(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 665 875**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 4/24 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.12.2004 PCT/EP2004/053383**

(87) Fecha y número de publicación internacional: **15.06.2006 WO06061049**

(96) Fecha de presentación y número de la solicitud europea: **09.12.2004 E 04804756 (7)**

(97) Fecha y número de publicación de la concesión europea: **24.01.2018 EP 1825648**

(54) Título: **Método de acceso en una WLAN para un teléfono móvil IP con autenticación mediante HLR**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2018

(73) Titular/es:

TOGEWA HOLDING AG (100.0%)
NUSSBAUMSTRASSE 25
3000 BERN 32, CH

(72) Inventor/es:

HEUTSCHI, WALTER;
STADELMANN, TONI y
ZBÄREN, PETER

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Método de acceso en una WLAN para un teléfono móvil IP con autenticación mediante HLR

La presente invención se refiere a un método y a un sistema para telefonía y videotelefonía basados en IP, en los que los nodos de IP se autentican sobre la base de datos de autenticación de un módulo de identificación antes del registro en la red basada en IP.

La telefonía basada en IP es una tecnología que se ha transformado en los últimos años en una alternativa real a la transmisión de voz tradicional en redes de telefonía basadas en línea. Mientras que las conversaciones telefónicas tradicionales se transmiten como un flujo de datos continuo a través de una red telefónica, en telefonía basada en IP, los datos de voz se dividen en paquetes y se transmiten individualmente a través de una red de datos. Después de dividir grandes volúmenes de información acústica y transmitirla a través de la red, estos pequeños paquetes se vuelven a ensamblar en el extremo receptor. De esta manera los servicios de telefonía se pueden combinar con la red de datos, eliminando así la instalación y el cuidado de una red telefónica separada ya que los teléfonos basados en IP se pueden conectar a una red de datos a través de una interfaz correspondiente, y los datos de voz se pueden transmitir por medio de protocolos de red adecuados. Otra ventaja importante de la comunicación telefónica basada en IP en comparación con la telefonía tradicional es la oferta de servicios novedosos que son posibles solo a través de la tecnología basada en IP y representan un valor añadido en comparación con la telefonía tradicional. Entre otros, la telefonía basada en IP ofrece encriptación automática de la comunicación de voz, lo que permite conversaciones seguras ante escuchas. Este desarrollo en la telefonía basada en IP también ha tenido un efecto en el desarrollo paralelo de la videotelefonía basada en IP como alternativa a la tecnología tradicional de videoconferencia. Los enlaces de datos, cada vez más rápidos, permiten en la actualidad la transmisión simultánea de vídeo y audio de excelente calidad. En la videotelefonía basada en IP, los datos de voz e imágenes se dividen en paquetes como en la telefonía basada en IP, se envían a través de una red basada en IP y después se reensamblan en el extremo receptor.

Al mismo tiempo, el veloz desarrollo de redes inalámbricas de datos (WLAN 802.11, Bluetooth, etc.) y un número cada vez mayor de los llamados puntos de acceso en la zona pública (por ejemplo, en aeropuertos, estaciones de tren, centros de conferencias, salas de exposiciones y convenciones, espacios de gran afluencia en las ciudades) han dado como resultado dispositivos con capacidad IP que en la actualidad tienen una movilidad comparable solo a la de las redes de telefonía móvil actuales (GSM, UMTS, etc.). El acceso inalámbrico a servicios como Internet ya se da por hecho en la actualidad. Además, los teléfonos móviles basados en IP han estado disponibles desde hace algún tiempo, lo que permite la telefonía móvil basada en IP a través de una red inalámbrica local. Estos teléfonos IP móviles ya existen en realizaciones con cámaras integradas, de manera que, igualmente, la videotelefonía móvil basada en IP está cada vez más próxima.

Para establecer la comunicación y el intercambio de datos en telefonía y/o redes de videotelefonía, deben mantenerse ciertos estándares por todos los componentes de la red que se definen en protocolos o familias de protocolos. Por ejemplo, el protocolo E-DSS1 (Euro-ISDN) se conoce en el estado de la técnica para redes de telefonía de conmutación de circuitos, o se conocen los protocolos H.323, SIP, MEGACO o bien MGCP para telefonía y/o videotelefonía basada en IP.

Uno de los protocolos más utilizados para telefonía y/o videotelefonía basada en IP es el Protocolo de inicio de sesión (SIP, IETF RFC 3261, anteriormente RFC 2543). Esta especificación fue desarrollada por primera vez en mayo de 1999 por el Grupo de Trabajo de Ingeniería de Internet (IETF). Este protocolo de red tiene una estructura muy ligera y se basa en gran medida en HTTP (Protocolo de transferencia de hipertexto). Este protocolo permite establecer una sesión de comunicación entre dos o más participantes. Sin embargo, se trata estrictamente un protocolo de iniciación. Los sistemas de telefonía y/o videotelefonía basados en SIP utilizan otros protocolos, en particular SDP (Protocolo de descripción de sesión, IETF RFC 2327) y RTP (Protocolo de transporte en tiempo real, IETF RFC 1889) para el intercambio de datos. El SDP sirve en particular para negociar los códecs de audio y/o vídeo, los protocolos de transporte, etc., que se utilizarán entre los puntos terminales. El objetivo del RTP es transportar el flujo de datos multimedia (audio, vídeo, texto, etc.), es decir, codificar los datos, descomponerlos en paquetes y enviarlos. Los puntos terminales de comunicación en un sistema basado en SIP se denominan agentes de usuario. Se entiende por cliente de agente de usuario (UAC) un componente que inicia una consulta SIP (solicitud), el Servidor de agente de usuario (UAS) responde a esta solicitud con una respuesta (respuesta). Un agente de usuario (UA) puede asumir tanto el rol del UAC como el del UAS. Las solicitudes, de las cuales se emite un número limitado, se responden fundamentalmente mediante respuestas (aproximadamente 100 respuestas diferentes). Solo portan números para la diferenciación. Un agente de usuario envía un mensaje SIP a un proxy SIP por adelantado. Sobre la base de la dirección dada, el proxy decide a dónde debe enviarse el mensaje y luego lo reenvía. Estos proxies pueden estar fundamentalmente sin estado (sin estado) o con estado (de estado). Mientras que los proxies sin estado solamente reenvían mensajes y realmente no los reciben, de que, por ejemplo, se establece una conversación, los proxies de estado pueden asumir tareas que son útiles para establecer una conversación. Una de las tareas más importantes de un proxy de estado es la distribución de llamadas a varios destinos: en la denominada "bifurcación secuencial", los posibles destinos de llamadas se marcan uno tras otro, en la "bifurcación paralela" todos los destinos reciben un mensaje al mismo tiempo. Otro componente indispensable de

un sistema basado en SIP es un registrador SIP, en el cual todos los agentes de usuario deben estar registrados. Esta unidad lógica convierte una base de datos con información sobre los agentes de usuario que iniciaron sesión y dirige las consultas a estos destinos. Como regla general, el registrador y el proxy son el mismo programa, que regula el redireccionamiento interno sin tener que intercambiar mensajes. Finalmente, un sistema basado en SIP también comprende un servidor de redirección o una puerta de enlace, que, entre otros, garantiza la conexión entre la red de telefonía basada en IP y la PSTN.

SIP usa el método de registro en el registro. El UA indica dónde está localizable y recibe la confirmación con el código 200 (OK). Si el usuario es desconocido, se devuelve 404 (no encontrado); si el registro no está permitido, la respuesta es 403 (prohibido). Sin embargo, el requisito previo para el registro exitoso es la autenticación exitosa del agente de usuario en la red correspondiente y la verificación de su autorización para los servicios deseados. Para ello, los métodos de autenticación y autorización RADIUS y DIAMETER se usan principalmente en un entorno basado en SIP; que también se usan con muchas otras funciones de red.

El protocolo de autenticación RADIUS (Servicio de usuario de acceso telefónico de autenticación remota - IETF RFC 2138, 2868) se utiliza en muchas unidades de red en la actualidad, por ejemplo, enrutadores, servidores de módem, conmutadores, etc. El cliente de autenticación envía su nombre de usuario y contraseña al servidor RADIUS. El servidor RADIUS verifica esta información y autoriza al usuario al sistema. La razón de la prevalencia de RADIUS es que las unidades de red en general no pueden manejar una gran cantidad de usuarios de red, cada uno con diferente información de autenticación, porque esto excedería la capacidad de memoria de las unidades de red individuales, por ejemplo. RADIUS permite la administración central de una pluralidad de usuarios de red (añadir, eliminar usuarios, etc.). Por lo tanto, este es un requisito previo necesario para su servicio en ISP (proveedores de servicios de Internet), por ejemplo, porque a menudo tienen usuarios que ascienden de varios miles a varias decenas de miles. La autenticación remota de RADIUS basada en TACACS + (sistema de control de acceso mediante control del acceso desde terminales+) y LDAP (protocolo ligero de acceso a directorios) es relativamente segura contra los piratas informáticos, pero muchos otros protocolos de autenticación remota solo tienen una protección temporal, insuficiente o ninguna protección en absoluto contra los piratas informáticos. Otra ventaja de RADIUS es el hecho de que RADIUS fue durante mucho tiempo el estándar *de facto* para la autenticación remota, por lo que RADIUS es compatible con casi todos los sistemas.

Con el aumento en la complejidad de los servicios solicitados, sin embargo, RADIUS ha demostrado ser inadecuado para su uso en redes más grandes. Esto ha requerido el desarrollo de un nuevo protocolo. Sin embargo, el protocolo DIAMETER (IETF RFC 3588) no se desarrolló desde cero, sino que se conservó la mayor parte del protocolo RADIUS, eliminando sus errores. DIAMETER, como RADIUS, usa pares de atributos/valores (AVP) para facilitar datos y UDP como protocolo de transporte. Además, puede ampliarse añadiendo nuevos comandos y AVP. Representa un protocolo básico que cumple con los requisitos mínimos de un protocolo de transporte de autenticación. Por lo tanto, no se debe usar en general, sino que se debe usar siempre con una extensión específica para la aplicación. DIAMETER es un protocolo entre pares. El cliente DIAMETER normalmente inicia una solicitud de autenticación o autorización por parte de un usuario. El servidor DIAMETER recibe esta solicitud y la responde o la reenvía a un servidor proxy. El nodo móvil solicita el servicio deseado por medio del mensaje de solicitud de autenticación (ARM) que contiene los AVP. La información requerida para la autenticación se extrae de este mensaje e incluye AVP de DIAMETER. Este mensaje se reenvía entonces al servidor DIAMETER local, denominado AAAF. El AAAF reenvía el mensaje al servidor local de autenticación (AAAH). Si el AAAH puede autenticar con éxito al usuario, envía una solicitud de MIP de agente local (HAR) a un agente local. Este agente local procesa el mensaje DIAMETER después de recibir el HAR y luego prepara el HAA de respuesta con los datos requeridos, tal como la ID de sesión, etc., y lo envía al AAAH, que prepara la respuesta de autenticación (AMA) que contiene, entre otros, información para tunelizar mensajes y la envía a la AAAF. Con ello, se establece la conexión. La extensión de IP móvil también define numerosos casos especiales, tales como el manejo de transferencias.

Además de la autenticación y la autorización, surge la cuestión de los mecanismos de facturación adecuados en una red para telefonía y/o videotelefonía basadas en IP. El protocolo TAP (procedimiento contable transferido) del Grupo de Intercambio de Datos Contables Transferidos (TADIG) de la Asociación GSM es el protocolo conocido en el estado de la técnica para facturar el servicio reclamado por unidades móviles en redes GSM. La itinerancia es un concepto muy importante en las redes GSM. Este es un método que permite a un usuario de un teléfono móvil utilizar su aparato de teléfono móvil no solo en su red original, sino también en cualquier otra red dentro y fuera de su país. Sin embargo, este método requiere un concepto de facturación que pueda aglutinar la complejidad de los protocolos y los diversos servicios ofrecidos sin errores. Por lo tanto, los métodos de facturación para redes GSM de ninguna manera pueden ser triviales. En la actualidad en día existen más de 400 redes GSM operativas en todo el mundo, y se estima que hay más de 20.000 acuerdos de itinerancia individuales entre operadores de redes individuales. En consecuencia, existe un proceso extremadamente complejo de adquisición de información, distribución de información y análisis de información detrás de la idea aparentemente simple de itinerancia para posibilitar la facturación. En este contexto, el protocolo de procedimiento contable transferido (TAP) se utiliza para intercambiar información de facturación de itinerancia entre proveedores de servicios de red de telefonía móvil individuales. El 4 de junio de 2000, finalmente se lanzó TAP3 después de TAP2 y TAP2+. Ya existen subversiones de TAP3.1 y TAP3.2. TAP3 puede denominarse en la actualidad como el estándar, aunque TAP es un protocolo que continúa en desarrollo.

La mayoría del tráfico de voz o datos en redes GSM se origina o termina en una red distinta de aquella en la que se encuentra actualmente el usuario móvil. El operador de una red local cobra tarifas por una llamada que finaliza con uno de sus usuarios, independientemente de si se trata de una red fija o una red móvil. Para simplificar la recaudación de tarifas, los operadores de redes fijas locales celebran acuerdos mutuamente con operadores locales de redes de telefonía móvil. Por lo tanto, un operador de red de telefonía móvil en un país no necesita cerrar un acuerdo con el proveedor de red fija en otro país para facturar una llamada desde la red de telefonía móvil del primer proveedor a la red fija del segundo proveedor. El proveedor de red fija en el primer país normalmente ya tiene un acuerdo con el proveedor de red fija en el segundo país con respecto al tipo de facturación y tarifas, para que el operador de la red de telefonía móvil pueda facturar entonces los servicios en el primer país a través del proveedor de red fija con un convenio correspondiente. Los costes generalmente se facturan directamente al usuario (facturación minorista) o a través de un proveedor de servicios (facturación mayorista). El tipo de facturación de datos en itinerancia o tráfico de voz entre diferentes redes móviles (PMN: red móvil pública) se produce por medio del protocolo TAP. Los registros de llamadas en itinerancia normalmente se crean como TAP o como registros CIBER (registro de intercambio de facturación celular interoperador). Los registros CIBER se usan por operadores de redes móviles que operan con tecnologías basadas en AMPS, tales como AMPS, IS-136 TDMA e IS-95 CDMA. Se usa TAP principalmente por los proveedores de servicios de red móvil GSM/UMTS y es el protocolo principal para la facturación en las regiones dominadas por GSM/UMTS.

Los detalles sobre una llamada realizada por un usuario ubicado en una red extranjera (VPMN: red móvil pública visitada) se registran en un centro de conmutación móvil (MSC) de la red. Por lo tanto, cada llamada genera uno o más registros de llamada. El estándar GSM para estos registros se define en GSM 12.05, aunque muchos proveedores usan su propio formato. Los registros de llamadas del MSC se transmiten a un sistema de facturación del VPMN para su facturación. Estos registros de llamadas se convierten al formato TAP y se asignan al usuario correspondiente. A más tardar dentro de un período de tiempo predefinido (por ejemplo, 36 horas), los registros TAP se envían a los proveedores de servicios de red móvil correspondientes. Los archivos TAP contienen, además, información sobre la tarifa de servicio del proveedor (IOT: tarifa entre operadores), y todos los demás convenios bilaterales y esquemas de beneficios. Los registros TAP se envían directamente o, más comúnmente, a través de una oficina de facturación, tal como un centro de compensación. Si el operador de la red doméstica (HPMN: red móvil pública doméstica) recibe un registro TAP de la VPMN, este se convierte a un formato de Internet correspondiente y se factura junto con el registro de llamadas normales del usuario, que genera en la red doméstica. En la facturación mayorista en la que un proveedor de servicios factura los costes aplicables al usuario, la HPMN reenvía los registros al proveedor del servicio, que puede facturar las llamadas de nuevo en particular de acuerdo con sus propias tarifas y genera la liquidación, por ejemplo, con detalles de llamadas, para el usuario.

TAP3 es compatible con una diversidad de servicios. TAP3 se utiliza en la actualidad para la facturación entre proveedores de servicios GSM/UMTS y proveedores de servicios GSM/UMTS, proveedores de servicios GSM/UMTS y proveedores de servicios no GSM (itinerancia entre estándares) y proveedores de servicios GSM y de servicios satelitales, etc. Las tres categorías de servicios básicas de servicios de voz, fax y los denominados servicios complementarios ya reciben soporte desde TAP1. Sin embargo, la facturación del servicio de mensajes cortos (SMS) es menos trivial debido al uso del centro de servicio de mensajes cortos (SMS-C) de terceros. Los siguientes factores dificultan la facturación de SMS: 1) un usuario itinerante puede recibir un SMS en itinerancia (MT-SMS), 2) un usuario itinerante puede enviar un SMS en itinerancia (MO-SMS) utilizando el SMS-C de su red doméstica, y 3) un usuario itinerante puede enviar un SMS en itinerancia (MO-SMS) utilizando el SMS-C de una red extranjera. Por lo tanto, la facturación de los servicios de SMS es totalmente compatible solo desde TAP2+ en adelante. A partir de TAP3, también es compatible la facturación de datos de circuitos conmutados, HSCSD (datos de alta velocidad con conmutación de circuitos) y GPRS (servicio general de radio por paquetes). TAP3 también es compatible con todos los servicios de valor añadido (VAS), tal como la denominada facturación de contenido. Sin embargo, la facturación del servicio de valor añadido a menudo es difícil porque requiere el consentimiento del proveedor del servicio a los servicios facturados. La lógica mejorada móvil para aplicaciones personalizadas (CAMEL) es compatible desde la introducción de TAP3.4. CAMEL es especialmente importante para aplicaciones en servicios prepago para usuarios de itinerancia y podría alcanzar una gran importancia en el futuro. Otra aplicación importante de TAP3 es respaldar las facturaciones en la tarifa entre operadores (IOT). IOT hace posible que el proveedor de servicios de red pública móvil doméstica (HPMN) verifique ofertas y tarifas especiales de un proveedor de servicios extranjero (VPMN) y las envíe al usuario itinerante. Por lo tanto, por ejemplo, la VPMN puede brindar servicios o descuentos para varios servicios o niveles de llamada y la HPMN puede verificar estos de manera sencilla y ajustar sus tarifas. La posibilidad de facturar servicios de itinerancia independientemente de dónde se encuentre el usuario en ese momento es una valiosa ayuda para los proveedores de servicios de red móvil y evita la pérdida de ingresos con servicios provisionales a través de una VPMN. El protocolo TAP a partir de TAP3 también compila información detallada sobre dónde se inició una llamada y/o se reclamó un servicio, etc. y dónde se envió. Esta información ayuda a compilar un perfil sobre el usuario respectivo en función de su comportamiento, lo que proporciona información importante para adaptar y optimizar la oferta de servicios a las necesidades del usuario. En particular, se puede usar para ofrecer servicios especiales basados en la ubicación, por ejemplo, eventos deportivos, conciertos, etc. Finalmente, el protocolo TAP3, con el procedimiento contable devuelto (RAP), permite también un manejo de errores diferenciado. Por lo tanto, con RAP, la HPMN puede verificar y, si es necesario, descartar parcialmente, entre otros, archivos TAP entrantes con respecto a su validez y conformidad con el estándar TAP sin que por ello se

pierdan las facturaciones de los servicios que se transmitieron sin errores.

En la interfaz entre la telefonía basada en IP y/o la videotelefonía y las redes telefónicas tradicionales, se deben responder preguntas fundamentalmente similares a las de la facturación de conversaciones entre dos operadores diferentes de redes móviles. En primer lugar, existe típicamente una pluralidad de operadores, en donde se puede suponer en la práctica que cada uno de estos operadores está usando su propio modelo de tarifa. En segundo lugar, un cliente de un operador puede llamar a clientes cualesquiera de otros operadores, lo que se refleja en tarifas de conversación más altas. Las directrices generales para realizar pagos de compensación se encuentran en la Recomendación D.196 de la UIT, por ejemplo. Sin embargo, no hay estándares y protocolos públicamente accesibles para un procedimiento unificado en la compensación y liquidación de facturas. Además, hay varios proveedores para un centro compensación que pueden ser utilizados en particular por los operadores móviles para la liquidación de tarifas de itinerancia. Sin embargo, todos estos proveedores tienen en común el hecho de que, igualmente, no se está utilizando ninguna norma públicamente accesible.

Para que sea posible establecer tarifas para una conversación entre dos proveedores a través de una ubicación central, todos los proveedores deben usar un protocolo estándar. A estos efectos, la empresa TransNexus ha especificado el protocolo de liquidación abierta (OSP), que ETSI declaró como el estándar en su especificación TIPHON. Por un lado, el OSP define un marco básico para un intercambio de información estandarizado. Por otro lado, este estándar también prevé intencionalmente la especificación de que partes del protocolo pueden ser reemplazadas y/o expandidas. Por lo tanto, los requisitos especiales y los servicios específicos del operador también pueden integrarse.

Se usa una combinación de HTTP y S/MIME como protocolo de transmisión. El método POST de HTTP se usa para la transmisión. Aunque también existe el método PUT para transmitir datos a un servidor por HTTP, solo es posible mediante el método POST asignar los datos adjuntamente enviados a un determinado recurso en el extremo del servidor, lo que realiza un procesamiento adicional de los datos. Además, el contenido de los datos transmitidos consiste en un mensaje S/MIME. Para equilibrar los mensajes OSP con un centro de compensación, existen dos modos de operación: el modo en línea y el modo masivo. En el modo en línea, hay una conexión con el centro de compensación mientras se lleva a cabo una conversación entre los diferentes operadores de red. La razón de este enfoque es que algunas tareas pueden ser asumidas por el centro de compensación para que se produzca la llamada. Por ejemplo, si el servicio de soporte interno que pertenece a la persona que llama tiene muy poca información sobre el destino de la conversación, entonces el centro de compensación puede tomar decisiones de enrutamiento y proporcionar una dirección de contacto para el controlador de acceso de destino. Además, es concebible integrar la funcionalidad de un agente del área de servicio (SAB) en el centro de compensación. El objetivo de un SAB es determinar el método más oportuno para establecer la conversación, en el que se pueden tener en cuenta tarifas dependientes del horario y las cargas actuales en la red. Sin embargo, la desventaja del modo en línea es la ampliación del tiempo de retraso para establecer una conexión, porque en última instancia, el controlador de acceso de la persona que llama no solo debe esperar varias respuestas de su propio servicio de soporte interno, sino que también debe esperar sucesivamente las respuestas del centro de compensación. En el modo masivo, sin embargo, una conexión con el centro de compensación se establece solo en momentos predeterminados. Una ventaja de este método es que un proceso independiente del controlador de acceso puede leer los CDR del servicio de fondo y transmitirlos de una vez al centro de compensación. Otra ventaja en contraste con el método en línea es que un fallo temporal del centro de compensación no da lugar a ninguna perturbación reseñable en el propio sistema, porque si una transferencia de CDR se interrumpe y/o no se produce, puede simplemente repetirse en un momento posterior. Como desventaja más importante, sin embargo es evidente que un centro de compensación en modo masivo no puede funcionar como un SAB. Además, el centro de compensación no puede tomar decisiones de enrutamiento porque esto igualmente puede tener lugar solo en el modo en línea. Los componentes más importantes de un mensaje OSP son el intercambio de precios, el intercambio de autorización y el intercambio de uso. El intercambio de precios comprende el intercambio de información por el coste de una conversación telefónica. Este intercambio de precios consiste en la transmisión de una indicación de precios que debe confirmarse con una confirmación de precios. El intercambio de autorización se realiza cuando los recursos deben ser utilizados por el centro de compensación. Esto generalmente corresponde a la autorización para establecer una conversación telefónica. Al igual que el intercambio de precios, el intercambio de autorización también se basa en el envío de una solicitud de autorización que se confirma mediante una respuesta de autorización. El intercambio de uso incluye una descripción de los recursos utilizados. Para ello, se envía una indicación de uso que se confirma con una confirmación de uso, y dado que aún no se pueden diferenciar servicios por parte de OSP, el término "uso" se entiende que se refiere únicamente al tiempo de conversación de una conversación telefónica que se lleva a cabo.

El documento WO 2004/017564 A1 de la técnica anterior describe un método para itinerancia automática entre redes WLAN heterogéneas en el que un nodo de IP móvil solicita acceso a la WLAN en un punto de acceso y en el que el nodo de IP móvil responde a una solicitud del servidor de acceso para la autenticación y transmite un IMSI almacenado en una tarjeta SIM del nodo de IP móvil al servidor de acceso. Basado en el IMSI, mediante la información almacenada en una base de datos de usuarios de SIM, se adapta el canal de datos IP lógico de la WLAN a los correspondientes datos GSM para canales de señal y datos de una red GSM de una manera específica para el usuario y la autenticación del nodo de IP se realiza con un HLR de una red GSM. El método divulgado en el

documento WO 2004/017564 A1 está dirigido a la autenticación característica del servidor de acceso y el registro en el servidor de acceso de la WLAN en acceso a esta WLAN, y no puede usarse para formar subredes, en particular conexiones punto a punto protegidas dentro de una estructura de red abierta que ya se ha establecido, tal como telefonía y/o videotelefonía basada en IP (por ejemplo, mediante el protocolo de inicio de sesión SIP). El documento WO 2004/017565 A1, también proveniente de la técnica anterior, divulga un método para la determinación y facturación de servicios en itinerancia de un nodo de IP móvil en WLAN heterogéneas basadas en el método del documento WO 2004/0175654 A1. Para la facturación, los primeros registros de detalles de llamada se transfieren de un servidor de acceso a un módulo de facturación, y los segundos registros de detalles de llamada se transmiten desde el servidor de acceso a un módulo proxy. Por medio de un módulo de compensación, el servicio reclamado es facturado por un proveedor de una red fija y/o los archivos TAP son transmitidos a un proveedor de servicios GSM para la facturación. El método divulgado en el documento WO 2004/017565 A1 también depende de la autenticación, el registro y la facturación en el acceso a una WLAN por un servidor de acceso, y no puede usarse en la formación de subredes en conexiones de red abiertas existentes debido a las características específicas del servidor de acceso, en particular, conexiones punto a punto protegidas dentro de una estructura de red LAN/WLAN normal, tal como telefonía y/o videotelefonía basada en IP (por ejemplo, mediante el protocolo de Inicio de sesión SIP), en donde los nodos de IP ya tienen cada uno acceso a la red.

Sin embargo, la telefonía y/o la videotelefonía basada en IP en el estado de la técnica están asociadas con desventajas sustanciales. Si bien es cierto que en la actualidad es posible autenticar a los participantes en una conversación en una red basada en IP por medio de mecanismos de autenticación y autorización que se han descrito y verificar su autorización para ciertos servicios, estos métodos de autenticación y autorización son bastante complicados y además no cumplen con los altos estándares con respecto a la seguridad, facturación y autorización de servicios, tales como los que se ofrecen en las redes telefónicas tradicionales. En particular, las redes móviles GSM/UMTS ofrecen estándares con respecto a la autenticación y autorización que no pueden implementarse en una red basada en IP debido a sus propiedades intrínsecas, debido a que la arquitectura abierta del protocolo IP carece de una gran cantidad de información que es absolutamente esencial para una compatibilidad total con las redes GSM.

Por lo tanto, un objeto de la presente invención es proponer un nuevo y mejor método y un sistema para telefonía y/o videotelefonía basada en IP. En particular, este nuevo y novedoso método y sistema debería permitir ofrecer los mismos estándares con respecto al registro y/o la autenticación y autorización a los usuarios de telefonía y/o videotelefonía basados en IP que aquellos a los que están acostumbrados a partir de la telefonía tradicional, tal como telefonía móvil GSM.

De acuerdo con la presente invención, estos objetivos se logran en particular mediante los elementos de la parte caracterizadora de las reivindicaciones independientes. Las realizaciones ventajosas adicionales se derivan además de las reivindicaciones dependientes y la descripción a continuación.

En particular, estos objetivos se logran mediante la invención debido a que los datos de autenticación se transfieren entre al menos un nodo de IP y un segundo terminal, es decir, desde un módulo de identificación del nodo de IP, y los datos de registro se transmiten desde el nodo de IP a un módulo de registro, en donde el nodo de IP está autenticado en la red basada en IP y registrado en una base de datos de localización, en donde, por medio de los módulos de registro, los datos de autenticación se separan de los datos de registro y se dirigen a un módulo de autenticación, en el que, por medio del módulo de autenticación, así como por medio de un registro de ubicación de origen basado en los datos de autenticación, se realiza la autenticación del nodo de IP en el que, cuando la autenticación del nodo de IP es exitosa, se lleva realiza una actualización de localización en el registro de localización local y los datos de localización correspondientes se transmiten al módulo de registro, y en el que los datos de localización del nodo de IP se almacenan en la base de datos de localización por medio del módulo de registro, y los datos correspondientes se envían al módulo de identificación del nodo de IP, en el que el nodo IP está habilitado para telefonía basada en IP y videoconferencia. Esto tiene la ventaja de que, entre otros, se habilita la autenticación y/o autorización segura y conveniente de los usuarios en una red de telefonía y/o videotelefonía basada en IP. Al conectar la telefonía y/o videotelefonía basadas en IP mediante un método conveniente y seguro, se hace posible una autenticación y/o autorización de usuarios altamente segura y bien probada, como se conoce a partir de la telefonía móvil GSM.

En una variante de realización, se usan datos de autenticación que se ajustan al estándar GSM. Esta variante de autenticación tiene la ventaja de que, entre otros, se puede utilizar una infraestructura GSM existente de un proveedor sin modificaciones importantes. En este caso, los perfiles de usuario para los usuarios de telefonía y/o videotelefonía basadas en IP, se crean como para los usuarios de telefonía móvil ordinaria. Además, de esta manera se pueden utilizar los criterios de alta seguridad existentes de la tecnología GSM .

En otra variante de realización, se usa una tarjeta SIM como el módulo de identificación del nodo IP. Esto tiene la ventaja de que, entre otros, una tarjeta SIM es un medio ampliamente distribuido y probado para la identificación de nodos de IP, en particular, nodos de IP móviles. También cumple con altos estándares de seguridad y, gracias a su pequeño tamaño, también puede reemplazarse o transportarse fácilmente. Además, los costes de fabricación para dichas tarjetas SIM son bajos en comparación con otros mecanismos de identificación similares.

En otra variante de realización, la infraestructura que se usa para telefonía y/o videotelefonía basadas en IP se ajusta al protocolo SIP. Esta variante de realización tiene la ventaja de que, entre otros, el protocolo SIP es una alternativa ampliamente utilizada en telefonía y/o videotelefonía basadas en IP. SIP se basa en el protocolo HTTP, es fácil de implementar y permite una gran flexibilidad para una amplia diversidad de aplicaciones. Además, muchos productos que son compatibles con el protocolo SIP ya están disponibles en el mercado en la actualidad.

En otra variante de realización, los datos de autenticación se transmiten desde el nodo de IP al módulo de registro a través de una interfaz sin contacto. Esta variante de realización tiene la ventaja de que, entre otros, pueden usarse nodos de IP móviles, que permiten una mayor movilidad de los usuarios de telefonía basada en IP y/o telefonía móvil, en comparación con la telefonía móvil.

En otra variante de realización, los datos de autenticación se transmiten desde el nodo de IP al módulo de registro a través de una interfaz WLAN 802.11 y/o a través de una interfaz Bluetooth y/o GSM y/o UMTS. Esto tiene la ventaja de que las redes conocidas y establecidas se pueden usar para la transmisión de datos de autenticación, de manera que se pueden utilizar las instalaciones existentes (puntos de acceso).

En otra variante de realización, se usa un teléfono móvil con capacidad IP como el nodo de IP. Esta variante de realización tiene la ventaja de que la telefonía y/o la videotelefonía basadas en IP pueden utilizarse adicionalmente como un sustituto de la telefonía móvil tradicional sin que el usuario tenga que adquirir otro dispositivo.

En otra variante de realización, los registros de detalles de llamada del nodo de IP se transmiten al módulo de registro, en el que al menos la identidad del nodo de IP y/o la duración y/o el proveedor del servicio reclamado se detectan entonces y se reenvían a un módulo de facturación, y el módulo de facturación crea archivos de facturación de acuerdo con el servicio reclamado en base a los datos de facturación del módulo de registro y los primeros registros de datos de llamada, y transmite estos archivos de facturación con instrucciones de facturación a un módulo de compensación. Esto tiene la ventaja de que, entre otros, la facturación de los servicios reclamados se puede gestionar fácilmente a través de un módulo de compensación, en particular en el caso de compensación entre los diversos operadores de red.

En este punto, debe enfatizarse que la presente invención se refiere no solo al método de acuerdo con la invención, sino también a un sistema para realizar este método.

Las variantes de realización de la presente invención se describen a continuación sobre la base de ejemplos. Los ejemplos de las realizaciones que se describen a continuación se ilustran mediante las siguientes figuras adjuntas:

La figura 1 muestra un diagrama de bloques que ilustra esquemáticamente un método y un sistema para telefonía y/o videotelefonía basadas en IP del estado de la técnica. Los nodos de IP -30- acceden a la infraestructura para telefonía y/o videotelefonía basada en IP -50- a través de una red de datos -100-. Esta infraestructura para telefonía y/o videotelefonía basada en IP -50- comprende un módulo de registro -51-, un módulo de control -52- y una puerta de enlace IP/PSTN -53-, mediante lo cual se establece la comunicación con los teléfonos -31- conectados a través de la red de telefonía conmutada pública -200-.

La figura 2 muestra un diagrama de bloques que ilustra esquemáticamente un método de acuerdo con la invención y un sistema de acuerdo con la invención para telefonía y/o videotelefonía basada en IP, en el que los nodos de IP -10- comprenden un módulo de identificación -11- y acceden a una infraestructura para la telefonía y/o videotelefonía basadas en IP -50- a través de una red de datos -100-. Esta infraestructura para telefonía y/o videotelefonía basada en IP -50- comprende un módulo de registro -51-, un módulo de control -52- y una puerta de enlace IP/PSTN -53-, mediante la cual se establece la comunicación con los teléfonos -31- conectados a través de la red de telefonía conmutada pública -200-. Un módulo de autenticación -20- autentica el nodo de IP -10- basándose en los datos de autenticación almacenados en el módulo de autenticación -11- del nodo de IP -10- en un registro de localización local -25-.

La figura 2 ilustra una arquitectura que puede usarse para implementar la invención. En la figura 2, el número de referencia -10- indica un nodo de IP que tiene la infraestructura necesaria, incluyendo todos los componentes de hardware y software para realizar el método y/o sistema de acuerdo con la invención aquí descritos. Se entenderá como nodos de IP -10-, entre otros, todo los denominados equipos de premisa del cliente (CPE) que se proporcionan para su uso en diversos sitios de red y/o con diversas redes. Estos comprenden, por ejemplo, teléfonos y/o videoteléfonos basados en IP, así como todos los demás dispositivos con capacidad IP, por ejemplo, PDA, ordenadores portátiles o teléfonos móviles. Los nodos de IP -10- tienen una o más interfaces de red físicas diferentes que también pueden soportar varios estándares de red diferentes. Estas interfaces físicas de red del nodo de IP -10- pueden comprender, por ejemplo, interfaces sin contacto con WLAN (red de área local inalámbrica), Bluetooth, GSM (sistema global para comunicación móvil), GPRS (servicio generalizado de radio por paquetes), USSD (datos de servicios complementarios no estructurados), EDGE (Velocidades de datos mejoradas para la evolución GSM) o UMTS (sistema universal de telecomunicaciones móviles), etc. Sin embargo, éstas también pueden ser interfaces físicas de red con Ethernet, Token Ring o cualquier otra LAN (red de área local) cableada. Por

consiguiente, el número de referencia -100- representa las diversas redes, por ejemplo, una LAN inalámbrica (basada en IEEE 802.1x), una red Bluetooth, una LAN cableada (Ethernet o Token Ring), pero también una red móvil (GSM, UMTS, etc.) o una red PSTN. Las interfaces de red físicas del nodo de IP -10- pueden ser no solamente interfaces de conmutación de paquetes, tales como las utilizadas directamente por protocolos de red, sino también interfaces de conmutación de circuitos que pueden utilizarse por medio de protocolos tales como PPP (protocolo punto a punto), SLIP (protocolo de Internet de línea serie) o GPRS (servicio general de radio por paquetes) para la transferencia de datos.

Además, el nodo de IP -10- comprende un módulo de identificación -11-. Este módulo de identificación -11- puede implementarse en hardware o software y puede conectarse al nodo de IP -10- a través de una interfaz sin contacto o una interfaz que requiere contacto o que puede integrarse en el nodo de IP -10-. En particular, el módulo de identificación -11- puede implementarse como una tarjeta SIM, tal como las conocidas para teléfonos móviles. Este módulo de identificación -11- incluye, entre otros, los datos de autenticación relevantes para la autenticación del nodo de IP -10- en una red basada en IP para telefonía y/o videotelefonía. Estos datos de autenticación pueden comprender en particular un IMSI (identificador de abonado móvil internacional) y/o TMSI (identificador de abonado móvil temporal) y/o LAI (identificador de área de ubicación), etc., que se ajustan al estándar GSM.

Para el registro del nodo de IP -10- en la red para telefonía y/o videotelefonía basadas en IP, el nodo de IP -10- solicita acceso al servicio de telefonía y/o videotelefonía a través de una interfaz de contacto o sin contacto a la red basada en IP -100-. Como ya se ha descrito, la red basada en IP -100- puede incluir diversos estándares y protocolos de red, tales como redes inalámbricas WLAN 802.11 o Bluetooth o redes cableadas como Ethernet o Token Ring, etc. La infraestructura para telefonía y/o videotelefonía basada en IP -50- comprende un módulo de registro -51-, un módulo de control -52- y una puerta de enlace -53- que asegura la conexión entre la red basada en IP -100- y la red telefónica pública conmutada (PSTN) -200- y/o la red móvil. Esta infraestructura puede construirse de acuerdo con los requisitos del SIP (protocolo de inicio de sesión) y/o H.323 y/o MGCP (protocolo de control de pasarela de medios) y/o el protocolo MEGACO (control de pasarela de medios) para telefonía y/o videotelefonía basada en IP. Una solicitud de registro incluye los datos de autenticación del módulo de identificación -11- del nodo de IP -10- y los datos de registro para el registro en la red de telefonía y/o videotelefonía basada en IP. Los datos de autenticación pueden incluir, en particular, el IMSI desde una tarjeta SIM basada en GSM. Esta solicitud de registro se transmite al módulo de registro -51- de la red de telefonía y/o videotelefonía basada en IP, por ejemplo, a un registro SIP. Los datos de autenticación son separados de los datos de registro por el módulo de registro -51- y se transmiten a un módulo de autenticación -20-. En base a los datos de autenticación, las funciones de autenticación y/o autorización y/o configuración requeridas se generan por medio del módulo de autenticación -20-, para que el modelo de autenticación -20- lleve a cabo la autenticación y/o autorización del nodo de IP -10- en base a los datos de autenticación del módulo de identificación -11- del nodo de IP -10- en un registro de localización local (HLR) -25-. Este registro de localización local -25- puede ser, en particular, un registro de localización local (HLR) de una red GSM que incluye los perfiles de usuario correspondientes. También es concebible que, para la autenticación del nodo de IP -10-, el IMSI del módulo de identificación -11- del nodo de IP -10- se use solamente en una o varias de las etapas en la autenticación, mientras que con todas las demás etapas de autenticación, el IMSI se reemplaza por un IMSI temporal generado (denominado TMSI).

El siguiente método de respuesta al desafío se puede usar, en particular, para el procedimiento de autenticación. El módulo de identificación -11- (por ejemplo, la tarjeta SIM) recibe un número aleatorio de 128 bits (RAND) como desafío (pregunta). A continuación, se lleva a cabo un algoritmo confidencial específico para el operador respectivo en el módulo de identificación -11-, que recibe como entrada el número aleatorio RAND y una clave secreta Ki almacenada en el módulo de identificación -11- y de ello genera una respuesta de 32 bits (SRES) y una clave de 64 bits Kc. Kc sirve para cifrar la transferencia de datos a través de interfaces inalámbricas (Especificación técnica GSM GSM 03.20 (ETS 300 534): "Digital Cellular Telecommunication System (phase 2); Security-Related Network Functions", European Telecommunications Standards Institute, agosto de 1997). Para la autenticación, se usan múltiples desafíos RAND para generar una pluralidad de claves Kc de 64 bits. Estas claves Kc se combinan en una clave de sesión más larga. Al comienzo de la autenticación, el nodo de IP -10- transmite la identidad de abonado móvil internacional (IMSI) del usuario del módulo de identificación -11- al módulo de registro -51-. Con el IMSI, el módulo de registro -51- recibe n tripletes GSM en respuesta a un desafío de triplete del HLR -25- correspondiente. A partir de los tripletes, el módulo de registro 51 calcula la MAC_RAND y la clave de sesión K. El cálculo de los valores criptográficos de la clave de sesión K generada por SIM y el código de autenticación de mensaje MAC_RAND y MAC_SRES se describen, por ejemplo, en el documento "HMAC: Keyed-Hashing for Message Authentication" de H. Krawczyk, M. Bellar y R. Canetti (RFC2104, febrero de 1997). Entonces, el algoritmo de autenticación GSM se ejecuta en el módulo de identificación -11- del nodo de IP -10- y calcula una copia de MAC_RAND. El nodo de IP -10- controla que el valor calculado de MAC_RAND sea igual al valor obtenido para MAC_RAND. Si los dos valores no coinciden, el nodo de IP -10- interrumpe el procedimiento de autenticación y no envía ningún valor de autenticación calculado por el módulo de identificación -11- a la red. Dado que el valor RAND se recibe junto con el código de autenticación de mensaje MAC_RAND, el nodo de IP -10- puede garantizar que RAND es nuevo y se generó por la red. Cuando la autenticación es exitosa, se lleva a cabo una actualización de localización en el HLR -25- y el nodo de IP -10- recibe una entrada correspondiente en una base de datos de clientes del servidor de acceso.

Después de la autenticación y/o autorización exitosas en el registro de localización local -25-, los datos de localización correspondientes se transmiten desde el módulo de autenticación -20- al módulo de registro -51-. Por medio del módulo de registro -51-, los datos de localización se almacenan en una base de datos con información sobre los nodos de IP -10- en la red de telefonía y/o videotelefonía basadas en IP. En particular, estos datos de localización pueden incluir direcciones IP, direcciones MAG y otros datos relevantes para telefonía y/o videotelefonía basada en IP. Además de la autenticación en telefonía y/o videotelefonía basada en IP, los registros de detalles de llamada del nodo de IP -10- se transmiten al módulo de registro -51-, en donde el módulo de registro -51- detecta al menos la identificación del nodo de IP -10- y/o la duración y/o proveedor del servicio reclamado y lo reenvía a un módulo de facturación, y en donde el módulo de facturación genera archivos de facturación de acuerdo con el servicio reclamado en base a los datos de facturación del módulo de registro -51- y los primeros registros de detalles de llamada y los transmite con instrucciones de facturación a un módulo de compensación. A continuación, los datos de autenticación correspondientes se transmiten desde el módulo de registro -51- al módulo de identificación -51- del nodo de IP -10- y se guardan, con lo que el nodo de IP -10- se libera para telefonía y/o videotelefonía basada en IP.

REIVINDICACIONES

1. Un método para registrar un terminal IP en un registrador SIP (51) para el uso posterior de telefonía y/o videotelefonía basada en IP entre un primer terminal en forma de un nodo de IP (10) y un segundo terminal (30/31), en el que el nodo de IP (10) en la red de telefonía y/o videotelefonía basada en IP está autenticado, basándose en datos de registro transmitidos, por medio de un registrador SIP (51) y registrado en una base de datos de localización, **caracterizado por que**

el nodo de IP (10) solicita, a través de una solicitud de registro, acceso al servicio de telefonía y/o videotelefonía basado en IP, en el que la solicitud de registro incluye un IMSI de una tarjeta SIM (11) del nodo de IP (10), y los datos de registro para registrar el nodo de IP (10) en la red de telefonía y/o videotelefonía basada en IP de una infraestructura SIP, en donde los datos de registro contienen datos de localización en forma de una dirección IP del nodo de IP (10), y la solicitud de registro se transmite al registrador SIP (51), y en el que el registrador SIP (51) proporciona a la base de datos de localización la información relativa a los terminales conectados, y reenvía las solicitudes SIP a estos terminales mediante el uso de esta base de datos,

tiene lugar una autenticación antes del registro con el registrador SIP (51), en el que el registrador SIP (51) obtiene el IMSI de la tarjeta SIM (11), consulta un triplete GSM para un registro de localización local (HLR) correspondiente (25), y calcula los valores de autenticación del triplete GSM y los transmite a la tarjeta SIM,
después de una autenticación exitosa utilizando los valores de autenticación y el algoritmo de autenticación GSM, se lleva a cabo una actualización de localización para el HLR (25) en la tarjeta SIM,
los datos de localización del nodo de IP (10) se almacenan en la base de datos de localización por medio del registrador SIP (51), en donde el nodo de IP (10) está habilitado para servicios de telefonía y videotelefonía basados en IP, y

durante una llamada telefónica del nodo de IP (10), el registrador SIP (51) recopila datos de facturación que indican la identidad del nodo de IP y la duración de la llamada telefónica, y junto con los registros de detalles de llamadas transmite los mismos a un módulo de facturación, en el que el módulo de facturación genera archivos de facturación correspondientes a los datos de facturación del módulo de registro (51) y los registros de detalles de llamada, y los transmite junto con las instrucciones de facturación a un módulo de compensación.

2. El método de acuerdo con la reivindicación 1, **caracterizado por que** los datos de autenticación cumplen con el estándar GSM.

3. El método de acuerdo con una de las reivindicaciones 1 o 2, **caracterizado por que** los datos de autenticación y los datos de registro se transmiten desde el nodo de IP (10) al registrador SIP (51) a través de una interfaz sin contacto.

4. El método de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado por que** el nodo de IP (10) es un teléfono móvil con capacidad IP.

5. Un sistema para registrar un terminal IP en un registrador SIP para el uso posterior de telefonía y/o videotelefonía basada en IP entre un primer terminal en forma de un nodo de IP (10), que puede autenticarse en la red IP y registrarse en una base de datos de localización, y un segundo terminal (30/31), en el que el sistema incluye un registrador SIP (51) para registrar el nodo de IP (10) en la red de telefonía y/o telefonía basada en IP en una base de datos de localización, y en el que el registro se realiza usando los datos de registro transmitidos, **caracterizado por que**

el nodo de IP (10) incluye medios para generar una solicitud de registro para acceder al servicio de telefonía y/o videotelefonía basado en IP, en el que la solicitud de registro incluye un IMSI de una tarjeta SIM (11) del nodo de IP (10) y los datos de registro para el registro en la red de telefonía y/o videotelefonía basada en IP de una infraestructura SIP, en donde los datos de registro contienen datos de localización en forma de una dirección IP del nodo de IP (10), en el que la solicitud de registro es transmisible al registrador SIP (51), y en el que la base de datos de localización puede recibir información sobre los terminales conectados mediante el uso del registrador SIP (51), y las solicitudes SIP pueden enviarse a estos terminales, utilizando esta base de datos,

para una autenticación previa al registro con el registrador SIP, el registrador SIP (51) incluye medios para obtener el IMSI de la tarjeta SIM (11), y medios para consultar un triplete GSM para un registro de localización local (HLR) correspondiente (25), en el que los valores de autenticación son computables desde el triplete GSM y pueden transmitirse a la tarjeta SIM,

el sistema incluye un módulo de autenticación (25) con medios para llevar a cabo una actualización de localización para el HLR (25) después de la autenticación exitosa, utilizando los valores de autenticación y el algoritmo de autenticación GSM en la tarjeta SIM (11),

el registrador SIP (51) incluye medios para almacenar los datos de localización del nodo de IP (10) en la base de

datos de localización, en donde el nodo de IP (10) puede habilitarse para servicios de telefonía y videotelefonía basados en IP, y

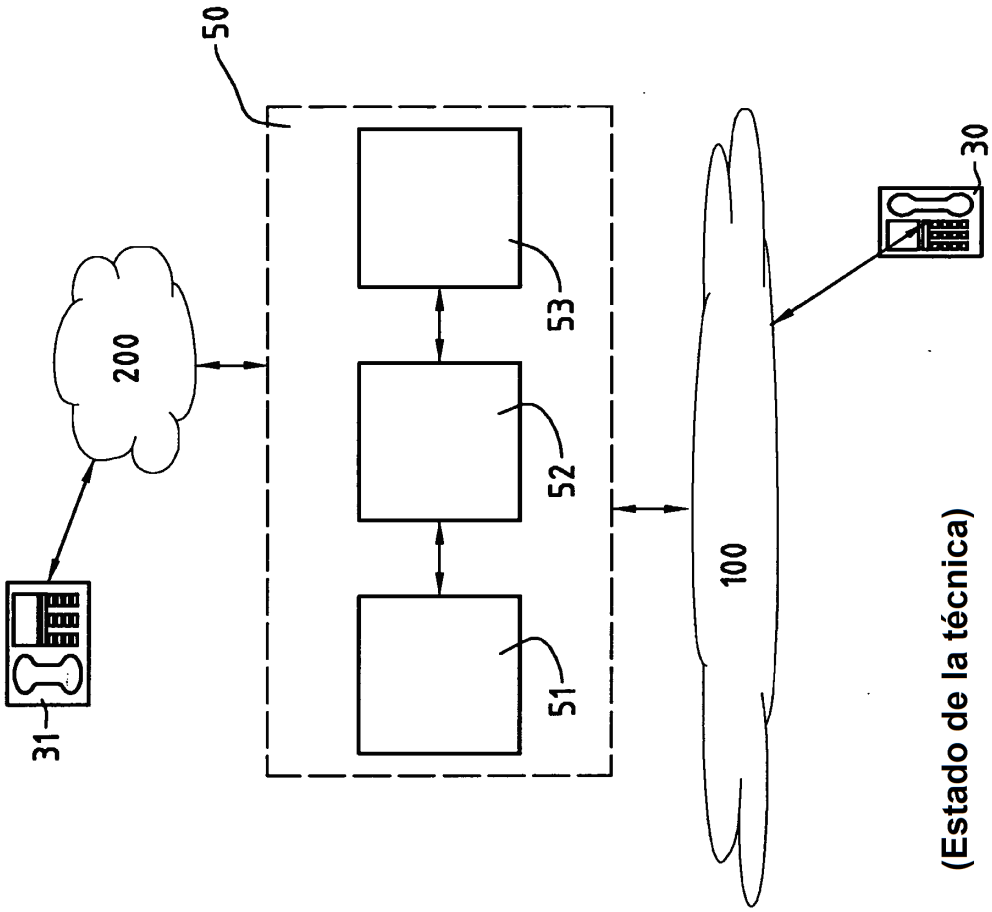
durante una llamada telefónica del nodo de IP (10), los datos de facturación que indican la identidad del nodo de IP y la duración de la llamada telefónica pueden recuperarse para el registrador SIP (51), y junto con los registros de detalles de llamada son transmisibles a un módulo de facturación, en el que los archivos de facturación, correspondientes a los datos de facturación del módulo de registro (51) y los registros de detalles de llamada pueden generarse por medio del módulo de facturación, y, junto con las instrucciones de facturación, son transmisibles a un módulo de compensación.

6. El sistema de acuerdo con la reivindicación 5, **caracterizado por que** los datos de autenticación cumplen con el estándar GSM.

7. El sistema de acuerdo con una de las reivindicaciones 5 o 6, **caracterizado por que** el registrador SIP (51) es un registro SIP.

8. El sistema de acuerdo con una de las reivindicaciones 5 a 7, **caracterizado por que** la transmisión de los datos de autenticación y los datos de registro tiene lugar desde el nodo de IP (10) al registrador SIP (51) a través de una interfaz sin contacto.

9. El sistema de acuerdo con una de las reivindicaciones 5 a 8, **caracterizado por que** el nodo de IP (10) es un teléfono móvil con capacidad IP.



(Estado de la técnica)

FIG. 1

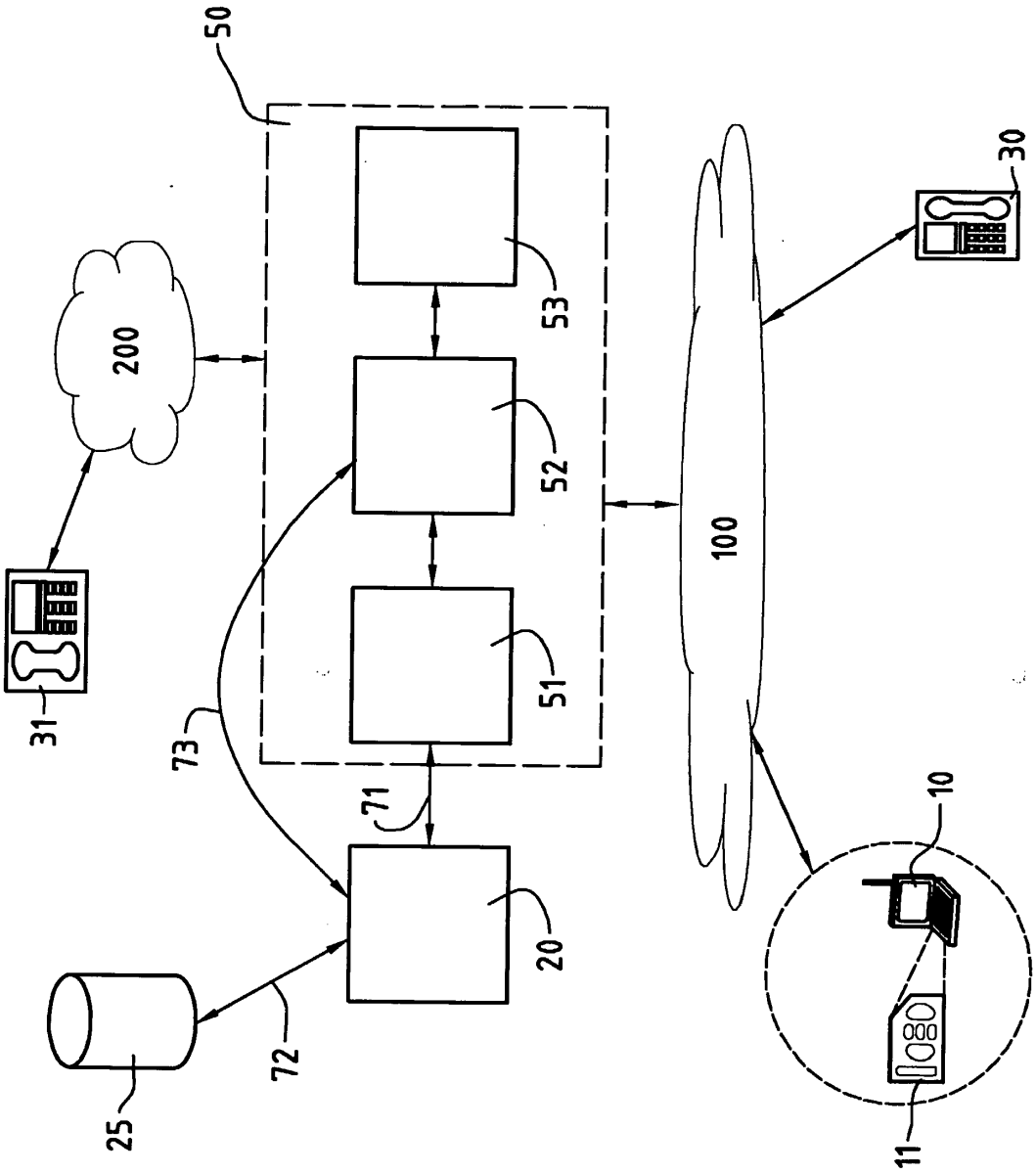


FIG. 2