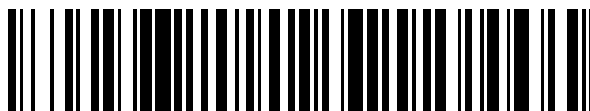


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 617 546**

51 Int. Cl.:

**H04L 29/06** (2006.01)

**H04W 4/06** (2009.01)

**H04W 80/04** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **23.02.2006 PCT/EP2006/060221**

87 Fecha y número de publicación internacional: **30.08.2007 WO07095995**

96 Fecha de presentación y número de la solicitud europea: **23.02.2006 E 06724873 (2)**

97 Fecha y número de publicación de la concesión europea: **14.12.2016 EP 1989853**

54 Título: **Sistema de conmutación y método correspondiente para la unidifusión o multidifusión de transmisiones de flujo de datos de extremo a extremo y/o multimedia entre nodos de red**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**19.06.2017**

73 Titular/es:

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

72 Inventor/es:

**HEUSCHI, WALTER;  
STADELMANN, TONI y  
ZBÄREN, PETER**

74 Agente/Representante:

**DURÁN MOYA, Luis Alfonso**

ES 2 617 546 T3

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

## DESCRIPCIÓN

Sistema de conmutación y método correspondiente para la unidifusión o multidifusión de transmisiones de flujo de datos de extremo a extremo y/o multimedia entre nodos de red

5 La presente invención se refiere a un método y un sistema para la unidifusión o multidifusión unidireccional o bidireccional de transmisiones de flujo de datos de extremo a extremo y/o multimedia en redes heterogéneas, en los que un nodo de red usa una solicitud para solicitar un enlace de datos a uno o más nodos de red desde una unidad de conmutación central en una red IP a través de una interfaz, en los que al menos un nodo de red es un nodo de red IP, cuyos nodos de red se registran con un módulo de registro de la unidad de conmutación central, y se usa un módulo de control de la unidad de conexión central para establecer la conexión entre los nodos de red. La invención se refiere particularmente a un método y un sistema para telefonía basada en IP y telefonía de vídeo en la que los nodos IP se autentican en base a los datos de autenticación de un módulo de identificación antes del registro en la red basada en IP.

15 Las transmisiones de flujo de datos de extremo a extremo y/o multimedia unidireccionales o bidireccionales en las redes IP, en particular la telefonía basada en IP, es una tecnología que se ha desarrollado en los últimos años para formar una alternativa real a la transmisión de datos y voz convencional, por ejemplo, a través de redes telefónicas de circuitos conmutados. Mientras que las llamadas telefónicas convencionales se transmiten como un flujo de datos continuo a través de una red telefónica, la telefonía basada en IP implica que los datos de voz se descomponen en paquetes y se transmiten individualmente a través de una red de datos. Cuando se han dividido y transmitido grandes volúmenes de información de audio a través de la red, estos pequeños paquetes se vuelven a compilar en el extremo de recepción. Esto permite combinar los servicios telefónicos con la red de datos, que dispensa la instalación y el mantenimiento de una red telefónica independiente, ya que los teléfonos basados en IP están conectados a una red de datos a través de una interfaz apropiada y los datos de voz pueden transmitirse utilizando protocolos de red adecuados. Una ventaja importante de las telecomunicaciones basadas en IP sobre la telefonía convencional es la provisión de nuevos servicios que sólo son posibles gracias a la tecnología basada en IP y que representan un valor añadido sobre la telefonía convencional. Entre otras cosas, la telefonía basada en IP proporciona cifrado automático de la comunicación de voz, lo que permite llamadas a prueba de escuchas ilegales. Este desarrollo de la telefonía basada en IP también ha influido en el desarrollo paralelo de la telefonía de vídeo basada en IP como alternativa a la tecnología convencional de videoconferencia. Hoy en día, los enlaces de datos cada vez más rápidos permiten la transmisión simultánea de imágenes y sonido en una calidad excepcional. En el caso de la videotelefonía basada en IP, como en el caso de la telefonía basada en IP, los datos de voz y de imagen se descomponen en paquetes, se envían a través de una red basada en IP y se recompilan en el receptor.

35 Al mismo tiempo, el rápido desarrollo de las redes de datos inalámbricas (WLAN 802.11, Bluetooth, etc.) y un número creciente de lo que se conoce como puntos de acceso en las zonas públicas (por ejemplo en aeropuertos, estaciones de ferrocarril, centros de conferencias, ferias y recintos feriales, plazas muy frecuentadas en las ciudades) han dado como resultado que los aparatos compatibles con IP puedan tener un nivel de movilidad comparable al de las actuales redes de telefonía móvil (GSM, UMTS, etc.). El acceso inalámbrico a servicios, tales como Internet, es ya una cuestión de rutina. Además, los teléfonos móviles basados en IP también han estado disponibles durante algún tiempo, lo que permite la telefonía móvil basada en IP a través de una red inalámbrica de área local. Estos teléfonos de IP móvil ya existen también en versiones con cámaras integradas, lo que significa que de nuevo, la videotelefonía basada en IP móvil está ahora al alcance.

45 Para establecer una comunicación y el intercambio de datos en redes telefónicas y/o videotelefónicas, todos los componentes de la red han de respetar ciertas normas que se estipulan en protocolos o familias de protocolos. Por ejemplo, se conocen en la técnica anterior el protocolo E-DSS1 (Euro-ISDN) para redes telefónicas de circuitos conmutados o los protocolos H.323, SIP, MEGACO o MGCP para telefonía y videotelefonía basada en IP.

50 Uno de los protocolos más utilizados para la telefonía y/o telefonía de vídeo basada en IP es el protocolo de inicio de sesión (SIP, IETF RFC 3261, anteriormente RFC 2543). Éste se especificó por la Internet Engineering Task Force (IETF) por primera vez en 1999. Este protocolo de red tiene una estructura muy simple y se parece mucho al HTTP (protocolo de transferencia de hipertexto (*Hypertext Transfer Protocol*)). Permite establecer una sesión de comunicación entre dos o más abonados. Sin embargo, se trata únicamente de un protocolo de inicio. Para el intercambio de datos, los sistemas de telefonía y/o videotelefonía basados en SIP utilizan otros protocolos, en particular SDP (Protocolo de Descripción de Sesión (*Session Description Protocol*), IETF RFC 2327) y el RTP (protocolo de transporte en tiempo real (*Realtime Transport Protocol*), IETF RFC 1889). SDP se utiliza particularmente para negociar los códecs de audio y/o vídeo, protocolos de transporte, etc., que se van a utilizar entre los puntos finales. La tarea 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 finales de comunicación en un sistema basado en SIP se denominan agentes de usuario. Un cliente de agente de usuario (UAC) se entiende que se refiere a un componente que inicia una solicitud SIP, y el servidor de agente de usuario (UAS) responde a esta solicitud con una respuesta. Un agente de usuario (UA) puede asumir el papel del UAC o del UAS. Las solicitudes, de las cuales hay un número limitado, se responden, en principio, por respuestas (aproximadamente cien diferentes). Simplemente se dan números para distinguirlos. Un agente de usuario envía un mensaje SIP a un proxy

SIP de antemano. En base a la dirección indicada, el proxy decide dónde debe enviarse el mensaje y lo envía. Estos proxies pueden, en principio, no tener estado o tener estado. Mientras que los proxies sin estado simplemente reenvían mensajes y no se percatan de que se está estableciendo una llamada, por ejemplo, los proxies con estado pueden realizar tareas que son útiles para establecer una llamada. Una de las tareas más importantes de un proxy con estado es la distribución de llamadas a varios destinos: en un caso de lo que se conoce como "bifurcación secuencial", los posibles destinos de llamada se marcan sucesivamente, y en el caso de una "bifurcación paralela", todos los destinos reciben un mensaje simultáneamente. Otro componente indispensable de un sistema basado en SIP es un registrador SIP, con el que todos los agentes de usuario necesitan registrarse. Esta unidad lógica gestiona una base de datos que contiene información sobre los agentes de usuario registrados y redirige las solicitudes a estos destinos. Normalmente, el registrador y el proxy son el mismo módulo, que regula la redirección de forma interna sin necesidad de intercambiar mensajes. Finalmente, un sistema basado en SIP también comprende un servidor de redireccionamiento o puerta de enlace, que asegura la conexión entre la red telefónica basada en IP y la PSTN, entre otros.

Para el registro, SIP utiliza el método de registro. El UA indica dónde debe ser alcanzado y recibe la confirmación con el código 200 (OK). Si el usuario no es conocido, se devuelve 404 (no encontrado); si el registro no lo permite, la respuesta es 403 (prohibido). Sin embargo, el requisito previo para el registro satisfactorio es la autenticación satisfactoria del agente de usuario en la red relevante y una verificación sobre su autorización para los servicios requeridos. Para ello, los métodos de autenticación y autorización RADIUS y/o Diameter se utilizan normalmente en un entorno basado en SIP, que también se utiliza para muchas otras funciones de red.

El protocolo de autenticación RADIUS (servicio de usuario de marcación autenticada remota (*Remote Authentication Dial In User Service*) - IETF RFC 2138, 2868) se utiliza actualmente en muchas unidades de red, tales como enrutadores, servidores de módem, conmutadores, etc. El cliente de autenticación envía su nombre de usuario y su contraseña al servidor RADIUS. El servidor RADIUS comprueba esta información y autoriza al usuario en el sistema. La razón de la propagación de RADIUS es, entre otros, que las unidades de red generalmente no pueden manejar un número muy grande de usuarios de la red, cada uno de los cuales tiene información de autenticación diferente, ya que, por ejemplo, esto superaría la capacidad de almacenamiento de las unidades de red individuales. RADIUS permite gestionar centralmente un gran número de usuarios de la red (adición, eliminación de usuarios, etc.). Por ejemplo, en el caso de los ISP (proveedores de servicios de Internet (*Internet Service Providers*)), este es por tanto un requisito previo necesario para el servicio, ya que su número de usuarios con frecuencia comprende varios miles a varias decenas de miles de usuarios. Además, RADIUS ofrece una protección permanente especial contra los piratas informáticos. La autenticación remota de RADIUS basada en TACACS+ (sistema de control de acceso mediante control del acceso desde terminales + (Terminal Access Controller Access Control System +)) y LDAP (protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol)) es relativamente segura contra los piratas informáticos. Por el contrario, muchos otros protocolos de autenticación remota sólo tienen protección intermitente, insatisfactoria o totalmente inexistente contra ataques de piratas informáticos. Otra ventaja de RADIUS es el hecho de que RADIUS fue durante mucho tiempo el estándar de facto para la autenticación remota, lo que significa que RADIUS también es compatible con casi todos los sistemas.

Sin embargo, a medida que aumenta la complejidad del servicio solicitado, se encontró que RADIUS no era adecuado para su uso en redes más grandes. Esto hizo necesario desarrollar un nuevo protocolo. Sin embargo, el protocolo Diameter (IETF RFC 3588) no se reconstruyó desde cero, sino más bien se mantuvo una gran proporción del protocolo RADIUS y se corrigieron los errores en el mismo. Como RADIUS, Diameter utiliza pares de atributo/valor (AVP) para transmitir datos y UDP como protocolo de transporte. Además, se puede ampliar añadiendo nuevos comandos y AVP. Es un protocolo básico que cumple los requisitos mínimos de un protocolo de transporte de autenticación. Por lo tanto, no se pretende que se utilice por sí solo, sino que debe utilizarse siempre con una extensión específica de la aplicación. Diameter es un protocolo de punto a punto. Normalmente, el cliente Diameter inicia una solicitud de autenticación o autorización de un usuario. El servidor Diameter recibe esta solicitud y la responde o la envía a un servidor proxy. El nodo móvil solicita el servicio requerido utilizando el mensaje de solicitud de autenticación (AMR), que contiene los AVP. La información requerida para la autenticación se extrae de este mensaje y se incluye en los AVP de Diameter. Este mensaje se envía al servidor Diameter local, que denomina AAAF. El AAAF envía el mensaje al servidor de inicio de autenticación (AAAH). Si el AAAH es capaz de autenticar al usuario con éxito, envía una solicitud MIP de agente local (HAR) a un agente local. Después de haber recibido el HAR, este agente local procesa en primer lugar el mensaje de Diameter y luego produce la respuesta HAA con los datos requeridos, tal como la ID de sesión, etc., y lo envía al AAAH. Esto último produce la respuesta de autenticación (AMA), que contiene información para el túnel de mensajes, entre otros, y lo envía al AAAF. Así, se establece la conexión. La extensión IP móvil define además numerosos casos especiales, tales como el manejo de traspasos.

Además de la autenticación y la autorización, una red de telefonía y/o telefonía de vídeo basada en IP requiere mecanismos de facturación adecuados. El protocolo TAP (procedimiento contable transferido (Transferred Account Procedure)) del grupo de intercambio de datos de la cuenta transferida de la asociación GSM (TADIG (GSM association's Transferred Account Data Interchange Group)) es el protocolo conocido en la técnica anterior para la facturación del servicio solicitado por las unidades móviles en las redes GSM. Un concepto muy importante en las redes GSM es la itinerancia, un método que permite a un usuario de radio móvil utilizar su radio móvil, no sólo en su red original, sino también en cualquier red deseada en casa o en el extranjero. Sin embargo, este método requiere

un concepto de facturación que puede traer la complejidad de los protocolos y los diversos servicios proporcionados sin error. Por lo tanto, los métodos de facturación para las redes GSM no deben ser en modo alguno triviales. Hoy en día, más de 400 redes GSM están en operación en todo el mundo y también se estima que hay más de 20.000 acuerdos de itinerancia individuales existentes entre los operadores de redes individuales. Para permitir la facturación, la idea aparentemente sencilla de itinerancia oculta un proceso extremadamente complejo de registro de información, distribución de información y evaluación de información. A este respecto, se utiliza el protocolo de procedimiento contable transferido (TAP) para el intercambio de información de facturación de itinerancia entre los distintos proveedores de servicios de red de telefonía móvil. El 4 de junio de 2000, TAP2 y TAP2+ se siguieron finalmente del lanzamiento de TAP3. Ya existen las subversiones TAP3.1 y TAP3.2. TAP3 puede denominarse hoy en día como el estándar, aunque TAP es un protocolo en evolución.

La mayor parte del tráfico de voz o datos en redes GSM entra o termina en una red diferente de la que está actualmente el usuario móvil. El operador de una red local cobra por cada llamada que termina en uno de sus usuarios, independientemente de si está implicada una red fija o una red móvil. Para simplificar la recaudación de cargos, los operadores de redes fijas locales establecen acuerdos mutuos con los operadores de redes de telefonía móvil locales. Por lo tanto, un operador de red móvil en un país no necesita celebrar un acuerdo con el proveedor de red de telefonía fija en otro país para facturar una llamada desde la red de telefonía móvil del primer proveedor a la red fija del segundo proveedor. Normalmente, el proveedor de la red de telefonía fija en el primer país ya ha celebrado un acuerdo sobre el tipo de facturación y los cargos con el proveedor de la red de telefonía fija en el segundo país, de manera que el operador de la red móvil en el primer país pueda entonces facturar por sus servicios a través del proveedor de la red fija con un acuerdo apropiado. Los costes suelen ser facturados al usuario directamente (facturación al por menor) o a través de un proveedor de servicios (facturación al por mayor). El tipo de facturación del tráfico de datos de itinerancia o de voz entre diferentes redes móviles (PMN: red móvil pública (Public Mobile Network)) se realiza usando el protocolo TAP. Los registros de llamadas de itinerancia se producen típicamente como registros TAP o CIBER (registro de intercambio de facturación entre proveedores móviles (Cellular Inter-carrier Billing Exchange Roamer)). Los registros CIBER se usan por operadores de redes de telefonía móvil que utilizan tecnologías basadas en AMPS, tales como AMPS, IS-136 TDMA e IS-95 CDMA. TAP se usa principalmente por los proveedores de servicios de red móvil GSM/UMTS y es el principal protocolo de facturación en las áreas dominadas por GSM/UMTS.

Los detalles de una llamada de un usuario que está en una red ajena (VPMN: red móvil pública visitada (Visited Public Mobile Network)) están registrados en un centro de conmutación móvil (MSC) de la red. Por lo tanto, cada llamada produce uno o más registros de llamadas. El estándar GSM para estos registros se define en GSM 12.05, aunque muchos proveedores utilizan sus propios formatos. Los registros de llamadas del MSC se transmiten a un sistema de facturación en la VPMN para la facturación. Estos registros de llamada se convierten entonces a formato TAP y se asocian con el usuario correspondiente. A más tardar dentro de un tiempo predefinido (por ejemplo, 36 horas), los registros TAP se envían a los proveedores de servicios de red móvil correspondientes. Los ficheros TAP contienen además información relativa a la tarifa de servicio del proveedor (IOT: tarifa entre operadores (Inter Operator Tariff)) y a todos los demás acuerdos bilaterales y regímenes de prestaciones. Los registros TAP se envían directamente, o más habitualmente, a través de un centro de facturación, tal como una cámara de compensación. Cuando el operador de red de origen (HPMN: red móvil pública de origen (Home Public Mobile Network)) recibe un registro TAP de la VPMN, se convierte en un formato interno apropiado y se factura junto con los registros de llamadas normales del usuario que se producen en la red doméstica. En el caso de una facturación al por mayor, en la que un proveedor de servicios factura los costes incurridos al usuario, la HPMN remite los registros al proveedor de servicios, que puede facturar de nuevo las llamadas, particularmente en base a sus propias tarifas, y produce, a modo de ejemplo, la factura con los detalles de las llamadas para el usuario.

TAP3 soporta una multiplicidad de servicios. En la actualidad, TAP3 se utiliza para la facturación entre los proveedores de servicios GSM/UMTS y los proveedores de servicios GSM/UMTS, los proveedores de servicios GSM/UMTS y los proveedores de servicios no GSM (itinerancia interurbana) y los proveedores de servicios GSM y los proveedores de servicios por satélite. Las categorías fundamentales de servicio, voz, fax y lo que se conoce como servicios complementarios, ya se han soportado desde TAP1. Por el contrario, la facturación del servicio de mensajes cortos (SMS) es menos trivial debido al uso de centros de servicio de mensajes cortos (SMS-C) pertenecientes a terceros. La facturación de SMS es más difícil por las siguientes razones: 1. Un usuario itinerante puede recibir un SMS durante la itinerancia (MT-SMS), 2. Un usuario itinerante puede enviar un SMS durante la itinerancia (MO-SMS) utilizando el SMS-C de su red doméstica, y 3. Un usuario itinerante puede enviar un SMS durante la itinerancia (MO-SMS) mediante el SMS-C de una red ajena. Por lo tanto, la facturación para servicios de SMS no es totalmente compatible hasta TAP2+. Desde TAP3 en adelante, también se admite la facturación de datos de conmutación de circuitos, HSCSD (datos de circuitos conmutados de alta velocidad) y GPRS (servicio radioeléctrico general por paquetes (General Packet Radio Service)). TAP3 soporta igualmente todos los servicios de valor añadido (VAS), tal como lo que se conoce como facturación de contenido. Sin embargo, la facturación de servicios de valor añadido es a menudo difícil, ya que presupone que el proveedor de servicios está de acuerdo con los servicios facturados. Desde la introducción de TAP3.4 se ha soportado la lógica mejorada de la aplicación a la medida de la red móvil (CAMEL). CAMEL es particularmente importante para aplicaciones en servicios de prepago para usuarios itinerantes y debería ser muy importante en el futuro. Otra aplicación importante de TAP3 es la compatibilidad con la facturación basada en tarifas interoperadoras (IOT). IOT permite que el proveedor de servicios

de red doméstica (HPMN) compruebe ofertas y tarifas específicas de un proveedor de servicios ajeno (VPMN) y los transmita al usuario itinerante. Por lo tanto, a modo de ejemplo, la VPMN puede proporcionar beneficios o descuentos para diferentes servicios o niveles de llamada y la HPMN puede verificarlos fácilmente y ajustar sus tarifas. La oportunidad de facturar servicios de itinerancia independientemente del lugar en el que se encuentra el usuario es una herramienta valiosa para los proveedores de servicios de red móvil y evita la pérdida de ingresos cuando una VPMN proporciona beneficios temporalmente. El protocolo TAP también comprende información detallada, desde TAP en adelante, respecto a desde dónde se realizó una llamada con precisión, o se usó un servicio, etc., y donde se realizó. Esta información ayuda a establecer un perfil del usuario respectivo sobre la base de su comportamiento, lo que proporciona información importante para ajustar y optimizar los servicios prestados en función de las necesidades de los usuarios. En particular, puede utilizarse para proporcionar servicios basados en una localización específica, tales como eventos deportivos o conciertos, etc. Finalmente, el protocolo del procedimiento de contabilidad devuelta (PAP) significa que TAP3 también permite un manejo diferenciado de los errores. Por lo tanto, RAP permite a la HPMN verificar los ficheros TAP entrantes, entre otros, para determinar la validez y el cumplimiento de la norma TAP y si es necesario rechazarlos en parte, sin perder por ello la facturación por los servicios que se han transmitido correctamente.

En la interfaz entre la telefonía y/o la telefonía de vídeo basada en IP y las redes telefónicas convencionales, es necesario, en principio, resolver problemas similares a los de la facturación de llamadas entre dos operadores de redes de telefonía móvil diferentes. En primer lugar, suele haber un gran número de operadores y, en la práctica, se puede suponer que cada uno de estos operadores utiliza su propio modelo arancelario. En segundo lugar, un cliente de un operador puede llamar a clientes arbitrarios de otro operador, lo que se reflejará en mayores cargos en las llamadas. Pueden encontrarse recomendaciones generales para efectuar pagos compensatorios en ITU recommendation D. 196, por ejemplo. Sin embargo, para el procedimiento estándar de compensación y liquidación no existen estándares y protocolos públicamente accesibles. Además, hay varios proveedores para una cámara de compensación que, en particular, pueden ser utilizados por los operadores de telefonía móvil para la facturación de tarifas de itinerancia. Sin embargo, una característica común de todos estos proveedores es que tampoco se utilizan estándares públicamente accesibles.

Para que sea posible cobrar por una llamada entre dos proveedores a través de un punto central, todos los proveedores han de usar un protocolo estándar. Para estos fines, la empresa TransN-exus ha especificado el protocolo de establecimiento abierto (OSP), que ETSI ha declarado como el estándar en su especificación TIPHON. En primer lugar, OSP define un marco básico para el intercambio estandarizado de información. En segundo lugar, la especificación también proporciona conscientemente partes del protocolo que pueden reemplazarse o ampliarse. Por lo tanto, también es posible incorporar requisitos especiales y servicios específicos del operador.

El protocolo de transmisión utilizado en el OSP es una combinación de HTTP y S/MIME. Para la transmisión, se utiliza el método POST de HTTP. Aunque el método PUT también existe para transmitir datos a un servidor utilizando HTTP, sólo puede usarse el método POST para asignar los datos que también se transmiten a un recurso de servidor particular que procesa los datos adicionalmente. Además, el contenido de los datos transmitidos comprende un mensaje S/MIME. Para alinear los mensajes OSP con una cámara de compensación, existen dos modos de operación: el modo en línea y el modo masivo. En el modo en línea, existe una conexión con la cámara de compensación mientras se realiza una llamada entre los distintos operadores de red. La razón de este enfoque es que la cámara de compensación puede realizar algunas tareas para configurar la llamada. Si, a modo de ejemplo, el servicio de fondo asociado con la persona que llama tiene demasiado poca información sobre el destino de la llamada, la cámara de compensación puede tomar decisiones de enrutamiento y puede proporcionar una dirección de contacto para el controlador de acceso de destino. Además, es concebible incorporar la funcionalidad de un agente de área de servicio (SAB) en la cámara de compensación. La tarea de un SAB es determinar la mejor manera de establecer la llamada, lo que puede implicar tener en cuenta las tarifas basadas en la hora del día y los niveles de carga actuales en las redes. Sin embargo, el inconveniente del modo en línea es un aumento en el tiempo de retraso para el establecimiento de la conexión, porque en última instancia, el guardián de la persona que llama debe esperar no sólo varias respuestas de su propio servicio de respaldo, sino también respuestas de la cámara de compensación. Por otra parte, en el modo masivo, sólo se establece una conexión a la cámara de compensación en los momentos prescritos. Una ventaja de este método es que un proceso que es independiente del guardián puede leer los CDR del servicio de respaldo y puede transmitirlos a la cámara de compensación sin interrupción. Otra ventaja, a diferencia del modo en línea, es que una ausencia temporal de la cámara de compensación no da lugar a interrupciones significativas en el propio sistema. Esto se debe a que si una transferencia de CDR se termina o no sucede, puede repetirse fácilmente en un momento posterior. Sin embargo, un inconveniente significativo que puede observarse es que una cámara de compensación no puede actuar como un SAB en el modo masivo. Además, la cámara de compensación no puede tomar decisiones de enrutamiento, ya que esto también puede hacerse sólo en el modo en línea. Los componentes más importantes de un mensaje OSP son el intercambio de precios, el intercambio de autorizaciones y el intercambio de uso. El intercambio de precios comprende el intercambio de información para los costes de una llamada telefónica. Este intercambio de precios comprende la transmisión de una indicación de precios, que debe confirmarse con una confirmación de precios. El intercambio de autorizaciones se realiza cuando los recursos deben ser utilizados por la cámara de compensación. Normalmente, esto corresponde a una autorización para el establecimiento de una llamada telefónica. Al igual que el intercambio de precios, el intercambio de autorización también se basa en la transmisión de una solicitud de autorización, que se confirma con

una respuesta de autorización. El intercambio de uso contiene una descripción de los recursos utilizados. Para ello, se envía una indicación de uso que se confirma con una confirmación de uso. Dado que el OSP todavía no puede distinguir ningún servicio, el término uso debe entenderse como el tiempo de llamada para una llamada telefónica realizada.

5 Sin embargo, la telefonía basada en IP y la telefonía de vídeo en la técnica anterior están asociadas a inconvenientes considerables. Aunque hoy es posible autenticar a los participantes de la llamada en una red basada en IP utilizando mecanismos de autenticación y autorización como se describe, y verificar su autorización para  
10 determinados servicios, estos métodos de autenticación y autorización son bastante complicados y tampoco cumplen los altos estándares con respecto a seguridad, facturación y autorización de servicio, tal como se proporcionan en las redes telefónicas convencionales. En particular, las redes de telefonía móvil GSM/UMTS proporcionan normas de autenticación y autorización que no pueden implementarse en una red basada en IP debido a sus características intrínsecas. Esto se debe a que la arquitectura abierta del protocolo IP carece de una gran cantidad de información que es absolutamente necesaria para una compatibilidad total con las redes GSM.

15 Por lo tanto, un objeto de la invención es proponer un método y un sistema novedosos y mejorados para transmisiones de flujo de datos y/o multimedia de extremo a extremo unidireccionales o bidireccionales en redes heterogéneas. En particular, este método y sistema novedosos y mejorados están destinados a permitir a los usuarios de telefonía y/o telefonía de vídeo basados en IP disponer de los mismos estándares de registro o autenticación y  
20 autorización que los que están acostumbrados a la telefonía convencional, tal como la telefonía móvil GSM.

De acuerdo con la presente invención, estos objetivos se consiguen particularmente por los elementos de la parte caracterizadora de las reivindicaciones independientes. Otras realizaciones ventajosas también se revelan por las reivindicaciones dependientes y la descripción.

25 En particular, la invención logra estos objetos ya que, para la unidifusión o multidifusión unidireccional o bidireccional de transmisiones de flujo de datos y/o multimedia de extremo a extremo en redes heterogéneas, un nodo de red usa una solicitud para solicitar un enlace de datos a uno o más nodos de red de una unidad de conmutación central en una red IP a través de una interfaz, en la que al menos un nodo de red es un nodo de red IP y al menos algunos de los nodos de red se registran con un módulo de registro de la unidad de conmutación central, y en la que un módulo de control de la unidad de conexión central se usa para establecer la conexión entre los nodos de red, ya que para el fin de la transmisión de flujo de datos y/o multimedia, al menos un nodo de red IP de una IMSI, almacenada en una tarjeta SIM del nodo de red IP, se transmite al módulo de registro bajo la petición del módulo de registro y la IMSI se almacena en una base de datos de usuario del módulo de registro, ya que un módulo de puerta de enlace de señalización se usa para complementar el canal de datos IP para formar canales de señales y datos de una red GSM, y el al menos un nodo de red IP se autentica tomando los datos GSM complementados de forma correspondiente como base para la generación de las funciones SS7/MAP necesarias, ya que el módulo de registro usa la base de datos de usuario y el módulo de puerta de enlace de señalización para autenticar el nodo de red IP sobre la base de la IMSI de la tarjeta SIM del al menos un nodo de red IP en un HLR y/o VLR y/o AuC y/o una base  
30 de datos funcionalmente equivalente, y ya que tras una autenticación satisfactoria, al menos un nodo de red IP recibe una entrada apropiada en la base de datos de usuario del módulo de registro, en la que el enlace de datos al uno o más nodos de red se establece por medio de un módulo de control de la unidad de conexión central. La invención tiene, entre otros, la ventaja de que es posible una autenticación y/o autorización segura y conveniente de los usuarios para una unidifusión o multidifusión unidireccional o bidireccional de transmisiones de flujo de datos y/o multimedia de extremo a extremo en redes heterogéneas, particularmente redes IP, usando una unidad de conmutación central, como se conoce a partir de la telefonía móvil GSM. En esta solicitud, "unidifusión" se entiende generalmente que significa un enlace de datos bidireccional y/o unidireccional de extremo a extremo entre dos nodos de red individuales, mientras que "multidifusión" se tiende en general de forma similar que significa un enlace de datos bidireccional y/o unidireccional de extremo a extremo entre uno y una pluralidad de nodos de red.

50 En una variante de realización, las transmisiones de flujo de datos y/o multimedia pueden comprender, a modo de ejemplo, particularmente telefonía y/o videotelefonía basada en IP. La telefonía y/o videotelefonía basada en IP puede basarse, al menos en parte, en el protocolo de inicio de sesión (SIP), en las que el módulo de control en la unidad de conexión central comprende un elemento de red proxy SIP, y en las que el módulo de registro comprende un elemento de red de registro SIP. Al menos un nodo de red IP puede ser un teléfono móvil compatible con IP o puede comprender un módulo apropiado. Esto tiene la ventaja, entre otras cosas, de que es posible una autenticación y/o autorización segura y conveniente de los usuarios en una red telefónica y/o videotelefónica basada en IP. Mediante la combinación de telefonía y/o videotelefonía basada en IP con un método conveniente y seguro, se hace posible la autenticación y/o autorización altamente salvaguardada y probada de los usuarios, como se conoce por la telefonía móvil GSM. El uso del protocolo SIP tiene la ventaja, entre otros, de que el protocolo SIP es una alternativa muy utilizada en las redes de telefonía y/o videoteléfono basadas en IP. SIP es fácil de implementar, se modela en el protocolo HTTP y permite un alto nivel de flexibilidad para una amplia variedad de aplicaciones. Igualmente, ya hay muchos productos en el mercado hoy en día que soportan protocolos SIP.

65 En otra variante de realización, tras una autenticación satisfactoria del nodo de red IP, se realiza una actualización de ubicación en el HLR y/o el VLR y/o AuC y/o una base de datos funcionalmente equivalente y los datos apropiados

se transmiten al módulo de registro. Esto tiene la ventaja de que además es posible que se realice de forma centralizada un tipo simple de control de sesión. El control de sesión resultante puede realizarse además del control de sesión en la unidad de conexión central.

5 En otra variante de realización, la autenticación por medio de la IMSI se toma como base para conceder la autorización de servicio apropiada para utilizar la unidad de conexión (10) y/o para la facturación del servicio solicitado mediante un módulo de facturación. Esta variante de realización tiene la ventaja, entre otras, de que puede realizarse una facturación simple para el servicio solicitado. A modo de ejemplo, por lo tanto, la facturación puede asignarse también directamente por medio de sistemas de facturación de proveedores de servicios en redes GSM  
10 sin la necesidad de alterar en modo alguno las infraestructuras existentes. A modo de ejemplo, la facturación también puede realizarse mediante la transmisión de registros detallados de llamadas producidos por medio del módulo de control y/o el nodo de red IP al módulo de registro, detectando el módulo de registro al menos la identidad del nodo de red IP y/o el periodo y/o el proveedor del servicio solicitado, y enviarlo/enviarlos a un módulo de facturación, y produciendo el módulo de facturación ficheros de facturación en línea con el servicio solicitado en base a los datos de facturación del módulo de registro y sobre la base de los registros detallados de llamadas, y transmitiéndolos con instrucciones de facturación a un módulo de compensación. La autenticación por medio de la  
15 unidad de conexión también se puede realizar, a modo de ejemplo, sólo si la solicitud de conexión y/o el establecimiento de conexión proceden de un nodo de red IP. Este es el caso en particular si la autenticación se utiliza sólo para realizar la facturación, por ejemplo. Si la solicitud procede de un nodo de red distinto de un nodo de red IP, tal como, por ejemplo, desde un dispositivo de red GSM, también pueden utilizarse, si están disponibles, los métodos de facturación que son típicos de esta red. El uso de los registros detallados de llamadas tiene la ventaja, entre otras, de que la facturación de los servicios solicitados puede gestionarse fácilmente por medio de un módulo de compensación, en particular en el caso de compensación entre los diversos operadores de red.

25 Aún en otra variante de realización, uno o más nodos IP pueden autenticarse utilizando el protocolo de autenticación extensible. Esto tiene la ventaja, entre otros, de que, en combinación con RADIUS, por ejemplo, se produce un método completo, independiente del hardware. En particular, EAP proporciona los mecanismos de seguridad necesarios para realizar la autenticación.

30 En principio, en lugar de la tarjeta SIM del nodo IP, también es posible utilizar cualquier módulo de identificación. Sin embargo, la tarjeta SIM tiene la ventaja, entre otros, de que la tarjeta SIM es un medio ampliamente utilizado y probado para identificar nodos IP, particularmente nodos IP móviles. Igualmente cumple los altos estándares de seguridad y, como resultado de su pequeño tamaño, también puede intercambiarse o transportarse fácilmente. Además, los costes de fabricación, de tal tarjeta SIM son bajos en comparación con otros mecanismos de  
35 identificación similares.

En una variante de realización, se utilizan datos de autenticación que cumplen la norma GSM. Esta variante de realización tiene la ventaja, entre otras, de que se puede usar una infraestructura GSM existente de un proveedor sin modificaciones relativamente grandes. En este caso, se crean perfiles de usuario para los usuarios de telefonía y/o videotelefonía basados en IP, al igual que para los usuarios de telefonía móvil convencional. Además, esto permite utilizar los criterios de seguridad existentes en la tecnología GSM.  
40

En otra variante de realización, los datos de autenticación se transmiten desde el nodo de red IP al módulo de registro utilizando una interfaz sin contacto. Esta variante de realización tiene la ventaja, entre otras cosas, de que pueden utilizarse nodos IP móviles, lo que permite una mayor movilidad de los usuarios de la telefonía basada en IP y/o telefonía móvil, comparable con la telefonía móvil.  
45

En otra variante de realización, los datos de autenticación se transmitirán desde el nodo IP al módulo de registro utilizando una interfaz WLAN 802.11 y/o Bluetooth y/o GSM y/o UMTS. Esto tiene la ventaja de que se pueden utilizar redes conocidas y establecidas para transmitir datos de autenticación, lo que significa que pueden utilizarse las instalaciones existentes (zonas públicas).  
50

En este punto, cabe señalar que la presente invención se refiere no sólo al método según la invención, sino también a un sistema para realizar este método.  
55

A continuación se describen variantes de realización de la presente invención con referencia a ejemplos. Los ejemplos de las realizaciones se ilustran mediante las siguientes figuras adjuntas:

La figura 1 muestra un diagrama de bloques que ilustra esquemáticamente un método según la invención y un sistema de acuerdo con la invención para transmisiones de datos y/o multimedios unidireccionales o bidireccionales de unidifusión o multidifusión en redes heterogéneas, particularmente para telefonía y/o videotelefonía basada en IP, en el que los nodos IP -40-/-41- comprenden un módulo de identificación -401-/-411- y utilizan una red de datos -30- para acceder a una unidad de conmutación -10- o infraestructura apropiada para las transmisiones de datos o establecimiento de enlaces de datos. El aparato de conexión -10- comprende un módulo de puerta de enlace de señalización -20-, un módulo de control -21-, un módulo de registro -22- y una pasarela IP/PSTN -23-, que se utiliza para establecer una comunicación con los teléfonos -50-, ..., -55- conectados por medio de la red de telefonía  
60  
65

pública conmutada -31/-32-.

La figura 2 muestra un diagrama de bloques que ilustra esquemáticamente un método y un sistema de telefonía o videotelefonía basada en IP en la técnica anterior. En este caso, los nodos IP -40-, ..., -42- utilizan una red de datos -30- para acceder a un sistema o una infraestructura apropiada para telefonía y/o videotelefonía basada en IP -60-.

5 Esta infraestructura para telefonía y/o videotelefonía basada en IP -60- comprende un módulo de registro -61-, un módulo de control -62- y una puerta de enlace IP/PSTN -63-, que se utiliza para establecer comunicación con los teléfonos -50-, ..., -53- conectados por medio de la red de telefonía pública conmutada -31-.

10 La figura 1 ilustra una arquitectura que puede usarse para implementar la invención. En la figura 1, el símbolo de referencia -40/-41- se refiere a un nodo de red IP que tiene la infraestructura necesaria, incluyendo todos los componentes de hardware y software, para implementar un método y/o un sistema de acuerdo con la invención como se describe. Se entiende por nodos de red IP -40/-41-, entre otros, todos los posibles "equipos de premisas de cliente" (CPE) proporcionados para su uso en diversas ubicaciones de red y/o con diversas redes. Este equipo comprende, a modo de ejemplo, teléfonos y/o videoteléfonos basados en IP, y también cualquier otro aparato compatible con IP, tal como PDA, portátiles o teléfonos móviles. Los nodos IP -40/-41- tienen una o más interfaces de red físicas diferentes, que también pueden soportar varios estándares de red diferentes. A modo de ejemplo, estas interfaces de red físicas del nodo IP -40/-41- pueden comprender interfaces sin contacto para WLAN (red de área local inalámbrica (Wireless Local Area Network)), Bluetooth, GSM (sistema global para comunicaciones móviles (Global System for Mobile Communication)), GPRS (servicio de radiocomunicaciones por paquetes generalizados (Generalized Packet Radio Service)), USSD (datos de servicios complementarios sin estructurar, (Unstructured Supplementary Services Data), etc. Sin embargo, también pueden ser interfaces de red físicas para Ethernet, Token Ring u otra LAN cableada (Red de área local). Por lo tanto, los símbolos de referencia -30/-31/-32- son las diversas redes, por ejemplo una LAN inalámbrica (basada en IEEE 802. 1x), una red Bluetooth, una LAN cableada (Ethernet o Token Ring), o bien una red de radio móvil (GSM, UMTS, etc.) o una red PSTN. Las interfaces de red físicas del nodo IP -40/-41- pueden ser no sólo interfaces de conmutación de paquetes, como se usan directamente por los protocolos de red, sino también interfaces de conmutación de circuitos, que pueden usarse por medio de protocolos tales como PPP (protocolo punto a punto (Point to Point Protocol)), SLIP (protocolo de Internet en línea en serie (Serial Line Internet Protocol)) o GPRS (Generalized Packet Radio Service) para la transferencia de datos.

30 Además, el nodo IP -40/-41- comprende un módulo de identificación -401/-411-. Este módulo de identificación -401/-411- puede implementarse en hardware o en software y puede estar conectado al nodo IP -40/-41- por medio de una interfaz de contacto o sin contacto, o puede estar integrado en el nodo IP -40/-41-. En particular, el módulo de identificación -41- puede estar en forma de una tarjeta SIM, como se conoce a partir de los teléfonos móviles. Este módulo de identificación -401/-411- contiene, entre otros, los datos de autenticación que son relevantes para autenticar el nodo IP -40/-41- en una red basada en IP para telefonía y/o videotelefonía. Estos datos de autenticación pueden comprender, en particular, una IMSI (identidad internacional del abonado móvil (International Mobile Subscriber Identifier)) y/o TMSI (identificador de abonado móvil temporal (Temporary Mobile Subscriber Identifier)) y/o LAI (identidad de área de localización (Location Area Identity)), etc., que se basan en el estándar GSM.

40 Para registrar el nodo IP -40/-41- para transmisiones unidireccionales o bidireccionales de unidifusión o multidifusión de transmisión de flujo de datos y/o multimedia de extremo a extremo, particularmente telefonía y/o videotelefonía basada en IP en redes heterogéneas -30/-31/-32-, un nodo de red utiliza una solicitud para solicitar un enlace de datos a uno o más nodos de red desde una unidad de conexión central -10- en una red IP -30- a través de una interfaz basada en contacto o sin contacto. En principio, se entiende que la conexión punto a punto (unidifusión) significa que se refiere a todas las conexiones directas entre dos abonados de red de punto a punto. Esto incluye las conexiones punto a punto y de extremo a extremo. En este contexto, las conexiones punto a punto funcionan sin una estación intermedia de conmutación real. Cubren la comunicación en las capas de red inferiores (1-3 en el modelo OSI). Las conexiones de extremo a extremo también cubren todas las conexiones en las capas de red más altas (4-7 en el modelo OSI). En el caso de la comunicación de extremo a extremo, siempre se utiliza una estación intermedia para la transferencia de llamadas. También se hace referencia en este contexto a una comunicación multisalto. La multidifusión denota la transmisión de datos en grupos (también denominada conexión multipunto). Para la multidifusión, los datos se transmiten a una pluralidad de abonados simultáneamente o a un grupo de abonados cerrado, usualmente sin multiplicar el ancho de banda por el número de receptores en el transmisor. Para multidifusión, el transmisor requiere sólo el mismo ancho de banda que un único receptor. Si se realiza la transmisión de datos orientada a paquetes, los paquetes se duplican en cada distribuidor (conmutador, enrutador) en la ruta. La multidifusión IP permite enviar datos de forma eficiente en redes TCP/IP a un gran número de receptores al mismo tiempo. Esto puede hacerse usando una dirección multidifusión específica. En IPv4, el rango de direcciones 224.0.0.0 a 239.255.255.255 (clase D) está reservado para esto, y en IPv6 cada dirección que comience con FFOO. Además, el protocolo IGMP se utiliza para la coordinación en IPv4. En IPv6, ICMPv6 puede realizar la función de control. En este documento, la unidifusión y la multidifusión también están destinadas explícitamente a ser entendidas como conexiones bidireccionales, es decir, los suscriptores de grupos individuales pueden comunicarse y transmitir datos a todos los demás. El sistema de conmutación de acuerdo con la invención comprende dicha unidad central de conexión -10- para generar enlaces de datos entre dos más nodos de red -40-, ..., -42/-50-, ..., -55/-60- sobre la base de una solicitud del nodo de red. Los nodos de red -40-, -42/-50-, -55/-60- comprenden al menos un nodo de red IP -40/-41-. La unidad de conexión central -10- comprende un módulo de registro -22- para registrar el nodo de red y comprende un módulo de control -21- para establecer la conexión entre



los nodos de red. Como se ha mencionado, al menos un nodo de red IP -40/-41- comprende una tarjeta SIM -401/-411- para almacenar una IMSI y también se refiere a transmitir la IMSI al módulo de registro 22 bajo petición. El IMSI puede almacenarse en una base de datos de usuario en el módulo de registro -22-. Para autenticar el uno o más nodos IP -40/-41-, la unidad de conexión central puede usarse el protocolo de autenticación extensible, por ejemplo. El sistema de conmutación también comprende un módulo de puerta de enlace de señalización -20- para complementar el canal de datos IP lógico para formar canales de señales y datos en una red GSM. Se usa un módulo de puerta de enlace MAP -25- para generar las funciones SS7/MAP necesarias para la autenticación del al menos un nodo IP -20-. Puede tener sentido para el módulo de puerta de enlace de señalización -20- y el módulo de puerta de enlace MAP -25- implementarse juntos en un único módulo. El módulo de registro -22- autentica el al menos un nodo de red IP -40/-41- usando la base de datos de usuario y el módulo de puerta de enlace de señalización -20- sobre la base de la IMSI de la tarjeta SIM -401/-411- de al menos un nodo de red IP -40/-41- en un HLR y/o VLR y/o AuC -26- y/o una base de datos funcionalmente equivalente. Tras la autenticación satisfactoria del al menos un nodo de red IP -40/-41- en la base de datos de usuario del módulo de registro -22-, se almacena una entrada apropiada y/o el enlace de datos al uno o más nodos de red se establece por medio de una módulo de control -21- en la unidad de conexión central -10-.

A modo de ejemplo, el nodo IP -40/-41- utiliza la interfaz a la red basada en IP -30- para solicitar acceso a un servicio de telefonía y/o telefonía de vídeo. Como ya se ha descrito, la red basada en IP -30- puede comprender varios estándares y protocolos de red, tales como redes inalámbricas WLAN 802.11 o Bluetooth o bien redes cableadas Ethernet o Token Ring, etc. La unidad de conexión central 10 comprende una pasarela IP/PSTN -23-, que asegura la conexión entre la red basada en IP -30- y la red de telefonía pública conmutada (PSTN) -31- y/o la red de telefonía móvil -32-. Es importante mencionar que la puerta de enlace IP/PSTN -23- puede ser operada de manera integrada con respecto a la unidad de conmutación central 10 y/o de forma remota con respecto a la unidad de conmutación central -10- a través de la red IP -30-. Las redes de telefonía móvil -32- también se pueden acceder a través del módulo de puerta de enlace de señalización -20-. La infraestructura pueden construirse de acuerdo con los requisitos del protocolo SIP (protocolo de iniciación de sesión) y/o H.323 y/o MGCP (protocolo de control de puerta de enlace de medios) y/o MEGACO (control de puerta de enlace de medios) para telefonía y/o videotelefonía basada en IP. Una solicitud de registro contiene los datos de autenticación del módulo de identificación -401/-411- del nodo IP -40/-41- y datos de registro para el registro en la red telefónica y/o videotelefónica basada en IP. En particular, los datos de autenticación pueden contener la IMSI de una tarjeta SIM basada en GSM. Esta petición de registro se transmite al módulo de registro -22- de la red de teléfono y/o videoteléfono basada en IP, por ejemplo a un registro SIP. Los datos de autenticación se separan de los datos de registro por el módulo de registro -22- y se transmiten a un módulo de autenticación, tal como un AuC (Centro de autenticación). En base a los datos de autenticación, se generan las funciones necesarias de autenticación y/o autorización y/o configuración, de manera que el módulo de autenticación realice la autenticación y/o autorización para el nodo IP -40/-41- sobre la base de los datos de autenticación del módulo de identificación -401/-411- del nodo IP -40/41- en un registro de localización de origen HLR y/o un registro de localización de visitante (VLR) y/o un centro de autenticación y/o una base de datos funcionalmente equivalente -26-. Como se menciona, esta base de datos -26- puede ser o comprender, en particular, un registro de ubicación de origen (HLR) para una red GSM y puede contener perfiles de usuario adecuados. También es concebible autenticar el nodo IP -40/-41- simplemente usando la IMSI del módulo de identificación -401/-411- del nodo IP -40/-41- en una o más de las etapas en la autenticación, mientras que la IMSI se reemplaza por una IMSI generada temporalmente (llamado TMSI) para todas las demás etapas de autenticación.

Para el método de autenticación, es posible utilizar en particular el siguiente método pregunta-respuesta. Como la pregunta (petición), el módulo de identificación -401/-411- (por ejemplo, la tarjeta SIM) se proporciona con un número aleatorio de 128 bits (RAND). A continuación, el módulo de identificación -401/-411- ejecuta un algoritmo confidencial que es específico del operador respectivo y que, como entrada, recibe el número aleatorio RAND y una clave secreta Ki almacenada en el módulo de identificación -401/-411-, y esto se utiliza para generar una respuesta de 32 bits (SRES) y una clave de 64 bits Kc. Kc se utiliza para encriptar 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 una pluralidad de preguntas RAND para generar una pluralidad de claves Kc de 64 bits. Estas claves Kc se combinan para formar una clave de sesión más larga. Al comienzo de la autenticación a, el nodo IP -40/-41- transmite la identidad de abonado móvil internacional (IMSI) del usuario desde el módulo de identificación -401/-411- al módulo de registro -22-. Con la IMSI, el módulo de registro -22- recibe n tripletes GSM en una solicitud de triplete del HLR relevante -26-, o la base de datos pertinente. El módulo de registro -22- utiliza los tripletes para calcular MAC\_RAND y la clave de sesión K. A modo de ejemplo, el cálculo de los valores criptográficos de la clave de sesión generada por SIM K y de los códigos de autenticación de mensajes MAC\_RAND y MAC\_SRES se puede encontrar en el documento "HMAC: Keyed-Hashing for Message Authentication" de H. Krawczyk, M. Bellare y R. Canetti (RFC2104, febrero de 1997). A continuación, el algoritmo de autenticación GSM se ejecuta en el módulo de identificación -401/-411- del nodo IP -40/-41- y calcula una copia de MAC\_RAND. El nodo IP -40/-41- comprueba que el valor calculado de MAC\_RAND es el mismo que el valor recibido de MAC\_RAND. Si los dos valores no coinciden, el nodo IP -40/-41- finaliza el método de autenticación y no envía ningún valor de autenticación calculado por el módulo de identificación -401/-411- a la red. Puesto que el valor RAND se recibe junto con el código de autenticación de mensaje MAC\_RAND, el nodo IP -40/-41- puede asegurar que RAND es nuevo y ha sido generado por la red. Si la autenticación tiene éxito, se puede realizar una

actualización de la ubicación en el HLR -26- o en la base de datos funcionalmente equivalente, por ejemplo, y el nodo IP -10- recibe una entrada apropiada en una base de datos de clientes del módulo de registro -22-.

5 Después de la autenticación y/o autorización en el registro de localización local -26- o la base de datos funcionalmente equivalente, los datos de localización relevantes se transmiten desde el módulo de autenticación al módulo de registro -22-. El módulo de registro -22- se utiliza para almacenar los datos de localización en una base de datos sobre los nodos IP -40-/-41- en la red telefónica y/o videotelefónica basada en IP. En particular, estos datos de localización pueden incluir dirección IP, dirección MAC y otros datos relevantes para la telefonía basada en IP y/o videotelefonía. Además de la autenticación en la red telefónica y/o videotelefonía basada en IP. También es posible  
10 que los registros detallados de llamadas producidos a través del módulo de control (-21-) y/o el nodo de red IP (-40-/-41-) se transmitan al módulo de registro -22-, por ejemplo. El módulo de registro -22- puede usarse entonces para detectar al menos la identidad del nodo IP -40-/-41- y/o el período y/o proveedor del servicio solicitado y para enviarlo/enviarlos a un módulo de facturación, por ejemplo. El módulo de facturación puede utilizarse para producir ficheros de facturación en línea con el servicio solicitado sobre la base de los datos de facturación del módulo de registro -40-/-41- y sobre la base de los registros detallados de llamadas y transmitirlos con instrucciones de facturación a un módulo de compensación. El módulo de registro -22- transmite a continuación los datos de autenticación apropiados al módulo de identificación -401-/-411- del nodo IP -40-/-41- y los almacena, con lo cual se libera el nodo IP -40-/-41- para la telefonía /o videotelefonía IP.

20 Como se ha mencionado, tras una autenticación satisfactoria del nodo de red IP -40-/-41-, se puede realizar una actualización de localización en el HLR -25- y/o VRL y/o AuC y/o una base de datos funcionalmente equivalente, y se pueden transmitir los datos apropiados al módulo de registro -22-. Esto puede hacerse, pero no es en modo alguno una característica que sea necesaria para la invención. La actualización de ubicación se utiliza sólo para el control de sesión. Es decir, una estación central puede comprobar si se usa el mismo número de identificación, tal como la IMSI y/o MSISDN, una pluralidad de veces y simultáneamente, por ejemplo de manera fraudulenta, mediante un mal uso de los módulos de identificación -401-/-411- y/o números de identificación que se han robados o adquirido ilegalmente de otra manera.

30 El módulo de control -21- también puede conceder la autorización de servicio apropiada para usar la unidad de conexión -10-, por ejemplo simplemente sobre la base de la autenticación por medio de la IMSI y/o el módulo de control -21- puede iniciar la facturación apropiada para el servicio solicitado usando un módulo de facturación -24- o una plataforma de facturación adecuada. Esto permite una facturación simple para el servicio solicitado. A modo de ejemplo, la facturación también se puede asignar directamente utilizando sistemas de facturación de proveedores de servicios en redes GSM sin necesidad de alterar de ninguna manera las infraestructuras existentes. La facturación también puede efectuarse transmitiendo registros detallados de llamadas desde el nodo de red IP -40-/-41- al módulo de registro -22-, por ejemplo, detectando el módulo de registro -22- al menos la identidad del nodo de red IP -40/41- y/o el período y/o el proveedor del servicio demandado y transmitirlo/transmitirlos al módulo de facturación -24-. El módulo de facturación -24- puede producir archivos de facturas, por ejemplo, en línea con el servicio demandado, sobre la base de los datos de facturación del módulo de registro -22- y sobre la base de los registros detallados de llamadas y puede transmitirlos con instrucciones de facturación a un módulo de compensación. La autenticación por medio de la unidad de conexión puede también realizarse, a modo de ejemplo, únicamente si la solicitud de conexión y/o el establecimiento de conexión proceden de un nodo de red IP -40-/-41-. Este es el caso particularmente si la autenticación se usa únicamente para realizar la facturación, por ejemplo. Si la solicitud procede de un nodo de red -50-,..., -50-/-60- distinto de un nodo de red IP -40-/-41-, tal como de un equipo de red GSM 60,  
45 entonces es posible usar los métodos de facturación que son típicos en esta red -31-/-32-, si están disponibles. El uso de los registros detallados de llamadas tiene la ventaja, entre otras, de que la facturación de los servicios demandados puede gestionarse fácilmente por medio de un módulo de compensación, particularmente en el caso de compensación entre los diversos operadores de redes.

50 Lista de referencias

- 10 Unidad de conmutación central
- 20 Módulo de puerta de enlace de señalización
- 21 Módulo de control
- 22 Módulo de registro
- 23 Puerta de enlace IP/PSTN
- 24 Módulo de facturación/plataforma de facturación
- 25 Puerta de enlace MAP
- 26 HLR/VLR/AuC
- 30 Red IP
- 31 PSTN (red de telefonía pública conmutada (Public Switched Telephone Network))
- 32 Red GSM
- 40/41/42 Nodo de red IP
- 401/411 SIM
- 50,..., 55 Nodos de red de la PSTN (Teléfono)
- 60 Nodos de red en una red móvil

## REIVINDICACIONES

1. Método para telefonía basada en IP y/o telefonía de vídeo basada en el Protocolo de Inicio de Sesión (SIP) en redes heterogéneas (30/31/32), en el que un nodo de red solicita una conexión de datos a uno o más nodos de red a través de una interfaz para una unidad de conexión central (10) de una red IP (30), en el que al menos un nodo de red es un nodo de red IP (40/41), y los nodos de red para un elemento de red de registro SIP (22) de la unidad de conexión central (10) se registran, y en el que la conexión entre los nodos de red se establece por medio de un elemento de red proxy SIP (21) de la unidad de conexión central (10), **caracterizado porque** para la transmisión de flujo de datos y/o multimedia del al menos un nodo de red IP (40/41), tras la solicitud por el elemento de red de registro SIP (22), una IMSI almacenada en una tarjeta SIM (401/411) de los nodos de red IP (40/41) se transmite al elemento de red de registro SIP (22), y la IMSI se almacena en una base de datos de usuario del elemento de red de registro SIP (22), el canal de datos IP lógico para los canales de señales y de datos de una red GSM se complementa por medio de un módulo de puerta de enlace de señalización (20), y las funciones SS7/MAP necesarias se generan para autenticar al menos un nodo de red IP (40/41), en base a los datos GSM complementados de forma correspondiente, por medio de una base de datos de usuario y un módulo de puerta de enlace de señalización (20), el elemento de red de registro SIP (22) realiza una autenticación de los nodos de red IP (40/41) en base a la IMSI de la tarjeta SIM (401/411) del al menos un nodo de red IP (40/41) para un HLR/VLR/AuC (26) y/o una base de datos funcionalmente equivalente, y tras una autenticación satisfactoria, el nodo de red IP (40/41) recibe una entrada correspondiente en la base de datos de usuario del elemento de red de registro SIP (22), en el que la conexión de datos para un nodo de red diferente se crea por medio del elemento de red proxy SIP (21) de la unidad de conexión central (10), en el que la autorización de servicio correspondiente para el uso de la unidad de conexión central (10) se concede en base a la autenticación por medio de la IMSI, y la facturación del servicio solicitado se realiza por medio de un módulo de facturación (24).
2. Método, según la reivindicación 1, **caracterizado porque** tras una autenticación satisfactoria del nodo de red IP (40/41), se realiza una actualización de ubicación del HLR (25) y/o el VLR y/o AuC, y los datos correspondientes se transmiten al elemento de red de registro SIP (22).
3. Método, según cualquiera de las reivindicaciones 1 a 3, **caracterizado porque** la autenticación se realiza por medio de la unidad de conexión central (10) únicamente si la solicitud de la conexión tiene origen en un nodo de red IP (40/41).
4. Método, según cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** la autenticación del uno o más nodos IP (40/41) se realiza a través de un Protocolo de Autenticación Extensible.
5. Método, según cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** al menos un nodo de red IP (40/41) es un teléfono móvil compatible con IP.
6. Método, según cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** los registros detallados de llamadas generados por el módulo de control (21) y/o los nodos de red IP (40/41) se transmiten al módulo de registro (22), en el que el elemento de red de registro SIP (22) registra al menos la identidad del nodo de red IP (40/41) y/o la duración y/o el proveedor del servicio solicitado y los transmite a un módulo de facturación (24), y el módulo de facturación (24) genera archivos de facturación correspondientes al servicio solicitado, basándose en los datos de facturación del elemento de red de registro SIP (22) y los registros detallados de llamadas, y los transmite junto con las instrucciones de facturación a un módulo de compensación.
7. Método, según cualquiera de las reivindicaciones 1 a 6, **caracterizado porque** la unidad de conexión central (10) presenta una puerta de enlace IP/PTSN (23) para la conexión entre la red basada en IP (30) y la red de telefonía pública conmutada (31) y/o la red de telefonía móvil (32), en el que la puerta de enlace IP/PSTN (23) se opera de forma integral con la unidad de conexión central 10, y/o por separado de la unidad de conexión central (10) a través de la red IP (30).
8. Sistema de conmutación para telefonía basada en IP y/o telefonía de vídeo basada en el Protocolo de Inicio de Sesión (SIP) en redes heterogéneas (30/31/32), en el que el sistema de conmutación incluye una unidad de conexión central (10) para generar conexiones de datos entre dos o más nodos de red (40,....,42/50,....,55/60) en base a una solicitud por parte de un nodo de red, incluyendo los nodos de red (40,....,42/50,....,55/60) al menos un nodo de red IP (40/41), en el que la unidad de conexión central (10) incluye un elemento de red de registro SIP (22) para registrar los nodos de red y un elemento de red proxy SIP (21) para establecer la conexión entre los nodos de red, **caracterizado porque** al menos un nodo de red IP (40/41) incluye una tarjeta SIM (401/411) para almacenar una IMSI y medios para transmitir la IMSI al elemento de red de registro SIP (22) tras una solicitud, en el que el elemento de red de registro SIP (22) incluye una base de datos de usuario para almacenar la IMSI, el sistema de conmutación incluye un módulo de puerta de enlace de señalización (20) para complementar un canal

- de datos IP lógico para los canales de señales y de datos de una red GSM, en el que las funciones SS7/MAP necesarias pueden generarse con el fin de autenticar el al menos un nodo IP (20) por medio de un módulo de puerta de enlace MAP (25),
- 5 el elemento de red de registro SIP (22) incluye medios para autenticar el al menos un nodo de red IP (40/41) por medio de la base de datos de usuario y el módulo de puerta de enlace de señalización (20), en base a la IMSI de la tarjeta SIM (401/411) del al menos un nodo de red IP (40/41) para un HLR y/o VLR y/o AuC (26) y/o una base de datos funcionalmente equivalente, y
- 10 tras una autenticación satisfactoria del al menos un nodo de red IP (40/41), una entrada correspondiente puede almacenarse en la base de datos de usuario del elemento de red de registro SIP (22), y/o la conexión de datos para un nodo de red diferente puede crearse por medio del elemento de red proxy SIP (21) de la unidad de conexión central (10), en el que el sistema de conmutación incluye una unidad de control para conceder una autorización de servicio correspondiente para el uso de la unidad de conexión central (10) en base a la autenticación por medio de la IMSI, y/o la unidad de conexión central incluye un módulo de facturación (24) para facturar el servicio solicitado.
- 15 9. Sistema de conmutación, según la reivindicación 8, **caracterizado porque** tras una autenticación satisfactoria del nodo de red IP (40/41), puede realizarse una actualización de ubicación del HLR (25) y/o el VLR y/o AuC, y los datos correspondientes pueden transmitirse al elemento de red de registro SIP (22).
- 20 10. Sistema de conmutación, según cualquiera de las reivindicaciones 8 a 9, **caracterizado porque** la autenticación del uno o más nodos IP (40/41) se implementa a través del Protocolo de Autenticación Extensible.
11. Sistema de conmutación, según cualquiera de las reivindicaciones 8 a 10, **caracterizado porque** el al menos un nodo de red IP (40/41) es un teléfono móvil compatible con IP.
- 25 12. Sistema de conmutación, según cualquiera de las reivindicaciones 8 a 11, **caracterizado porque** el elemento de red proxy SIP (21) y/o el nodo de red IP (40/41) incluyen medios para registrar y/o generar registros detallados de llamadas, estando los registros detallados de llamadas asociados al nodo de red IP correspondiente (40/41) mediante el elemento de red de registro SIP (22), en el que al menos la identidad del nodo de red IP (40/41) y/o la duración y/o el proveedor del servicio solicitado pueden registrarse y/o transmitirse a un módulo de facturación (24)
- 30 por medio del elemento de red de registro SIP (22) basándose en los registros detallados de llamadas, y los archivos de facturación pueden generarse por medio del módulo de facturación (24) correspondiente al servicio solicitado, basándose en los datos de facturación del elemento de red de registro SIP (22) y los registros detallados de llamadas, y estos, junto con las instrucciones de facturación, pueden transmitirse a un módulo de compensación.

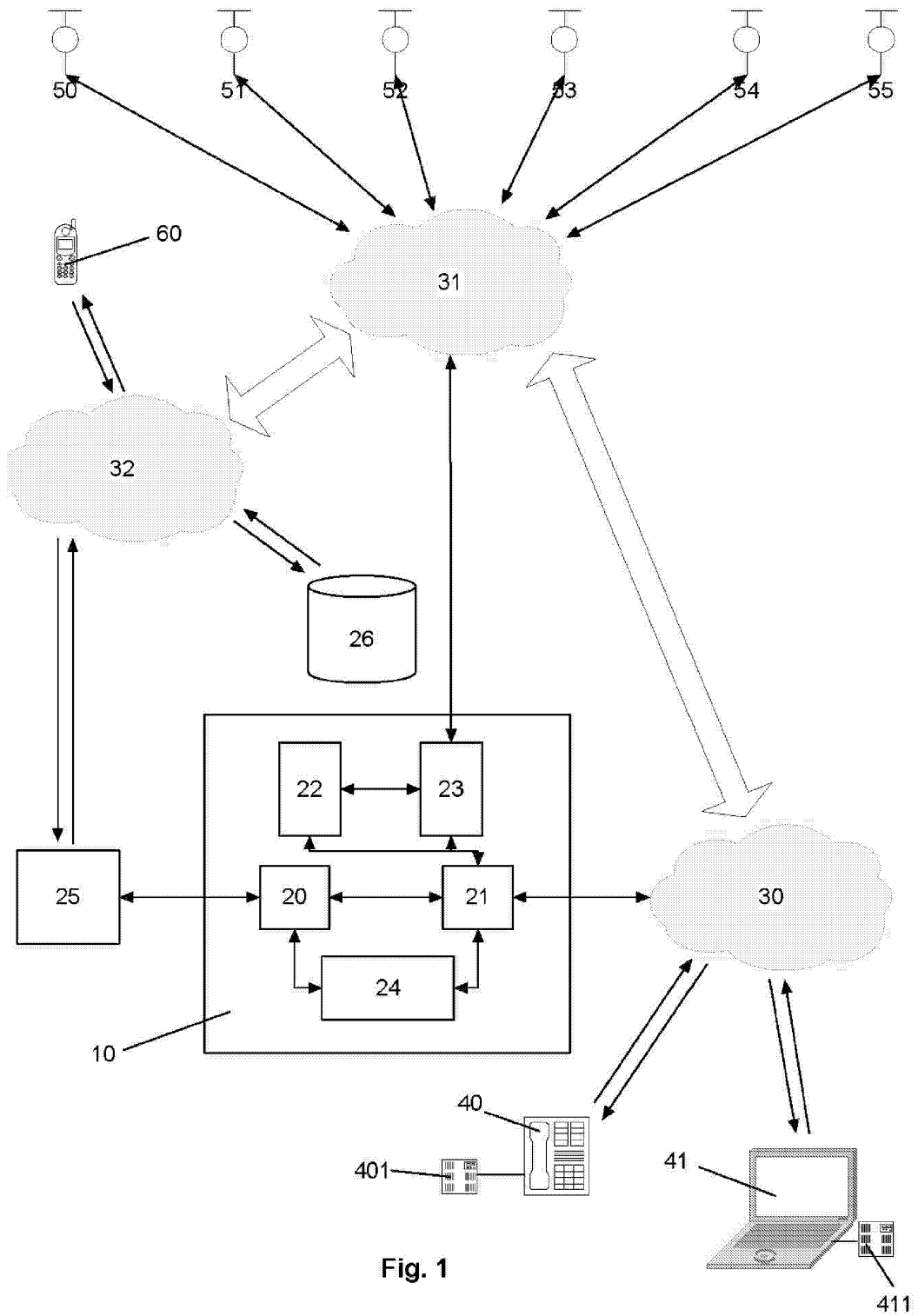


Fig. 1

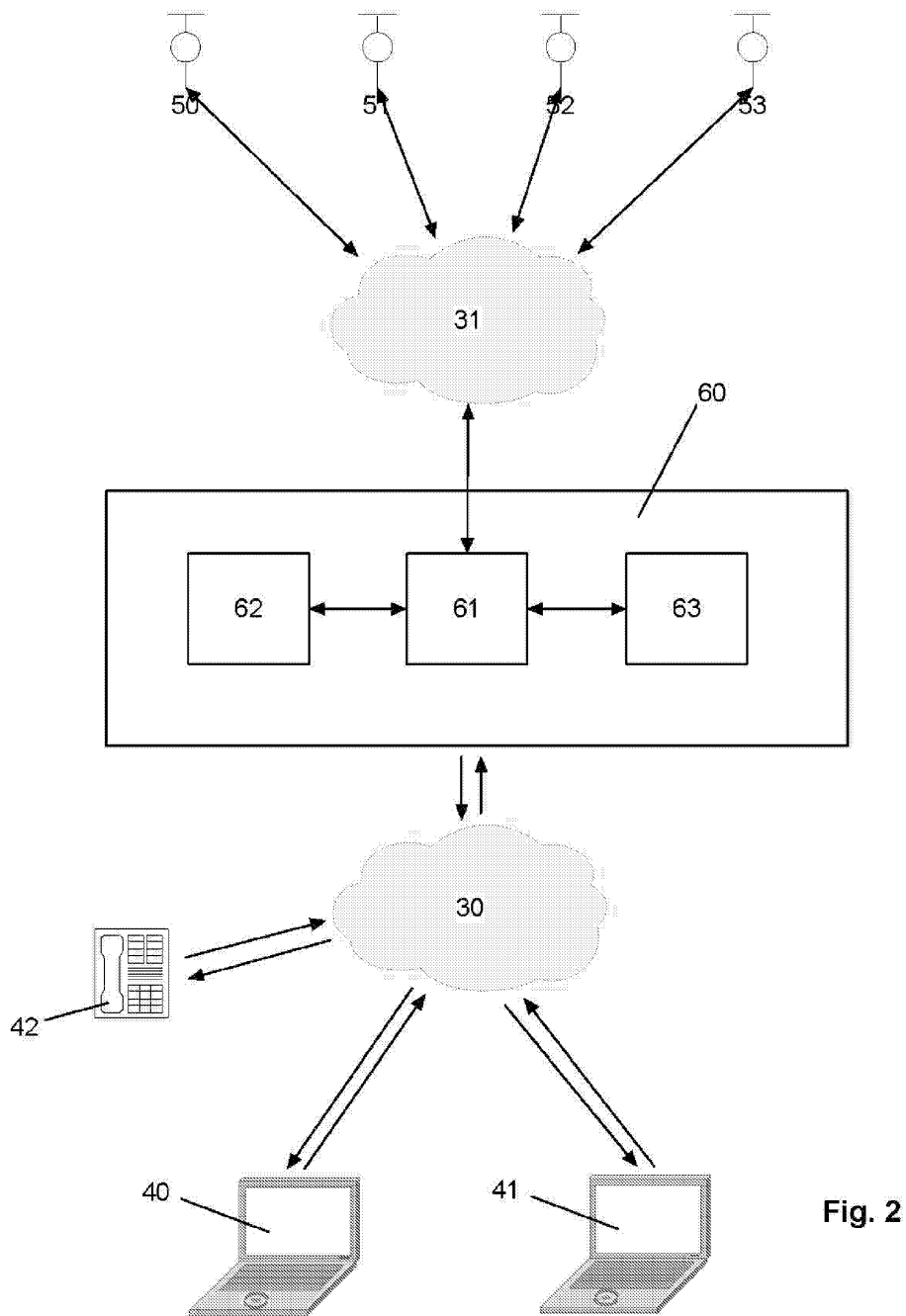


Fig. 2