(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 416**

(51) Int. CI.:
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **01911500 .5**
(96) Fecha de presentación: **15.01.2001**
(97) Número de publicación de la solicitud: **1247411**
(97) Fecha de publicación de la solicitud: **09.10.2002**

(54) Título: **MÉTODO Y APARATO EN UN SISTEMA DE TELECOMUNICACIONES.**

(30) Prioridad:
15.01.2000 EP 00850007

(45) Fecha de publicación de la mención BOPI:
13.03.2012

(45) Fecha de la publicación del folleto de la patente:
13.03.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
CHARAS, Philippe

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Método y aparato en un sistema de telecomunicaciones.

Campo técnico de la invención

La presente invención se refiere generalmente a un método para su uso en sistemas de comunicaciones, y más particularmente, la invención se refiere a un método de itinerancia global independiente del acceso. La invención se refiere también a un sistema y aparato para llevar a cabo el método.

Antecedentes de la invención

Un gran número de estándares de acceso de telefonía fija y móvil están ahora disponibles, tales como el Wideband-Code Division Multiple Access (W-CDMA – Acceso Múltiple por División de Código de Banda Ancha), Universal Mobile Telephone System-Time Division Duplex (UMTS-TDD – Sistema de Telefonía Móvil Universal -Transmisión Bidireccional por División de Tiempo), CDMA 2000, Wireless-Local Area Network (W-LAN – Transmisión inalámbrica-Red de Área Local), EDGE, etc., todos los cuales pertenecen a los estándares inalámbricos de 3ª Generación. Cada tipo de estándar de acceso tiene su propio concepto de red particular, en el que el Mobile Internet Protocol (Mobile IP – Protocolo de Internet de Telefonía Móvil) y el protocolo de túnel de General Packet Radio Service (GPRS – Servicio de Radio en paquetes General) son los dos conceptos principales. La invención, no obstante, no está limitada a los conceptos mencionados anteriormente.

La patente de Estados Unidos 5.862.480 describe un método para autorizar a una unidad de abonado a que se comunique utilizando una o más redes de radiofrecuencia. En este método, un servidor de acceso recibe una solicitud de acceso a la red desde una red solicitante acerca de si a la unidad del abonado se le permite acceder a la red. El servidor de acceso determina si un grupo al cual pertenece la unidad del abonado está autorizado a acceder a la red o a otra red basándose en la ubicación de la unidad del abonado. El servidor de acceso permite o deniega el acceso de la unidad del abonado a la red solicitada.

Cuando se utilizan los métodos actualmente disponibles, la interoperabilidad entre diferentes conceptos de red no está garantizada. Esto se debe principalmente a tres obstáculos. Primero, existe una falta de perfiles de abonado, estándares de servicio y mecanismos de validación comunes, que eviten la ejecución de políticas relativas, pero que no estén limitados a la autorización de acceso y de servicio, y al registro de operaciones y movilidad en diferentes redes. Segundo, existe una falta de Quality of Service (QoS – Calidad de Servicio) común frente a un paradigma de asignación de recurso en las redes de acceso, debido a un planteamiento ascendente en lugar de descendente en el diseño de las capas de enlace de datos respecto a requisitos de QoS. Tercero, existe una falta de estándares de capa superior comunes en los terminales, que impide la transparencia de servicio cuando los terminales de usuario, es decir, los clientes, itineran entre diferentes redes que llevan servicios específicos.

Así, existe un problema con la interoperabilidad entre redes heterogéneas principalmente debido a problemas con la validación y la transparencia de servicio en y entre diferentes redes. Es, por supuesto, teóricamente posible armonizar redes dispares en todos los niveles anteriores y crear así una interoperabilidad. Existe, no obstante, una necesidad de una manera orgánica de integrar redes heterogéneas y proporcionar así itinerancia global independiente del acceso.

Compendio de la invención

La presente invención proporciona por lo tanto una solución a los problemas de integrar redes heterogéneas, que proporcionan itinerancia global independiente del acceso y acceso a servicios por medio de redes heterogéneas, sin necesidad de armonizar redes dispares.

Un objeto de la invención es proporcionar itinerancia global independiente del acceso en redes heterogéneas.

Otro objeto de la invención es proporcionar una ejecución de política y transparencia de servicio cuando los terminales itineran entre diferentes redes heterogéneas.

La invención logra los objetos mencionados anteriormente en realizaciones de la misma:

sacando al menos las funciones relativas a servicios esenciales o a todos de la red a la periferia, es decir, clientes o terminales de usuario, separando las funciones de servicio y de acceso,
concibiendo el mecanismo de transporte entre clientes o terminales y servidores como una línea de paquetes, no necesariamente añadiendo un valor extra excepto la clasificación de transporte y de Quality of Service (QoS – Calidad de Servicio) del mismo,
separando la registro de operaciones de transporte del registro de operaciones de servicios e introduciendo el pago de transporte en tiempo real,

definiendo políticas, básicamente un conjunto de derechos y obligaciones, en un punto de definición de política, por ejemplo, servidores de operador, que ejecuten políticas en un punto de ejecución de política que reside en el cliente, por ejemplo el terminal de usuario, y
estandarizando y modularizando una arquitectura de cliente o de terminal que soporta las entidades anteriores.

Más específicamente, las políticas definidas en el punto de definición de política son ejecutadas localmente en el terminal de usuario en un punto de ejecución de política local en lugar de, como siempre, en la red. Por políticas en este contexto, se quiere decir, entre otras cosas, un conjunto de derechos y obligaciones que pertenecen a la validación de usuarios, la autorización al acceso y a servicios así como a la compra y negociación de recursos de transporte y seguridad. Las políticas de contabilidad pueden gobernar las funciones de registro de operaciones para el registro de operaciones del acceso y el registro de operaciones del servicio. Mediante la separación de las funciones de servicio y de acceso, se puede pagar el transporte separadamente, por ejemplo, en tiempo real por medio de una tarjeta de crédito, una tarjeta de prepago, una tarjeta de monedero o similar y se pueden pagar los servicios como siempre, por ejemplo, mediante la factura de un proveedor de servicio, por ejemplo.

El cliente o el terminal actúan así más como un gestor de perfil personal, ejecutando políticas, gestionando con ello los derechos a servicios y al acceso. Servicios y acceso están controlados en el terminal mediante el punto de ejecución de política local y el gestor de terminal/perfil es independiente del acceso, puesto que el acceso puede ser comprado en tiempo real. Así, el abonado puede acceder a cualquier red en cualquier momento, considerando que se proporciona el módulo de acceso de módem correcto o de capa 1 y de capa 2. Se hace referencia al modelo de Open Systems Interconnect (OSI – Interconexión de sistemas Abiertos).

Adoptando la solución propuesta, como se describe en realizaciones de la invención, es posible la validación entre redes heterogéneas tales como CDMA 2000, W-LAN, EDGE y UMTS. La capacidad, con la presente invención, de comprar acceso también abre la posibilidad de que el terminal actúe como una plataforma de comercio electrónico; es decir, el terminal puede ser utilizado para comprar cualquier cosa, no sólo acceso.

El término transporte utilizado en esta memoria puede identificar una red de acceso tal como CDMA 2000, W-CDMA, etc. o por ejemplo tanto una red de acceso como una red de IP de núcleo. El término acceso se utiliza como sinónimo del término transporte.

Aunque la invención ha sido resumida anteriormente, el método y disposición de acuerdo con las reivindicaciones independientes adjuntas definen el alcance de la invención. Varias realizaciones se definen también en las reivindicaciones dependientes.

Breve descripción de los dibujos

Los objetos y ventajas de la invención se comprenderán leyendo la siguiente descripción detallada junto con los dibujos, en los cuales:

la figura 1 muestra una representación esquemática de la arquitectura para la itinerancia global de acuerdo con la presente invención;
la figura 2 muestra una realización de un método de pago anónimo de acuerdo con la presente invención;
la figura 3 muestra una vista detallada de una realización de un punto de ejecución de política local de acuerdo con la presente invención;
la figura 4 muestra una vista detallada de una realización de un portal de telefonía móvil seguro de acuerdo con la presente invención;
la figura 5 es un diagrama de señalización de ejemplo que ilustra la señalización implicada en un establecimiento de sesión de acuerdo con la presente invención;
la figura 6 es una vista detallada de una realización de ejemplo del terminal de acuerdo con la presente invención;
la figura 7 muestra esquemáticamente un Policy Domain (PD – Dominio de Política) de acuerdo con la presente invención; y
la figura 8 muestra un escenario de acceso mixto de acuerdo con la presente invención.

Descripción detallada

Las diferentes características de la invención se describirán ahora con referencia a las figuras, en las cuales partes similares están identificadas con los mismos caracteres de referencia. En la siguiente descripción, con el propósito de explicación y no de limitación, se establecen detalles específicos, tales como circuitos, componentes, técnicas, etc. particulares, con el fin de proporcionar un profundo conocimiento de la presente invención. No obstante, resultará evidente para un experto en la materia que la presente invención puede ser puesta en práctica en otras realizaciones que se separan de estos detalles específicos. En otros casos, se omiten descripciones detalladas de métodos, dispositivos y circuitos bien conocidos, con el fin de no oscurecer la descripción de la presente invención.

La presente invención describe un método de y un sistema para proporcionar itinerancia global independiente del acceso entre redes heterogéneas y resuelve el problema con la ejecución de políticas y transparencia de servicio en y entre redes diferentes. La solución contiene un número de características sobresalientes.

1) Una relación de cliente-servidor.
2) Una "línea de paquetes" transparente, que interconecta a servidores se interconexión y clientes con una cierta Calidad del Servicio.
3) Un Policy Definition Point (PDP - Punto de Definición de Política) asociado con o que reside en un grupo de servidores que definen políticas que pertenecen a servicios, validación, registro de operaciones de autorización, y
4) Un Policy Enforcement Point (PEP – Punto de Ejecución de Política), asociado con o que reside en el cliente, que ejecuta políticas definidas en el punto de definición de política, en el terminal (cliente).
5) Mecanismos de facturación separados para acceso y servicios, es decir, transacciones basadas en cliente-servidor.
6) Una transformación del nodo de acceso en un punto de venta para acceso, que ofrece un transporte de IP transparente.
7) Módulos de acceso de capa 1 y capa 2 eliminables (módems) e intercambiables para los clientes (terminales) para acceder a diferentes estándares de telefonía fija y móvil.

La solución de acuerdo con la invención se describirá también ahora con más detalle con referencias a las figuras 1a7.

La figura 1 muestra una representación esquemática de una arquitectura para itinerancia global de acuerdo con la invención. La arquitectura puede dividirse en un dominio de servicio (no-sombreado), y un dominio de transporte 140 (sombreado).

El dominio del servicio, que cubre las capas superiores, por ejemplo el modelo de OSI, consiste en un grupo de servidores llamado Secure Mobile Portal (SMP – Portal de Telefonía Móvil Seguro) 100 y un cliente, gobernado por un Local Policy Enforcement Point (LPEP - Punto de Ejecución de Política Local) 110 que reside en el cliente o terminal 120. Una línea de transporte de ejecución codificada segura 130 conecta el SMP 100 y el LPEP 110 en una relación de Cliente-Servidor. Esta línea está habilitada para el establecimiento de secretos compartidos entre el SMP 100 y el LPEP 110, contenidos en una política, que se utiliza para generar claves de codificación para los paquetes, por ejemplo, paquetes de IP (Internet Protocol – Protocolo de Internet). Puesto que cada paquete de IP está codificado con una única clave, es decir, un secreto compartido entre el proveedor del servicio y el comprador del servicio, cada paquete recibido por el SMP 100 se verá como una validación de facto del comprador del servicio o del abonado por el proveedor del servicio.

El SMP 100 actúa como un Policy Definition Point (PDP – Punto de Definición de Política) para las políticas de definición del LPEP 110 con respecto a servicios, registro de operaciones, movilidad y seguridad para el abonado. El LPEP 110 que reside en el cliente 120 ejecuta las políticas definidas en el SMP 100. Una característica de la arquitectura es que la facturación para transporte y servicios puede ser separada. Se puede pagar el transporte en tiempo real utilizando, por ejemplo, una tarjeta de prepago, tarjeta de crédito, tarjeta de monedero u otras. Se pueden pagar las transacciones en el dominio del servicio como siempre, por ejemplo, mediante factura, por ejemplo.

El dominio del transporte, que consiste en una red de núcleo 140 basada en IP y en redes de acceso basadas en IP tales como las designadas por el acrónimo CDMA 2000-, EDGE-, W-LAN-, W-CDMA- o redes fijas o de cable, paquetes de transportes del SMP 100 al LPEP 110. La parte de capa 1 y de capa 2 150 del cliente o terminal 120 también pertenece al dominio del transporte y es preferiblemente implementada como módulos intercambiables (módems) para diferentes estándares de acceso tales como W-CDMA, EDGE, CDMA 2000, W-LAN etc. El dominio del transporte no necesariamente añade valor a los paquetes, excepto que clasifica los paquetes de acuerdo con la Calidad del Servicio y transporta los paquetes al destino final, garantizando el acceso a recursos físicos donde sea apropiado.

Las diferentes redes de acceso en el dominio del transporte deben tener las interfaces y soporte apropiados acordados en las definiciones de Calidad de Servicio, una llamada línea de paquetes 130. La línea de paquetes 130 proporciona funciones de capa 1 y de capa 2 para transportar tráfico de datos a través de interfaces de radio o aérea, por ejemplo. Como parte del dominio del transporte, las redes de acceso deben también ser capaces de procesar la información de facturación en la realización de la invención en la que la facturación del transporte es independiente de la facturación del servicio. Esto es, donde la facturación del acceso es independiente de cualquier otra facturación, y se ve como una entidad separada. El dominio del transporte implica así medios para facturar a un abonado el transporte utilizado, por ejemplo, por medio de una tarjeta de prepago, tarjeta de crédito, tarjeta de monedero u otro medio. No es necesario que un abonado sea validado o autorizado por un proveedor de servicio antes de que tenga lugar la facturación del transporte. Sólo es necesario validar la tarjeta de prepago, tarjeta de

crédito, tarjeta de monedero u otros, es decir, es posible implementar métodos de pago anónimos para el transporte. Los proveedores de acceso pueden aceptar diferentes tipos de métodos de pago para el pago del transporte; por ejemplo algunos proveedores de acceso pueden aceptar todas las principales tarjetas de crédito y su propia tarjeta de monedero especial para pagar el acceso a sus redes. Esto puede compararse a cuando los comercios tienen una pegatina en la entrada informando de qué tarjetas de crédito aceptan, por ejemplo.

La figura 2 es una realización de ejemplo de un método de pago anónimo mostrado. El terminal 120 transmite un canal de acceso aleatorio (en GSM, típicamente el RACCH) que incluye información de pago 200 a un nodo de acceso 210. La información de pago identifica el Credential Verifier (CV – Verificador de Credencial) 220, por ejemplo el emisor de una tarjeta de crédito o una suscripción de acceso, la identidad del abonado en una forma codificada y la verificación del crédito en una forma codificada, por ejemplo un número de tarjeta de crédito. Esta información es recibida en el nodo de acceso 210, que lee la dirección al CV 220, añade un número de transacción a la identidad del usuario y la verificación del crédito, y transmite esa información 230 al CV 220 identificado, por ejemplo un servidor de MasterCard®. El CV 220 descodifica los paquetes enviados desde el nodo de acceso 210 con claves únicas para ese abonado particular y comprueba si la identidad del usuario y el número de verificación del crédito son correctos. De esta manera el abonado puede ser identificado de manera única, y así, validado. Si la relación entre la identidad del usuario y la verificación del crédito es correcta el CV 220 devuelve un mensaje con el mismo número de transacción y un reconocimiento 240 positivo al nodo de acceso 210. El nodo de acceso devuelve a continuación un mensaje 250 a una interfaz módem/encaminador contenida en el terminal 120, que contiene una dirección de IP y un reconocimiento positivo, facilitando el acceso. La dirección de IP es almacenada en la interfaz módem/encaminador y en el LPEP 110 y está asociada con un servicio solicitado por el abonado en las capas de servicio 260.

La estructura y operación de una realización de ejemplo del LPEP 110 residentes en el cliente o terminal 120 se describirá ahora con más detalle con referencia a la figura 3 de los dibujos. Como se ha explicado anteriormente, el LPEP 110 ejecuta políticas con respecto a la validación de abonados, autorización de acceso y a servicios, registro de operaciones, movilidad y seguridad para el abonado o los abonados a los cuales proporciona servicio el LPEP 110. Estas políticas están definidas en el SMP 100 que actúa como un PDF y la relación entre el PDP y el LPEP 110, es decir, entre el SMP 100 y el abonado está definida de manera única mediante estas políticas en la base de datos 300 de autorización de LPEP.

Cada relación que el abonado tiene con los SMPs 100 o con los CVs 220 está definida con varios parámetros 310. En la realización mostrada al menos se han definido cuatro parámetros. Estos son obligaciones, derechos, y un secreto compartido, es decir, una identidad única y una clave de codificación, y una dirección de IP para el SMP 100 ó el CV 220. Estas relaciones son negociadas bien en tiempo real utilizando una infraestructura de clave pública o mediante la contratación de un servicio y la recepción de las obligaciones, derechos, secreto compartido y dirección de IP 310 para el SMP 100 ó el CV 220 por correo electrónico, por ejemplo.

El LPEP 110 es también responsable de validación del abonado por medio, por ejemplo, de un código PIN o un lector de huella. Si el abonado es autorizado obtiene acceso al LPEP 110. Es posible que el LPEP 110 proporcione servicio a más de un abonado, entonces la base de datos 320 de validación almacena varios abonados A, B,… 330 y sus claves de identificación correspondientes clave 1, clave 2,… 340. La clave de LPEP 350 por otro lado se utiliza para identificar al LPEP 110 al SMP 100 y para la codificación del tráfico entre el LPEP 110 y el SMP 100 ó CV 220.

Durante una sesión de comunicación el LPEP 110 mantiene un informe de registro de operaciones 360 que contiene información de registro de operaciones 370 que pertenece a la sesión, tal como momento de inicio, momento de finalización y servicio utilizado. Este informe de registro de operaciones 360 puede ser utilizado por el SMP 100 para propósitos de tarificación y de auditoría. Al completarse la sesión el LPEP 110 puede enviar el informe de registro de operaciones 360 al SMP 100 y el SMP 100 contesta en acuerdo o en desacuerdo, es decir, compara el informe de registro de operaciones en el SMP 100 con el generado en el LPEP 110. Alternativamente el informe de registro de operaciones 360 es transmitido desde el LPEP 110 al SMP 100 a intervalos regulares, tal como el final del día.

Con referencia ahora a la figura 4 de los dibujos, la estructura y operación de una realización de ejemplo del SMP 100 se describirá con más detalle. Como se ha explicado anteriormente, el SMP 100 define políticas con respecto a la validación de abonados, la autorización para el acceso y los servicios, registro de operaciones, movilidad y seguridad para los abonados a los que el SMP 100 proporciona servicio. Así, el SMP 100 contiene un Encrypted Subscriber Register (ESR – Registro de Abonado Codificado 400 que lleva direcciones de IP de abonado o network address identifiers (NAI – Identificadores de Dirección de Red), por ejemplo, n.n@telia.mob, así como claves de codificación para cada abonado y servicio individual al que el SMP 100 proporciona servicio. Esto, para proporcionar codificación, validación y autorización a los servicios proporcionas. El SMP 100 también contiene un Global Location Register (GLR – Registro de Ubicación Global) 410 que indica en qué redes de acceso está residiendo (visitando) el abonado actualmente. Para ser capaz de proporcionar servicios de voz el SMP 100 contiene también un servidor de voz 420 para proporcionar por ejemplo voz sobre IP. El SMP 100 puede considerarse como un grupo de servidores que proporcionan servicios tanto seguros como no seguros al abonado; servicios seguros como el comercio

electrónico 430, alarmas de seguridad, servicios de salud, etc. y servicios no seguros como navegación por la red 440 y servicios de catálogo/información 450, por ejemplo. El SMP 100 contiene también un servidor de registro de operaciones seguro 460 para el registro de operaciones y la auditoria de registros. El SMP 100 también puede actualizar las políticas en el LPEP 110. Por ejemplo si el abonado no paga las facturas para un servicio particular, ese servicio puede ser bloqueado.

Con referencia ahora al diagrama de señalización de ejemplo mostrado en la figura 5 de los dibujos, la iniciación de una sesión se describirá con más detalle. Para iniciar una sesión un abonado 580 transmite una solicitud de validación 500 que incluye la identidad de un abonado y una clave correspondiente, por ejemplo un personal identification number (PIN – Número de Identificación Personal) o una huella, para obtener acceso al terminal y los derechos del LPEP 110. Cuando el abonado 580 recibe una respuesta de validación 505 indicando que el abonado 580 está validado para utilizar el terminal, una solicitud de servicio 510 es transmitida al LPEP 110. El LPEP 110 decide acerca de un acceso adecuado dependiendo del servicio solicitado por el abonado y transmite una solicitud de acceso 515 identificando el abonado y la correspondiente información de pago 520, todo, excepto la dirección al CV codificado mediante la clave del LPEP, hasta la red de acceso 585 elegida. La red de acceso 585 lee la solicitud de pago e identifica la dirección al Credential Verifier (CV – Verificador de Credencial) 220, genera un número de transacción y añade la solicitud de pago, es decir, la identidad del usuario en una forma codificada y la verificación del crédito en una forma codificada, por ejemplo un número de tarjeta de crédito, y transmite el mensaje 525 al CV 220. El CV 220 descodifica el mensaje y si la relación entre la identidad del usuario y la verificación del crédito es correcta, el CV transmite un mensaje con el mismo número de transacción y verifica las credenciales del abonado 530. La red de acceso 585 transmite un OK al acceso 535 junto con una dirección de IP al LPEP 110 y al mismo tiempo la red de acceso 585 transmite un mensaje 540 al SMP 100 indicando en qué red está residiendo el abonado 580. El LPEP 110 reconstruye 545 a continuación el servicio 510 requerido en el SMP 100 y el abonado 580 y el SMP llevan a cabo una sesión 550. El LPEP 110 y el SMP 100 monitorizan 555 todas las transacciones entre el LPEP 110 y el SMP 100 para propósitos de registro de operaciones. Para finalizar la sesión el abonado 580 transmite un mensaje de finalización de sesión 560 al LPEP 110 que transmite un mensaje de finalizar la sesión 565 al SMP 100. Cuando la sesión ha finalizado el LPEP 110 envía una solicitud de registro de operaciones 570 al SMP 100 que la compara con la solicitud de registro de operaciones generada en el SMP 100 y devuelve una confirmación de registro de operaciones negativa 575 al LPEP 110.

Con referencia a la figura 6, las realizaciones y funciones del cliente o terminal se describirán con más detalle. El terminal está básicamente separado en tres partes, una parte de acceso, una parte de control y una parte de servicio. La parte de acceso contiene un número de opciones de acceso (módems) 600a-c. Estas opciones de acceso pueden físicamente estar situadas en el propio terminal o en el terminal de alguien más, o ser una interfaz de Bluetooth® que se conecta a módems remotos, por ejemplo en el maletín del abonado. La parte de servicio contiene una interfaz de usuario y application programming interfaces (API's - Interfaces de programación de aplicación) aplicables para los servicios. La parte de control contiene un motor de ejecución de política 610 y un depósito de política 620.

El terminal contiene también un conmutador de IP de capa 2 630 y un encaminador de IP de capa 3 640 entre los módems 600a-c y la interfaz 650 de aplicaciones. Esto permite al usuario 660 la posibilidad de tener varios flujos de información entre aplicaciones 670 y módems 600a-c activos al mismo tiempo. Por ejemplo, ¿puede mantenerse un flujo de datos de voz sobre IP a través de una red de W-CDMA, al mismo tiempo que se mantiene un flujo de multimedios a través de una red W-LAN, mientras el terminal está recibiendo al mismo tiempo un flujo de mejor esfuerzo desde otro terminal, a través de un módem de Bluetooth®? Esta posibilidad de encaminar una pluralidad de flujos de datos desde una pluralidad de módems 600a-c es posible debido al conmutador de IP 630 de capa 2 incluido, y al encaminamiento de IP 640 de capa 3. Esta realización también hace posible que el terminal transmita una sesión de comunicación desde una red de comunicación a otra, re-encaminando el flujo de datos desde un puerto de módem a otro.

La función de descubrimiento de acceso 680 del terminal está activa continuamente, rastreando los alrededores para posibilidades de acceso y genera un registro de todas las posibilidades de acceso disponibles. La función de selección de acceso 690 es responsable de solicitar acceso y presentar credenciales a la red de acceso deseada, dependiendo del servicio solicitado de las capas de servicio y también de preparar la interconexión con la red de acceso elegida.

El motor de ejecución de política 610 y el depósito de política 620 en la parte de control conecta los módems 600a-c en la parte de acceso con el usuario 660 y las API's en la parte de servicio. Más específicamente el motor de ejecución de política 610 en la parte de control tiene la responsabilidad de una variedad de tareas tales como la validación del usuario 660 para el terminal, la autorización del usuario 660 para servicios y la obtención de datos de registro de operaciones. Estas y otras tareas se describirán también en relación con la figura 8.

El depósito de política 620 del terminal puede considerarse como una base de datos que contiene la relación del abonado con los proveedores de acceso, los proveedores de servicio, así como con clientes individuales, es decir

las obligaciones, derechos, secretos compartidos y direcciones a verificadores de credencial o SMP's. Estas relaciones pueden variar y ser, en ocasiones, extremadamente complejas. También, estas relaciones pueden necesitar ser actualizadas en cualquier momento.

Algunos proveedores de servicio pueden por ejemplo, tener una relación jerárquica entre diferentes aspectos de sus servicio. Por ejemplo, una red de acceso especial o una puerta de enlace especial pueden necesitar ser utilizadas o pasadas antes de que se pueda ejecutar un servicio particular, y quizás deberá reconstruirse una relación fiable para una sesión particular. Otro proveedor de servicio podría ser no jerárquico, lo que significa que los diferentes servicios están abiertos y reconstruidos al mismo nivel, por ejemplo donde puede utilizarse cualquier red de acceso.

Un abonado puede tener una relación con muchas estructuras diferentes, jerárquica y plana. Por ejemplo, el abonado A tiene una suscripción privada con el proveedor X para voz y navegación por la Red. Bajo el servicio de voz, el abonado A se comunica siguiendo una política específica con el abonado B. El abonado A también tiene una relación de negocios específica con el abonado C, de manera que todos los paquetes hacia el abonado C serán codificados y directamente transferidos al abonado C. Además de este contrato privado con el proveedor X y su relación ocupacional con el abonado, el abonado A también puede ser un miembro de un club de negocios exclusivo que opera un servidor del club. Esta tasa de pertenencia a un club proporciona al abonado A servicios de tráfico de voz y de datos codificados a todos los demás miembros del club de negocios. El banco en el cual tiene una cuenta el abonado A puede también operar un servidor de su propiedad, y puede haber desplegado una política en el terminal del abonado A, de manera que siempre tiene acceso a su cuenta bancaria, incluso a media noche. Tanto el banco como el club de negocios necesitan comprar el servicio de algún MSP, con el fin de conocer el paradero del abonado A, esto es, a menos que los propios banco o club de negocios operen en MSP. Todas estas relaciones se reflejan en el depósito de política 620.

Cada relación en la que un usuario 660 ó abonado les gustaría entrar está definida utilizando un número de al menos tres o cuatro parámetros. Estos son derechos, obligaciones, secreto compartido y dirección hasta un verificador de credencial o SMP, creando así un bloque de política. El depósito de política 620 contiene varios bloques de política que definen las relaciones que existen entre el usuario 660 y diferentes proveedores de servicio así como individuales.

Al depósito de política 620 puede accederse desde el exterior 695 del terminal siempre que el usuario haya abierto el depósito de política 620, por ejemplo un código de identificación personal, una lectura de huella u otro medio. Entonces, un proveedor de servicio puede actualizar su bloque de política y sus coeficientes de acoplamiento relevantes. Una vez que el proveedor del servicio ha introducido sus políticas en el depósito de política 620 éstas pueden ser actualizadas a voluntad por el proveedor del servicio, siempre que tal acuerdo exista. Si tal acuerdo no existe el abonado debe abrir el depósito de política 620 cada vez, antes de que puedan hacerse cambios.

El motor de ejecución de política 610 ejecuta así políticas definidas en depósitos de política 620. Esto implica, por ejemplo, que pueden proporcionarse alquiler de coches, habitaciones de hotel, etc. con motores de ejecución de política 610 que ejecutan las políticas en un depósito de política 610 de un usuario o de un visitante. Tanto el motor de ejecución de política 610 como el depósito de política 620 están preferiblemente implementados como programas de ordenador u otro medio adecuado, por ejemplo, tarjetas inteligentes junto con un producto de acceso inalámbrico adecuado tal como el Bluetooth®. Otras implementaciones son, por supuesto, posibles, por ejemplo circuitos integrados, una tarjeta de circuito en el terminal o como una tarjeta de circuito separada que pueda ser insertada en cualquier terminal apropiado.

La figura 7 muestra un llamado Policy Domain (PD – Dominio la política) y subdominio. El dominio de política contiene múltiples bloques de política 625 que contienen todas las relaciones específicas que existen entre el usuario y los proveedores de servicio, así como individuales. Cada dominio de política puede contener subdominios 635 que definen un espacio de dominio reservado para una aplicación particular.

Una matriz de acoplamiento está definida entre los bloques de política, definiendo su relación jerárquica. Las relaciones entre los bloques de política xi, yj y los bloques de política xk, yl se determinan mediante un coeficiente de acoplamiento K, ij, kl. Si el coeficiente de acoplamiento es 0, entonces no existe ninguna relación. Si el coeficiente de acoplamiento es +1, entonces el bloque k, l es dependiente del bloque i, j, lo que implica que el bloque i, j tiene una posición superior en la jerarquía que el bloque k, l, y el bloque i, j debe ser reconstruido antes que el bloque k, l.

Si el coeficiente de acoplamiento es -1, entonces el bloque k, l desbanca al bloque i, j, implicando que el bloque i, j tiene una posición más baja en la jerarquía que el bloque k, l.

Con referencia ahora tanto a la figura 6 como a la 8, las tareas de la parte de control del terminal se describirán con más detalle junto con un escenario de acceso mixto. Supóngase que las posibilidades de acceso consisten en varias redes diferentes, tales como W-CDMA 700, EDGE 705, GPRS 710, CDMA-2000 715, W-LAN 720 ó Fija o de Cable 725 y que la red de transporte es una red de núcleo 730 basada en IP. Para obtener el acceso a las funciones del

terminal y al motor de ejecución de política 610 y al depósito de política 620 el usuario 660 debe ser validado. Así, una solicitud de validación es transmitida al motor de ejecución de política 610 que comprueba la validación con los bloques de política relevantes en el depósito de política 620. Cuando el usuario 660 es validado todos los derechos y obligaciones asociados con el usuario en el depósito de política 620 están abiertos.

La función de descubrimiento de acceso 680, que está continuamente activa, ha rastreado todas las redes de acceso disponibles y encontrado las posibilidades de acceso 700-725 mencionadas anteriormente, y hecho un registro de lo que está disponible. El usuario 660 ahora, por ejemplo desea iniciar un servicio de Red y por consiguiente por medio del acuerdo de parámetros de la interfaz de aplicaciones 650, es decir, algún valor de Calidad de Servicio para la sesión, por ejemplo, la velocidad de transmisión. La interfaz de aplicaciones 650 pide a continuación al motor de ejecución de política 610 que reconstruya el servicio de Red solicitado. El motor de ejecución de política 610 obtiene a continuación datos del depósito de política 620 y de la función de selección de acceso 690 para establecer un canal que cumpla con los parámetros acordados y con el servicio solicitado y a continuación activa la conexión.

Si el usuario 660 no tiene un contrato para la red solicitada, el motor de ejecución de política 610 presenta credenciales al proveedor de acceso apropiado. Las credenciales pueden ser, por ejemplo, una tarjeta de crédito aceptada por el proveedor del acceso. El motor de ejecución de política 610 lanza a continuación el servicio de Red solicitado de acuerdo con las políticas en el depósito de política 620. El motor de ejecución de política 610 rastrea los datos intercambiados durante el servicio de Red ejecutado de acuerdo con políticas para propósitos de registro de operaciones y de verificación. Entonces el motor de ejecución de política 610 desconecta la aplicación 670 y reúne los datos de registro de operaciones.

Existe otra posibilidad si el terminal no tiene el módem apropiado 600a-c para la mejor red de acceso. Imagínese por ejemplo que la red de GPRS 710 es la más adecuada para el servicio de Red solicitado pero que el terminal de usuario sólo tiene una interfaz de W-CDMA. La solución es el módem de Bluetooth® 740 a-b unido al terminal, lo que hace posible utilizar los módems 600a-c de un terminal vecino. El módem de Bluetooth® 740a-b en el terminal vecino actúa entonces como un punto de acceso o puente para acceder al módem de GPRS del otro terminal.

El usuario o abonado físico posee el PEP. El contenido del PEP puede pertenecer a muchos participantes. El abonado controla el acceso al PEP, y puede delegar estos derechos a otro participante, por ejemplo un operador u otro proveedor de servicio. Al PD y a sus sub-dominios se puede acceder desde fuera, siempre que el usuario inicialmente abra el PD (mediante un PIN de apertura de tarjeta o por otro medio). El proveedor de servicio puede introducir su bloque de política, así como los factores de acoplamiento relevantes que definen la relación entre las políticas del operador del servicio. Una vez que el proveedor del servicio ha introducido sus políticas en el PEP, éstas pueden ser actualizadas a voluntad por el proveedor del servicio, siempre que tal acuerdo exista. Si no existe tal acuerdo, entonces el PD debe ser abierto cada vez por defecto, por ejemplo.

El LPEP puede ser realizado físicamente de muchas maneras diferentes. Puede estar incluido en un terminal de telefonía móvil, puede ser parte de un equipo de terminación de red en la residencia, puede ser una placa separada que puede ser insertada en cualquier terminal apropiado cuando el usuario desea hacer una llamada, o puede ser una tarjeta de PEP separada encapsulada junto con un producto de acceso inalámbrico adecuado (tal como un Bluetooth®). El PEP puede comunicarse con el cliente que el abonado desea utilizar para comunicarse de acuerdo con los principios definidos anteriormente.

REIVINDICACIONES

1. Un sistema de comunicación para proporcionar itinerancia global independiente del acceso que incluye al menos dos redes de comunicación que son heterogéneas entre sí, al menos un terminal (120) para intercambiar información con al menos dos redes de comunicación que son heterogéneas entre sí, al menos un punto de definición de política (100) que forma una relación de cliente-servidor con el citado al menos un terminal (120), al menos un punto de ejecución de política (110) que ejecuta políticas definidas en el citado punto de definición de política (100), **caracterizado porqu**e el citado al menos un punto de ejecución de política (110) está situado en el citado al menos un terminal (120) y **porque** las citadas políticas pertenecen a servicios, validación, autorización y registro de operaciones.

2. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de definición (100) incluye medios para definir las citadas políticas.

3. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de ejecución de política (110) incluye medios (610, 620) para ejecutar las citadas políticas.

4. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** la citada relación de cliente-servidor está realizada mediante una línea de paquetes (130) transparente que transporta y clasifica paquetes de acuerdo con la Calidad del Servicio.

5. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado al menos un terminal (120) soporta simultáneamente relaciones de cliente-servidor independientes en curso.

6. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de definición de política (100) incluye medios para definir políticas en otros grupos de servicios diferentes del suyo propio.

7. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de ejecución de política (110) incluye medios (610, 620) para ejecutar una pluralidad de políticas que emanan de una pluralidad de redes y de proveedores de servicio.

8. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de de definición de política (100) está implementado mediante un medio de código de software.

9. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de de ejecución de política (110) está implementado mediante medios de código de software.

10. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de definición de política (100) incluye un registro de ubicación global (410) que indica en qué red de acceso reside el citado al menos un terminal (120).

11. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado punto de definición de política (100) incluye también una base de datos de abonado (400) que incluye medios para almacenar direcciones de IP de abonado y claves de codificación para cada uno de los citados abonados.

12. Un sistema de comunicación de acuerdo con la reivindicación 1, **caracterizado porque** el citado sistema de comunicación incluye un verificador de credencial que proporciona medios para el pago anónimo del acceso para al menos una de las citadas redes heterogéneas entre sí.

13. Un método para la itinerancia global en un sistema de comunicación que incluye al menos dos redes de comunicación que son heterogéneas entre sí, al menos un terminal (120) para intercambiar información con al menos dos redes de comunicación que son heterogéneas entre sí, formando al menos un punto de definición de política (100) una relación de cliente-servidor con el citado al menos un terminal (120), estando el método caracterizado por políticas de ejecución definidas en el citado punto de definición de política (100) en un punto de ejecución de política (110) en el citado al menos un terminal (120) y perteneciendo las citadas políticas a servicios, validación, autorización y registro de operaciones.

14. El método de la reivindicación 13, caracterizado por definir las citadas políticas en el punto de definición de política (100).

15. El método de la reivindicación 13, caracterizado por ejecutar las citadas políticas en el citado punto de ejecución de política (110) definido en el citado punto de definición de política (100).

16. El método de la reivindicación 13, caracterizado también porque la citada relación de cliente-servidor se proporciona transportando y clasificando paquetes de acuerdo con la Calidad del Servicio.

17. El método de la reivindicación 13, caracterizado también porque el punto de definición de política (100) está definiendo políticas en otros grupos de servidores diferentes del suyo propio.

18. El método de la reivindicación 13, caracterizado por almacenar en el citado punto de definición de política (100) en un registro de ubicación global en qué red de acceso reside el citado al menos un terminal (120).

19. El método de la reivindicación 13, caracterizado por almacenar en el citado punto de definición de política (100) direcciones de IP del abonado y claves de codificación para cada uno de los citados abonados.

20. Un terminal de telefonía móvil (120) que está adaptado para llevar a cabo itinerancia global independiente del acceso al menos a dos redes de comunicación que son heterogéneas entre sí, **caracterizado porque** el citado terminal de telefonía móvil (120) comprende:

- medios para recibir una política desde un punto de definición de política (100) en una relación de cliente-servidor,
- un punto de ejecución de política (110) que ejecuta políticas definidas en el citado punto de definición de política (100),
- las citadas políticas pertenecientes a servicios, validación, autorización y registro de operaciones.

21. El terminal de telefonía móvil (120) de acuerdo con la reivindicación 20, incluyendo el citado terminal (120) medios (610, 620) para ejecutar las citadas políticas.

22. El terminal de telefonía móvil (120) de acuerdo con la reivindicación 20 ó 21, **caracterizado porque** la citada relación de cliente-servidor está realizada mediante una línea de paquetes (130) transparente que transporta y clasifica paquetes de acuerdo con la Calidad del Servicio.

23. El terminal de telefonía móvil (120) de acuerdo con la reivindicación 20, 21 ó 22, **caracterizado porque** el citado terminal (120) soporta simultáneamente relaciones de cliente-servidor independientes en curso.

24. El terminal de telefonía móvil (120) de acuerdo con cualquiera de las reivindicaciones 20 a 23, **caracterizado porque** el citado punto de ejecución de política (110) incluye medios (610, 620) para ejecutar una pluralidad de políticas que emanan de una pluralidad de proveedores de redes y de servicios.

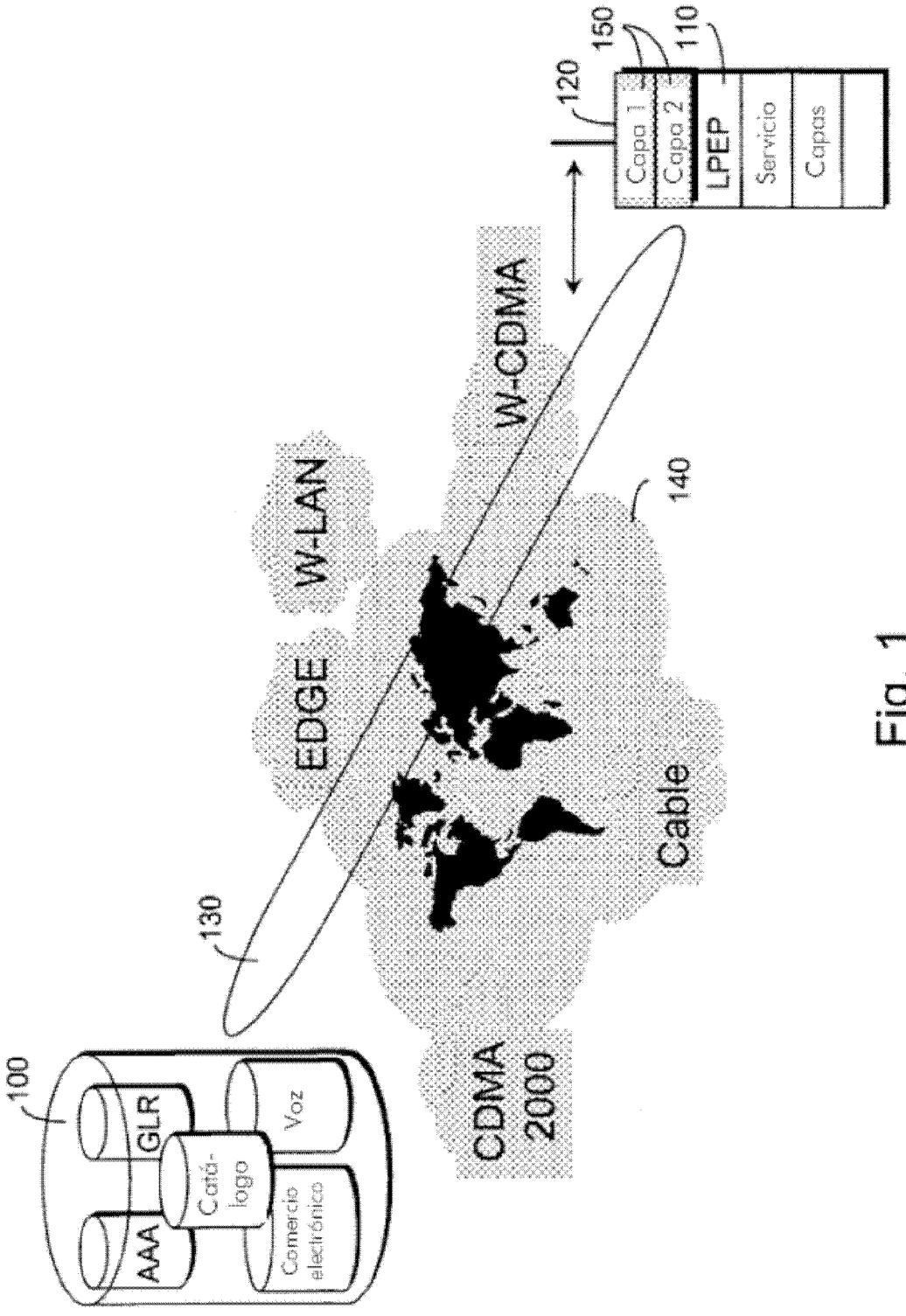
100
GLR
AAA
Catá-
logo
Voz
Comercio
electrónico
130
CDMA
2000
EDGE
W-LAN
W-CDMA
Cable
140
120
150
110
Capa 1
Capa 2
LPEP
Servicio
Capas

Fig. 1

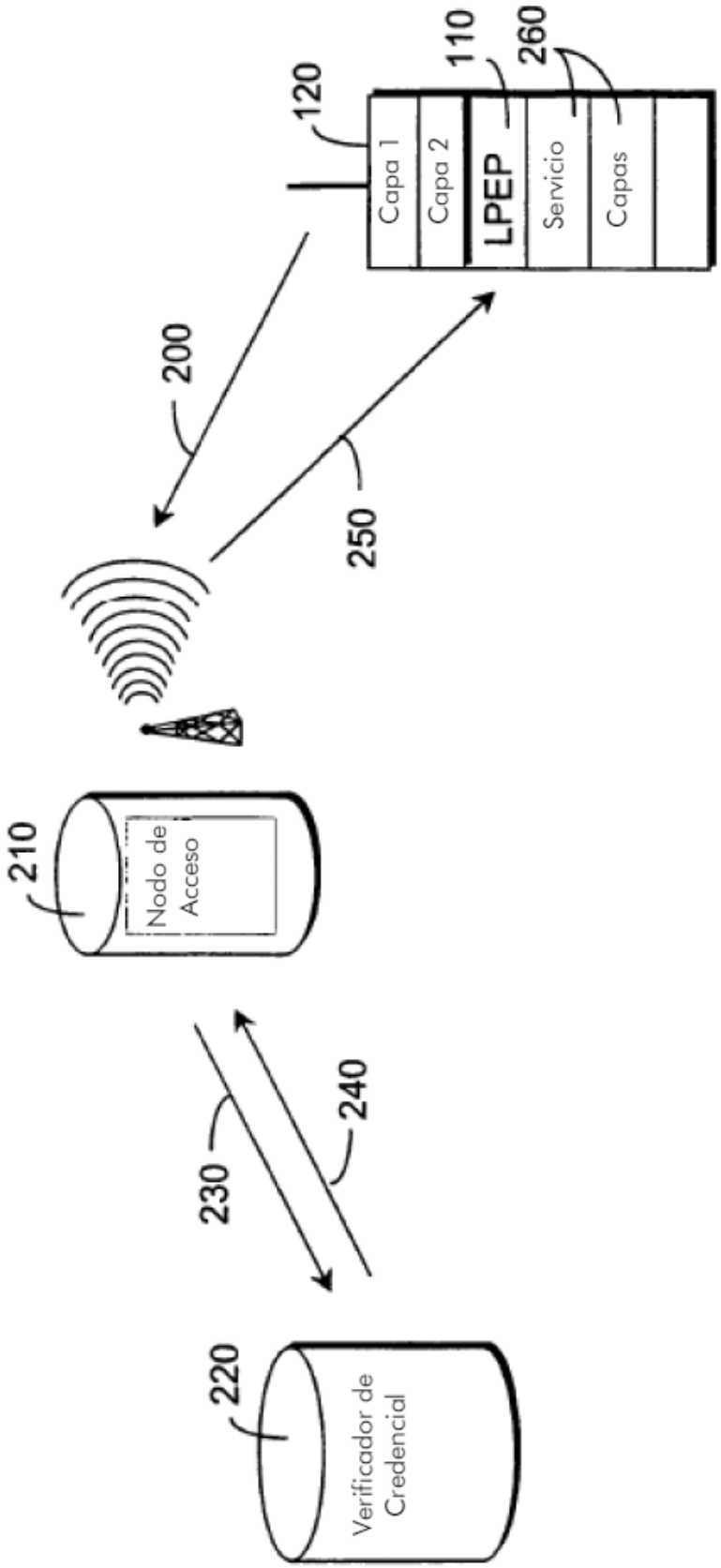
120
110
260
Capa 1
Capa 2
LPEP
Servicio
Capas
200
250
210
Nodo de Acceso
230
240
220
Verificador de Credencial

Fig. 2

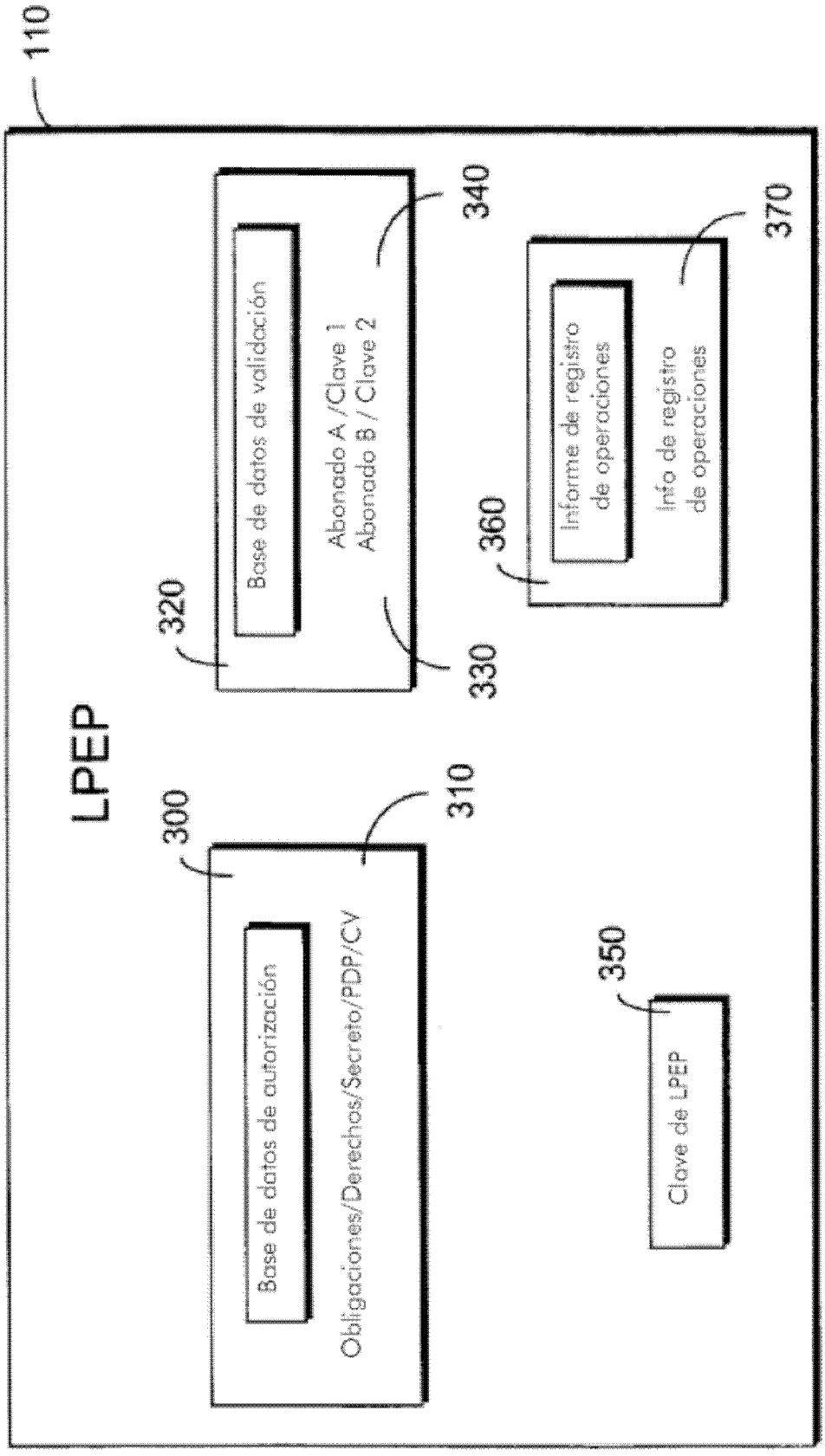
110
LPEP
300
Base de datos de autorización
Obligaciones/Derechos/Secreto/PDP/CV
310
320
Base de datos de validación
Abonado A /Clave 1
Abonado B / Clave 2
330
340
350
Clave de LPEP
360
Informe de registro de operaciones
Info de registro de operaciones
370

Fig. 3

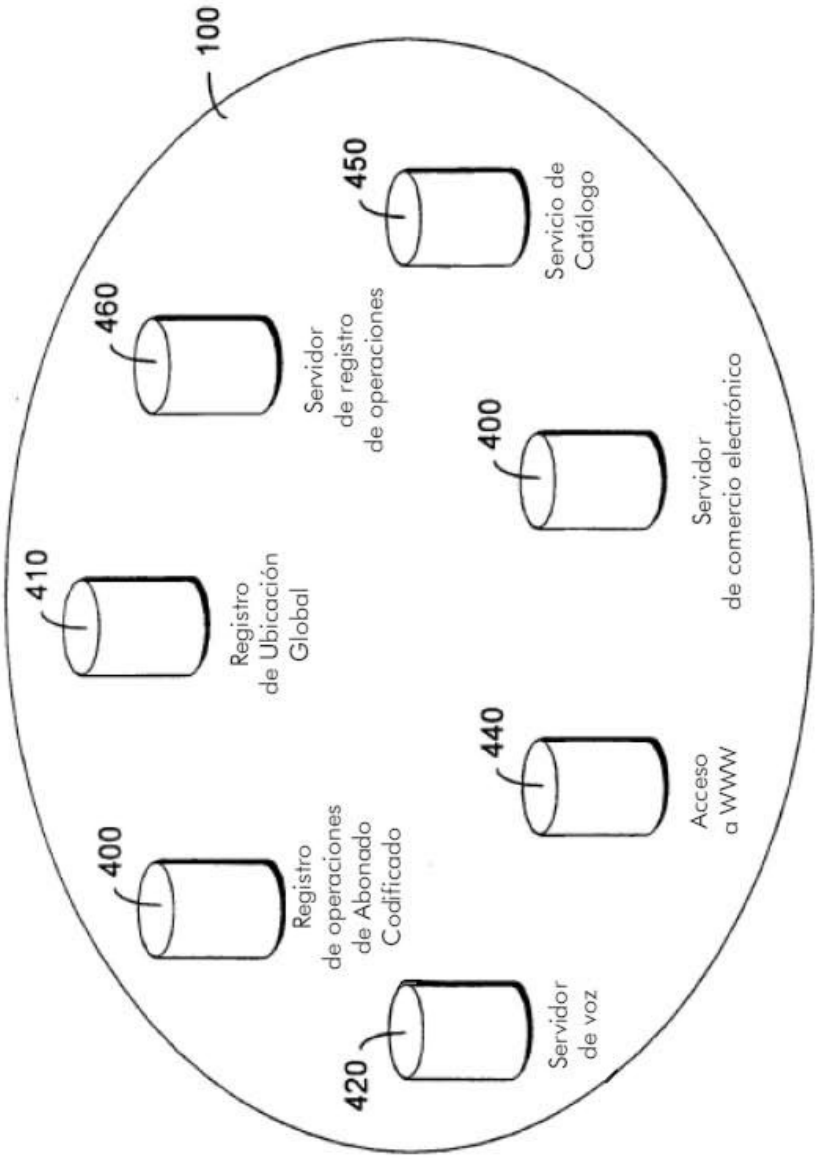
100
450
Servicio de Catálogo
460
Servidor de registro de operaciones
400
Servidor de comercio electrónico
410
Registro de Ubicación Global
440
Acceso a WWW
400
Registro de operaciones de Abonado Codificado
420
Servidor de voz

Fig. 4

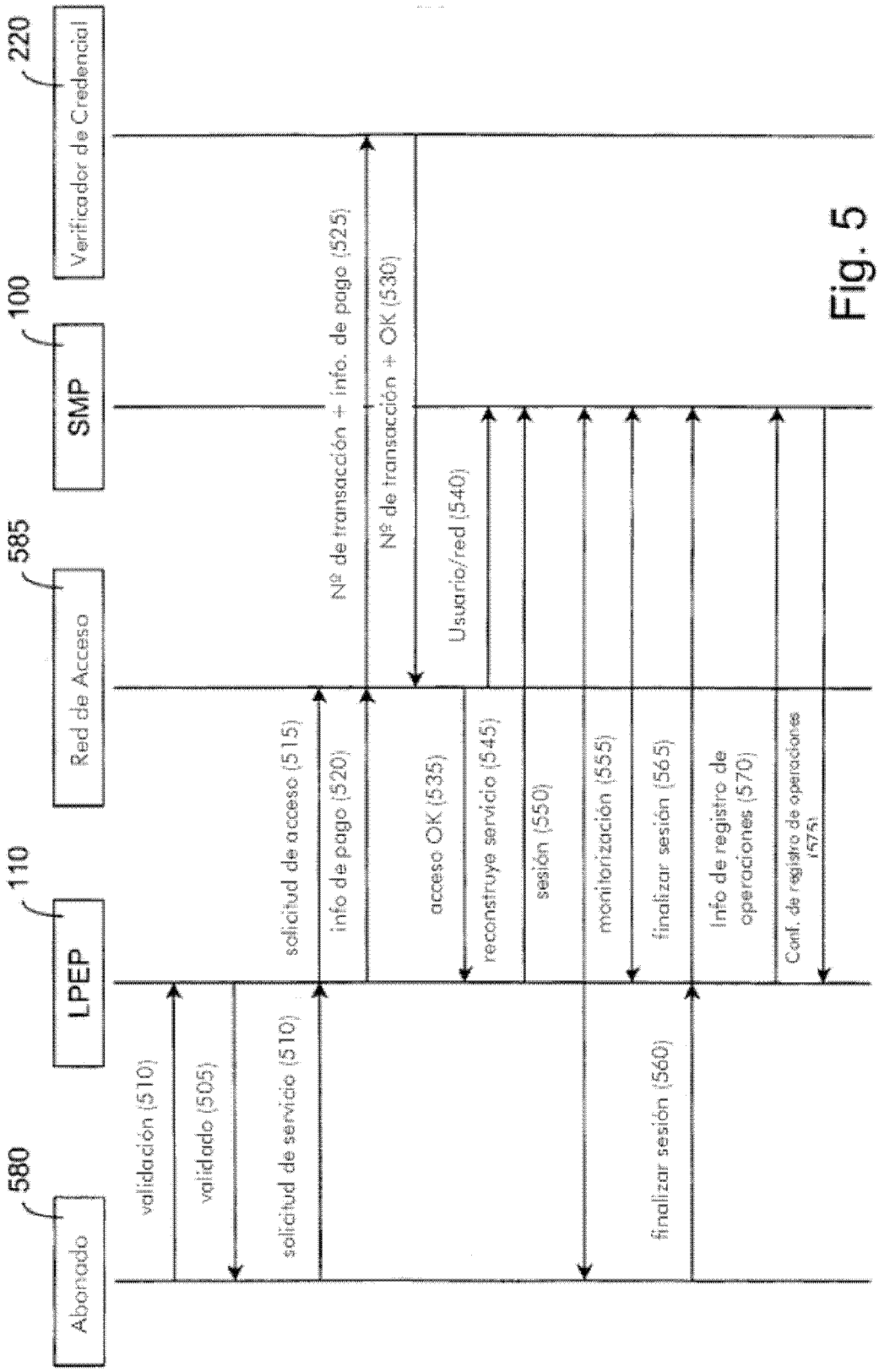
580
Abonado
110
LPEP
585
Red de Acceso
100
SMP
220
Verificador de Credencial
validación (510)
validado (505)
solicitud de servicio (510)
solicitud de acceso (515)
info de pago (520)
Nº de transacción + info. de pago (525)
acceso OK (535)
Nº de transacción + OK (530)
reconstruye servicio (545)
Usuario/red (540)
sesión (550)
monitorización (555)
finalizar sesión (565)
info de registro de operaciones (570)
Conf. de registro de operaciones (575)
finalizar sesión (560)

Fig. 5

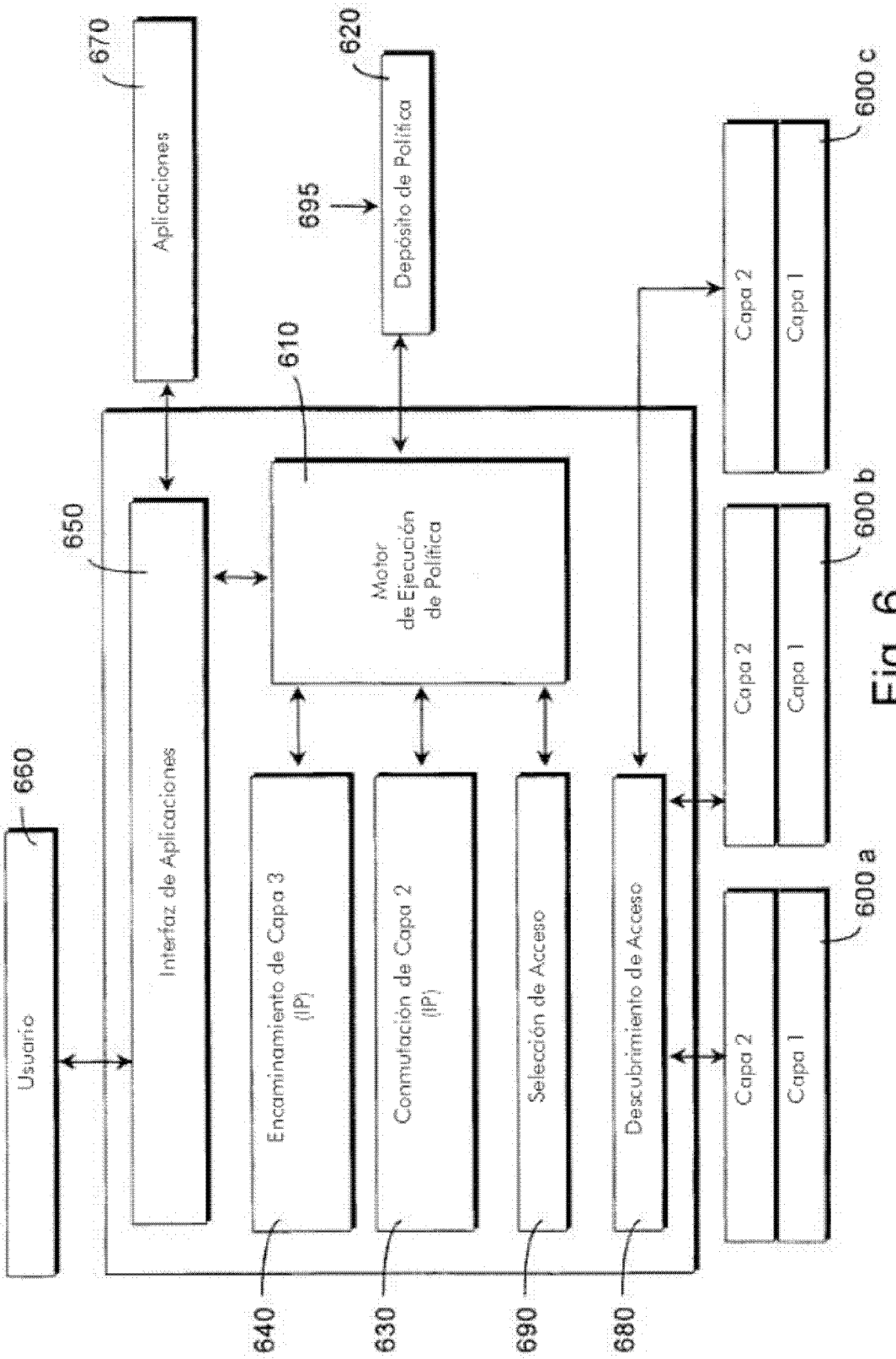
670
Aplicaciones
620
Depósito de Política
695
610
650
Motor de Ejecución de Política
Interfaz de Aplicaciones
660
Usuario
Encaminamiento de Capa 3 (IP)
Conmutación de Capa 2 (IP)
Selección de Acceso
Descubrimiento de Acceso
640
630
690
680
Capa 2
Capa 1
600 c
600 b
600 a

Fig. 6

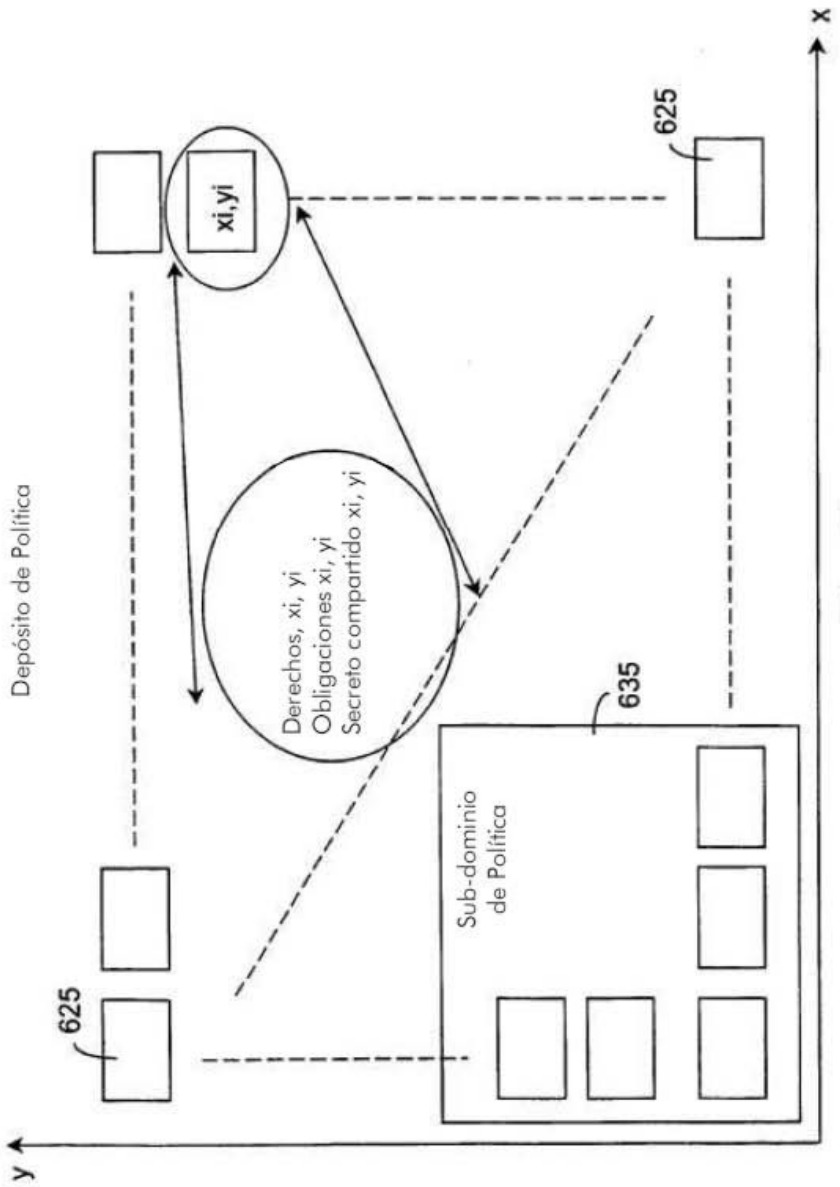
x
y
Depósito de Política
xi,yi
625
625
Derechos, xi, yi
Obligaciones xi, yi
Secreto compartido xi, yi
635
Sub-dominio
de Política

Fig. 7

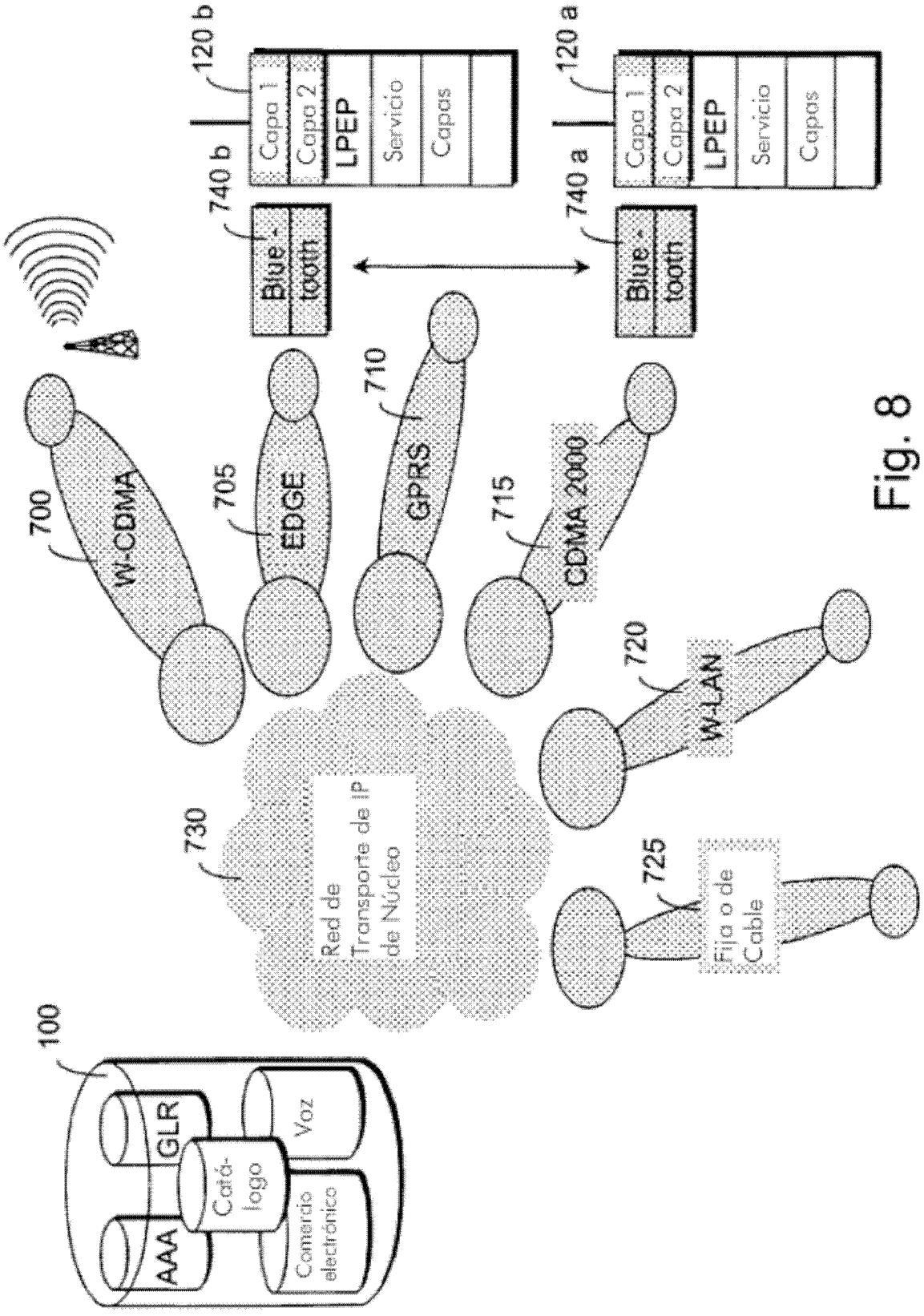
120 b
120 a
Capa 1
Capa 2
LPEP
Servicio
Capas
740 b
740 a
Blue-tooth
700
W-CDMA
705
EDGE
710
GPRS
715
CDMA 2000
720
W-LAN
725
Fija o de Cable
730
Red de Transporte de IP de Núcleo
100
AAA
GLR
Catá-logo
Voz
Comercio electrónico

Fig. 8