funcional de un Nodo móvil en una red basada en un Protocolo de Internet Móvil Proxy;

La Figura 2 es una disposición de un sistema de Interceptación Legal de acuerdo con un primer aspecto de la presente invención, en el que las Pasarelas de Acceso Móvil o los Anclajes de Movilidad Local actúan como Elementos de Control de Interceptación.

35 La Figura 3 es una disposición de un sistema de Interceptación Legal de acuerdo con un segundo aspecto de la presente invención, en el que las Pasarelas de Acceso Móvil o los Anclajes de Movilidad Local actúan como fuentes de Retención de Datos.

La Figura 4 es un diagrama de flujo que muestra la interceptación de datos de acuerdo con un aspecto de la invención.

Descripción detallada

40 La Figura 1 muestra una arquitectura funcional de un Nodo Móvil (1) en una red basada en el Protocolo de Internet Móvil Proxy.

45 Una vez que el nodo móvil 1 ingresa a un Protocolo de Internet Móvil Proxy v6 dominio 2 y se conecta a un enlace de acceso, una Pasarela 3 de Acceso Móvil (MAG) en ese enlace de acceso, después de identificar el nodo móvil 1 y adquirir su identidad, determina si el nodo móvil 1 está autorizado para el servicio de gestión de movilidad basado en red.

50 Si la red 2 ha determinado que el servicio de gestión de movilidad basado en la red debería ofrecerse a ese nodo móvil 1, la red 2 garantiza que el nodo móvil 1 que utiliza cualquiera de los mecanismos de configuración de direcciones permitidos por la red puede obtener la configuración de direcciones en la interfaz conectada y moverse a cualquier lugar en ese dominio de Protocolo de Internet Móvil Proxy.

55 La configuración de la dirección obtenida puede incluir la dirección o direcciones de su prefijo o prefijos de la red doméstica, la dirección del enrutador por defecto en el enlace y otros parámetros de configuración relacionados.

60 Desde la perspectiva del nodo móvil 1, todo el dominio del Protocolo de Internet móvil de Proxy puede aparecer como un solo enlace. La red 2 puede tener cuidado de que el nodo móvil 1 crea que siempre está en el mismo enlace en el que obtuvo su configuración de dirección inicial, incluso aunque su punto de conexión en esa red ha cambiado.

El nodo móvil 1 puede ser un nodo solo IPv4, un nodo solo IPv6 o un nodo doble IPv4/IPv6. En función de lo que esté habilitado en la red para ese nodo móvil, el nodo móvil podrá obtener direcciones IPv4, IPv6 o doble IPv4/IPv6 y moverse a cualquier lugar en ese dominio de Protocolo de Internet Móvil Proxy.

65

- 5 Si el nodo móvil 1 realiza una transferencia entre interfaces al mover su configuración de dirección de una interfaz a la otra y si un Anclaje 4 de Movilidad Local (LMA) recibe una sugerencia de transferencia a partir del servicio de la Pasarela 3 de Acceso Móvil (MAG) sobre el mismo, el Anclaje 4 de Movilidad Local puede asignar el mismo prefijo o prefijos de red doméstica que previamente asignó antes de la transferencia.
- 10 El nodo móvil 1 también puede ser capaz de realizar una transferencia cambiando su punto de conexión de una primera Pasarela 3 de Acceso Móvil a una Pasarela 3' de Acceso Móvil diferente utilizando la misma interfaz y, por lo tanto, puede mantener la configuración de la dirección en la interfaz adjunta.
- 15 Los procedimientos entre el nodo móvil 1 y las entidades funcionales definidas y la señalización entre las Pasarelas 3 de Acceso Móvil y los Anclajes 4 de Movilidad Local necesarios para configurar un túnel para transportar paquetes entre el Nodo Móvil 1 y las Pasarelas de Acceso Móvil son conocidos por los expertos en la materia según se define en el proyecto de IETF "Proxy Mobile IPv6, y no se describe aquí en detalle.
- 20 Tales procedimientos pueden incluir, por ejemplo, solicitud de enrutador y anuncio de enrutador, actualización de vinculación de proxy y aceptación de vinculación de proxy, actualización de vinculación de proxy de cancelación de registro. El formato de los paquetes tunelizados también se especifica y se puede usar en una realización preferida de la presente invención.
- 25 La identidad de un nodo móvil en el dominio Protocolo de Internet Móvil Proxy v6 es el identificador estable de un nodo móvil 1, que las entidades de movilidad en un dominio de Protocolo de Internet Móvil Proxy v6 pueden adquirir y usar para identificar de manera predecible un nodo móvil. Por lo general, esto puede ser un identificador tal como un Identificador de Acceso a la Red (NAI).
- 30 Con referencia a las Figuras 2 y 4, se describe una arquitectura para acceder a datos relacionados con las comunicaciones en un sistema 10 de Interceptación Legal de acuerdo con la invención.
- 35 El sistema de Interceptación Legal 10 puede comprender un Elemento 11 de Control de Interceptación (ICE) que proporciona al equipo de usuario del usuario objetivo acceso a la red de telecomunicaciones.
- 40 Según la invención, el Anclaje 4 de Movilidad Local y/o la Pasarela 3 de Acceso Móvil se definen como Elementos 11 de Control de Interceptación con el fin de interceptar la señalización y el contenido de la comunicación para un nodo móvil 1 que es un objetivo para la interceptación legal. Los nodos de red, incluidos el Anclaje 4 de Movilidad Local y/o la Pasarela 3 de Acceso Móvil, pueden definirse igualmente como Elementos de Control de Interceptación.
- 45 El sistema 10 de Interceptación Legal de acuerdo con la invención puede comprender además una o más Instalaciones de Monitoreo del Cumplimiento de la Ley (LEMF) 12, a través de las cuales las Agencias de Cumplimiento de la Ley (LEA) respectivas pueden recibir información de Interceptación.
- 50 Una entidad de la Función 13 de Administración (ADMF) puede configurarse adicionalmente para enviar la identidad de destino y los datos de autorización de Interceptación Legal recibidos desde las respectivas Agencias de Cumplimiento de la Ley a los Elementos 11 de Control de Interceptación.
- 55 La Función 13 de Administración puede interactuar a través de una primera Interfaz 14 de Traspaso (HI1) con todas las Agencias de Cumplimiento de la Ley que pueden requerir la Interceptación en la red de interceptación y pueden mantener las actividades de interceptación de las Agencias de Cumplimiento de la Ley individuales separadas y conectadas a la red de interceptación.
- 60 La Función 13 de Administración también se puede usar para ocultar a los Elementos 11 de Control de Interceptación que las activaciones múltiples de diferentes Agencias de Cumplimiento de la Ley en el mismo objetivo pueden haber estado activas.
- 65 Además, la Función 13 de Administración puede dividirse para asegurar la separación de los datos de aprovisionamiento procedentes de diferentes agencias.
- Cada Elemento 11 de Control de Interceptación físico puede estar vinculado a la Función de Administración 13 por medio de su propia interfaz X1_1. En consecuencia, cada Elemento 11 de Control de Interceptación individual puede realizar una Interceptación, es decir, activación, desactivación, interrogación e invocación, independientemente de otros Elementos 11 de Control de Interceptación.
- Para entregar la información interceptada a las Agencias de Cumplimiento de la Ley, se pueden prever dos entidades de Funciones de Entrega (DF), cada una intercambiando partes respectivas de información con la Función 13 de Administración, a través de las interfaces X1_2 y X1_3, y la Instalación 12 de Monitoreo del Cumplimiento de la Ley

5 En particular, una entidad 15 de Función de Entrega DF2 puede estar configurada para recibir Información Relacionada con la Interceptación (IRI) a partir del Elemento 11 de Control de Interceptación, a través de una Interfaz X2, y para convertir y distribuir la Información Relacionada con la Interceptación a las Agencias de Cumplimiento de la Ley pertinentes a través de una segunda Interfaz 16 de Traspaso (HI2) mediante una Función 17 de Mediación (MF).

10 La Información Relacionada con la Interceptación puede ser una recopilación de información o datos asociados con servicios de telecomunicación que implican la identidad objetivo, tal como la información o datos asociados a llamadas, por ejemplo, intentos de llamada fallidos, información o datos asociados al servicio, por ejemplo, gestión del perfil de servicio por abonado, e información de ubicación.

15 Una entidad 18 de Función de Entrega DF3 puede configurarse para recibir información de Contenido de Comunicaciones (CC) desde los Elementos 11 de Control de Interceptación a través de una interfaz X3, y para convertir y distribuir dicha información a la Agencia de Cumplimiento de la Ley pertinente a través de la Función 19 de Mediación y una tercera Interfaz 20 de Traspaso (HI3).

20 El Contenido de las Comunicaciones puede ser información diferente de la información Relacionada con la Interceptación, que se intercambia entre dos o más usuarios de un servicio de telecomunicaciones y, más en general, puede incluir información que, como parte de algún servicio de telecomunicaciones, podría almacenarse por un usuario para su posterior recuperación por otro usuario.

En el funcionamiento de acuerdo con la invención, la activación de la Interceptación Legal para un objetivo específico se puede realizar en la interfaz X1_1 utilizando el Identificador de Acceso a la Red.

25 La Información Relacionada con la Interceptación puede ser proporcionada por el Anclaje 4 de Movilidad Local y la Pasarela 3 de Acceso Móvil en la interfaz X2, cada vez que se detecte un evento basado en el Protocolo de Internet Móvil Proxy en el Anclaje 4 de Movilidad Local o en la Pasarela 3 de Acceso Móvil.

30 De nuevo, tales eventos pueden incluir solicitud de enrutador y anuncio, Actualización de Vinculación de Proxy y Aceptación y Actualización de Vinculación de Proxy de cancelación de registro.

35 Los expertos en la técnica aprecian que se pueden informar los parámetros aplicables definidos en el Protocolo de Internet Móvil de Proxy para cada mensaje. Los expertos en la técnica también aprecian que la Información Relacionada Interceptada puede ser proporcionada por otros nodos de red que implementan las funcionalidades de Anclaje de Movilidad Local y/o Pasarela de Acceso Móvil.

40 El Contenido de comunicación interceptado para un Nodo Móvil 1 que es el objetivo de la interceptación puede ser duplicado por el Anclaje 4 de Movilidad Local y/o por la Pasarela de Acceso Móvil a través de la interfaz X3. El contenido interceptado de la comunicación puede ser duplicado por otros nodos de red que implementan las funciones de Anclaje de Movilidad Local y/o Pasarela de Acceso Móvil.

45 La presente invención define así un mecanismo que se puede usar para permitir la interceptación legal de un objetivo cuando se utilizan arquitecturas y protocolos de red basados en el Protocolo de Internet Móvil Proxy, con referencia particular al Protocolo de Internet Móvil Proxy v6. La invención se ha descrito en términos de funciones lógicas definidas por IETF, pero es aplicable a cualquier nodo de red que implemente dichas funciones lógicas.

Toda la información de tráfico se puede utilizar para un almacenamiento adecuado con el fin de satisfacer los posibles requisitos legales relacionados con la Retención de Datos.

50 A este respecto, la Figura 3 representa una disposición para retener datos en un Proveedor 21 de Servicios de Comunicación (CSP) de acuerdo con la presente invención. Específicamente, al Proveedor 21 de Servicios de Comunicación se le puede proporcionar un Sistema 23 de Retención de Datos (DRS) para intercambiar los datos retenidos que relacionan la información con una Autoridad Solicitante 24, que puede ser una Agencia de Cumplimiento de la Ley (LEA).

55 El Proveedor 21 de Servicios de Comunicación (CSP) puede incluir la Pasarela 3 de Acceso Móvil 3 y el Anclaje 4 de Movilidad Local, configurado para funcionar como fuentes de Retención de Datos.

60 Los datos intercambiados entre el Proveedor 21 de Servicios de Comunicación y la Autoridad Solicitante 24 pueden incluir solicitudes a partir de la Autoridad Solicitante 24, respuestas correspondientes a partir del Sistema 23 de Retención de Datos y otra información de Retención de Datos, tales como los resultados de las solicitudes y reconocimientos de recepción. Las interfaces a través de las cuales el Proveedor 21 de Servicios de Comunicación y el Sistema 23 de Retención de Datos intercambian los datos anteriores con la Autoridad Solicitante se denotan como Interfaces de Traspaso.

65

5 La Interfaz de Traspaso genérica adopta una estructura de dos puertos en la que la información administrativa de solicitud/respuesta y la información de datos retenidos se separan lógicamente. En particular, un primer puerto 25 de Interfaz de Traspaso HI-A puede configurarse para transportar diversos tipos de información administrativa, de solicitud y respuesta desde/a la Autoridad Solicitante 24 y una organización en el Proveedor 21 de Servicios de Comunicación que es responsable de los asuntos de Datos Retenidos, identificados por una Función 27 de Administración.

10 Una segunda Interfaz 26 de Traspaso HI-B puede configurarse para transportar la información de datos retenidos almacenada en un depósito 29 desde el Proveedor de Servicios de Comunicación 21 a la Autoridad Solicitante 24. Los parámetros de datos retenidos individuales deben enviarse a la Autoridad Solicitante 24 al menos una vez, si está disponible. Para este objetivo, se puede proporcionar una función 28 de Mediación/Entrega, para recuperar los datos retenidos del depósito 9 y reenviar dichos datos a la Autoridad Solicitante 24 en un formato adecuado a través de la HI-B 26.

15 Claramente, varias modificaciones serán evidentes y pueden ser hechas fácilmente por los expertos en la técnica sin apartarse del alcance de la presente invención. Por lo tanto, el alcance de las reivindicaciones no estará limitado por las ilustraciones o las formas de realización preferidas dadas en la descripción en forma de ejemplos, sino que las reivindicaciones abarcarán todas las características que residen en la presente invención, incluidas todas las características que serían tratadas como equivalentes por los expertos en la técnica. En particular, en vista de la descripción anterior, está claro que, en este texto y en las reivindicaciones adjuntas, los términos Anclaje de Movilidad Local y Pasarela de Acceso Móvil abarcan cualquier nodo de red que implemente dichas funciones. El alcance de la invención está definido por las reivindicaciones adjuntas.

25 Cuando las características técnicas mencionadas en cualquier reivindicación están seguidas por signos de referencia, dichos signos de referencia se han incluido con el único propósito de aumentar la inteligibilidad de las reivindicaciones y, por consiguiente, dichos signos de referencia no tienen ningún efecto limitante en la interpretación de cada elemento identificado a modo de ejemplo por dichos signos de referencia.

REIVINDICACIONES

- 5 1. Un método para usar en una red de telecomunicaciones para proporcionar a las Agencias de Cumplimiento de la Ley datos de Interceptación relacionados con un nodo móvil objetivo (1) conectado a un dominio (2) de Protocolo de Internet Móvil Proxy de la red de telecomunicaciones a través de una Pasarela (3) de Acceso Móvil , que está conectado a un Anclaje (4) de Movilidad Local a través de un túnel que transporta paquetes entre el nodo móvil de destino (1) y la Pasarela (3) de Acceso Móvil, comprendiendo el método los pasos para configurar al menos uno de entre dicha Pasarela (3) de Acceso Móvil y dicho Anclaje (4) de Movilidad Local para operar como Elementos (11) de Control de Interceptación, en donde la información relacionada con la interceptación es proporcionada respectivamente por al menos uno de entre dicha Pasarela (3) de Acceso Móvil y dicho Anclaje (4) de Movilidad Local para una Función (15) de Entrega a través de una interfaz X2 cada vez que se detecta un evento basado en el Protocolo de Internet Móvil Proxy en al menos uno entre dicha Pasarela (3) de Acceso Móvil y dicho Anclaje (4) de movilidad local, respectivamente.
- 15 2. El método de la reivindicación 1, en el que tanto el Anclaje (4) de Movilidad Local como la Pasarela (3) de Acceso Móvil están configurados para operar como Elementos (11) de Control de Interceptación.
- 20 3. El método de la reivindicación 1 o 2, que comprende además usar el Identificador de Acceso a la Red asociado al nodo móvil objetivo (1) para activar la interceptación legal para el nodo móvil objetivo (1).
- 25 4. El método de acuerdo con la reivindicación 3, en el que la activación de la Interceptación Legal en el nodo móvil objetivo (1) se realiza mediante el Anclaje (4) de Movilidad Local o la Pasarela (3) de Acceso Móvil en una interfaz X1_1 que conecta los Elementos (11) de Control de Interceptación a una Función (13) de Administración.
- 30 5. El método de acuerdo con la reivindicación 1, en el que dicho evento basado en el Protocolo de Internet Móvil Proxy incluye al menos uno de los siguientes eventos: solicitud de enrutador, aviso de enrutador, actualización de vinculación de proxy, aceptación de vinculación de proxy, actualización de vinculación de proxy de cancelación de registro.
- 35 6. El método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que dicho Protocolo de Internet Móvil Proxy es el Protocolo de Internet Móvil Proxy v6.
- 40 7. Un sistema (10) de Interceptación Legal para la interceptación de datos relacionados con un nodo móvil objetivo (1) conectado a un dominio (2) de Protocolo de Internet Móvil Proxy de una red de telecomunicaciones a través de una Pasarela (3) de Acceso Móvil, que está conectado a un Anclaje (4) de Movilidad Local a través de un túnel que transporta paquetes entre el nodo móvil objetivo (1) y la Pasarela (3) de Acceso Móvil, en donde al menos uno de entre dicho Anclaje (4) de Movilidad Local y dicha Pasarela (3) de Acceso Móvil son configurados para operar como Elementos (11) de Control de Interceptación, están conectados a una Función (15) de Entrega a través de una interfaz X2 y están configurados para proporcionar información relacionada con la Interceptación a dicha Función (15) de Entrega a través de dicha interfaz X2 cada vez que un evento basado en el Protocolo de Internet Móvil Proxy se detecta en al menos uno de entre dicha Pasarela (3) de Acceso Móvil y dicho Anclaje (4) de Movilidad Local, respectivamente.
- 45 8. El sistema de Interceptación Legal de la reivindicación 7, en el que tanto el Anclaje (4) de Movilidad Local como la Pasarela (3) de Acceso Móvil están configurados para operar como Elementos (11) de Control de Interceptación.
- 50 9. Una Pasarela (3) de Acceso Móvil configurado para operar como Elemento (11) de Control de Interceptación para un sistema (10) de Interceptación Legal de acuerdo con la reivindicación 7.
- 55 10. Un Anclaje (4) de Movilidad Local configurado para operar como Elemento (11) de Control de Interceptación para un sistema (10) de Interceptación Legal de acuerdo con la reivindicación 7.
11. Una red de telecomunicaciones que comprende un sistema (10) de Interceptación Legal de acuerdo con la reivindicación 7.
12. Un programa informático que se puede cargar en al menos uno de entre una Pasarela (3) de Acceso Móvil y un Anclaje (4) de Movilidad Local para realizar el método de la reivindicación 1 cuando se carga en al menos uno de entre dicha Pasarela (3) de Acceso Móvil (3) y dicho Anclaje (4) de movilidad local, respectivamente.

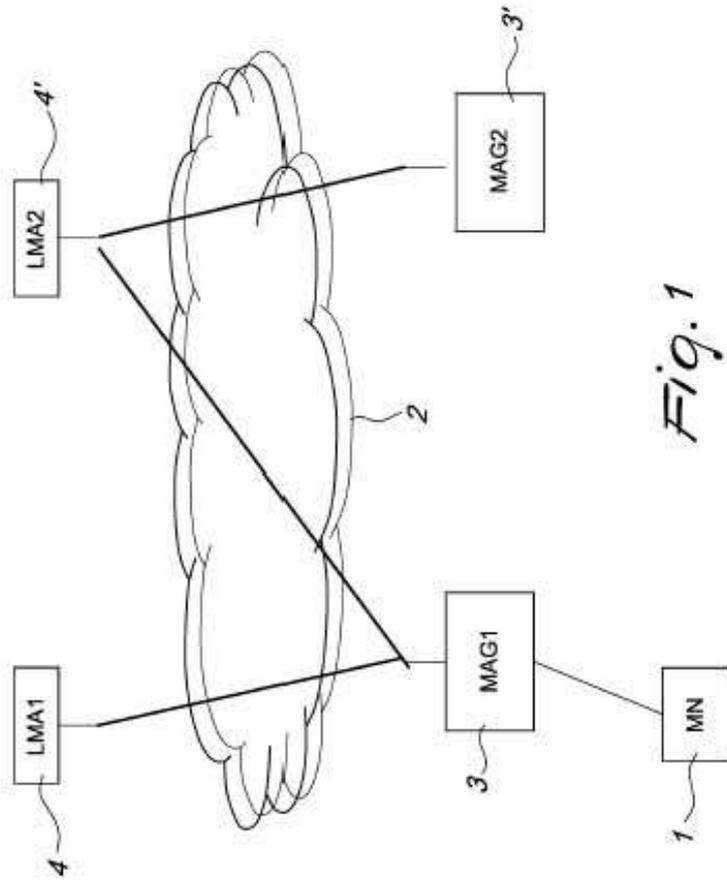


Fig. 1

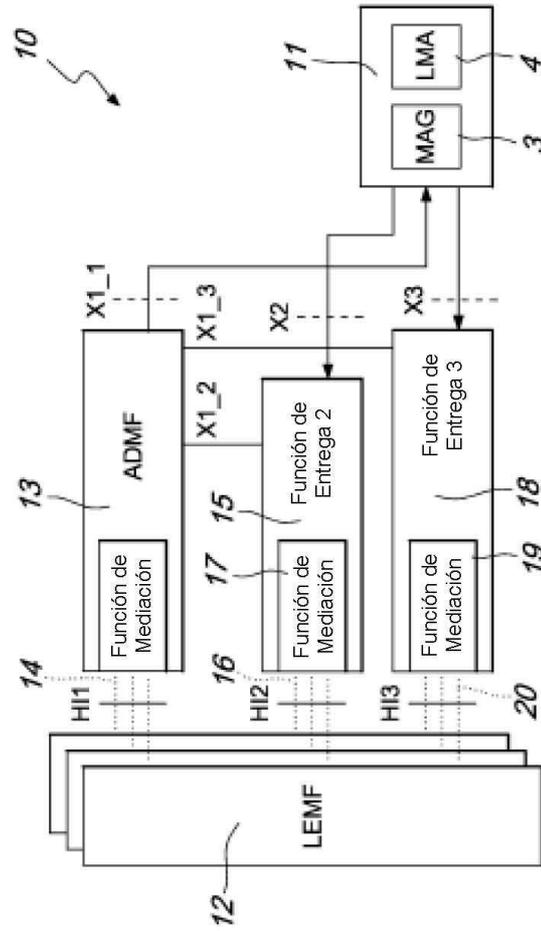


Fig. 2

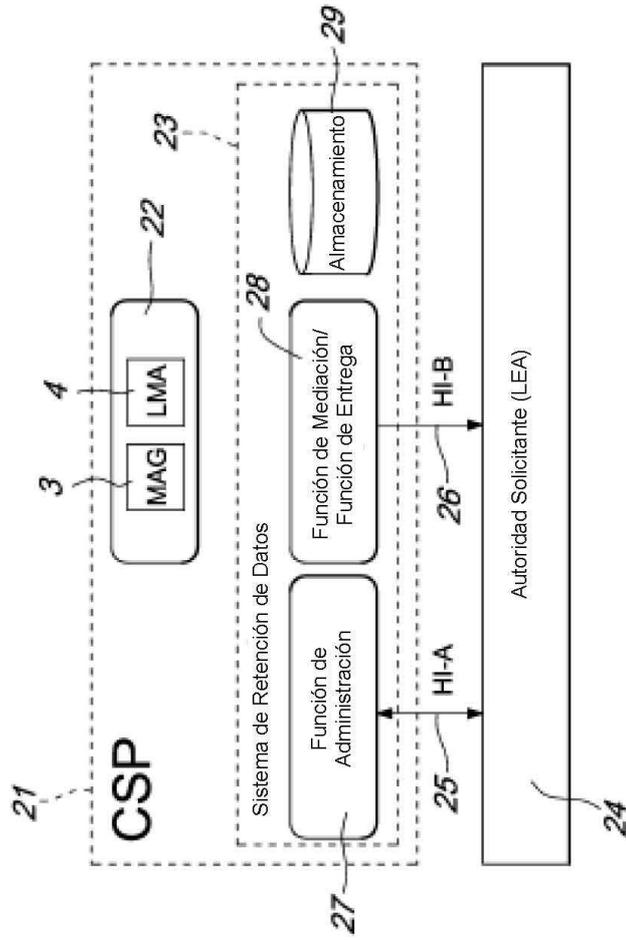


Fig. 3

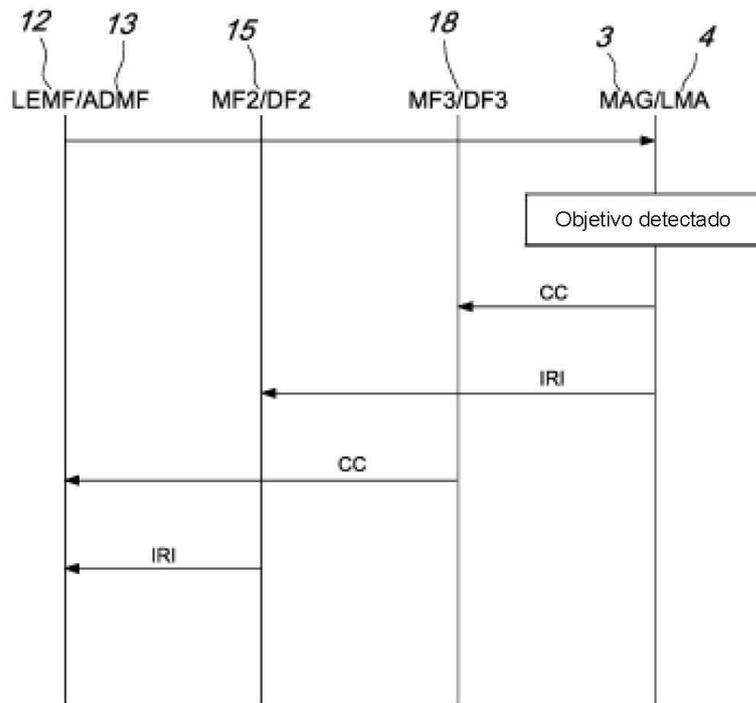


Fig.4