(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 935**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04L 12/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08760601 .8**
(96) Fecha de presentación: **05.06.2008**
(97) Número de publicación de la solicitud: **2283607**
(97) Fecha de publicación de la solicitud: **16.02.2011**

(54) Título: **Cobro por servicios en una red de comunicación**

(45) Fecha de publicación de la mención BOPI:
19.11.2012

(45) Fecha de la publicación del folleto de la patente:
19.11.2012

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

(72) Inventor/es:
SVEDBERG, JOHAN

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Cobro por servicios en una red de comunicación

CAMPO TÉCNICO

La invención se refiere al campo del cobro por servicios en una red de comunicación.

ANTECEDENTES

El subsistema multimedia IP (IMS, IP Multimedia Subsystem) es la tecnología definida por el Proyecto de Asociación de Tercera Generación (3GPP, Third Generation Partnership Project) para proporcionar servicios multimedia IP sobre redes de comunicación móviles. Los servicios multimedia IP proporcionan una combinación dinámica de voz, video, mensajería, datos, etc., dentro de la misma sesión.

El IMS hace uso del protocolo de inicio de sesión (SIP, Session Initiation Protocol) para establecer y controlar llamadas o sesiones entre terminales de usuario. El protocolo de descripción de sesión (SDP, Session Description Protocol), transportado mediante señales SIP, se utiliza para describir y negociar los componentes de los medios de la sesión. Mientras que el SIP fue creado como un protocolo usuario a usuario, el IMS permite a los operadores y proveedores de servicio controlar el acceso de los usuarios a los servicios y cobrar en consecuencia a los usuarios.

La figura 1 muestra esquemáticamente cómo el IMS encaja en la arquitectura de red móvil en el caso de una red de acceso del Servicio General de Radiocomunicaciones por Paquetes (GPRS, General Packet Radio Service). Tal como se muestra en la figura 1, el control de las comunicaciones se produce en las tres capas (o planos). La capa inferior es la capa de conectividad 1, denominada asimismo el plano portador, y a través del cual son dirigidas las señales hacia/desde el equipo de usuario, UE (user equipment), que accede a la red. Las entidades comprendidas en la capa de conectividad 1 que conectan un abonado IMS a los servicios IMS, forman una red que se denomina la red de acceso de conectividad-IP, IP-CAN (IP-Connectivity Access Network). La red GPRS incluye varios nodos de soporte GPRS (GSNs, GPRS Support Nodes). Un nodo 2 de soporte de pasarela GPRS (GGSN, gateway GPRS support node) actúa como una interfaz entre la red básica GPRS y otras redes (red radioeléctrica y la red IMS). La capa intermedia es la capa de control 4, y en la parte superior está la capa de aplicación 6.

El IMS 3 incluye una red central 3a, que funciona sobre la capa intermedia de control 4 y la capa de conectividad 1, y una red de servicio 3b. La red central IMS 3a incluye nodos que envían/reciben señales hacia/desde la red GPRS a través de la GGSN 2a en la capa de conectividad 1, y nodos de red que incluyen funciones 5 de control de llamada/sesión (CSCFs, Call/Session Control Functions), que funcionan como servidores intermedios SIP dentro del IMS en la capa intermedia de control 4. La arquitectura 3GPP define tres tipos de CSCF: la CSCF de servidor intermedio (P-CSCF, Proxy CSCF), que es el primer punto de contacto dentro del IMS para un terminal SIP; la CSCF de servicio (S-CSCF, Serving CSCF), que proporciona al usuario servicios a los que éste está abonado; y la CSCF de interrogación (I-CSCF, Interrogating CSCF), cuya función es identificar la S-CSCF correcta y enviar a dicha S-CSCF una solicitud recibida desde un terminal SIP a través de una P-CSCF. La capa superior de aplicación 6 incluye la red de servicio IMS 3b. Se disponen servidores de aplicación (AS, Application Servers) 7 para implementar funcionalidad de servicio IMS.

IMS está previsto para distribuir servicios tales como telefonía multimedia, IPTV, mensajería, presencia, pulsar para hablar, etc. IMS se utiliza para gestionar autenticación y autorización de usuarios y otras funciones, direccionamiento y establecimiento de sesión, cobro al usuario final y contabilidad entre operadores, lógica de servicio, calidad de servicio adecuada, y colaboración entre operadores. Habitualmente, un operador IMS es un operador móvil, fijo o de acceso a internet.

Existe ya un gran número de servicios de internet basados en un modelo HTTP basado en web. Cuando se requiere autenticación y autorización de usuarios, esto se lleva a cabo en un esquema por servicio. Los sitios web que cobran por servicios tienen habitualmente una opción de registro que requiere su propio conjunto de IDs y contraseñas de usuario. Existen soluciones de infraestructura de clave pública (PKI, Public key infrastructure) que prevén un mecanismo para proporcionar autenticación global. Un ejemplo de un servicio de este tipo es openID (ver http://openid.net/). Para cobrar al usuario por un servicio basado en web, el proveedor del servicio puede realizar el cobro en la tarjeta de crédito o de débito del usuario, o utilizar un servicio de pago por internet tal como Paypal. Alternativamente, el proveedor puede cobrar al cliente.

Las redes IMS están dotadas de medios para llevar a cabo autenticación de usuario, facturación y contabilidad. IMS está evolucionando hacia la arquitectura de autenticación genérica (GAA, Generic Authentication Architecture), ver hftp://www.3gpp.org/ftp/Specs/html-info/33220.htm, con propósitos de autenticación. Esto puede utilizarse solamente para servicios proporcionados por el operador IMS u operadores IMS homólogos, y no para servicios no IMS, de manera que un usuario IMS que desee obtener un servicio de internet necesitaría autenticarse utilizando el modelo HTTP basado en web descrito anteriormente.

El modelo basado en web para autenticación y cobro requiere que el usuario introduzca una relación con cada proveedor con el que el usuario desee tratar. Esto presenta un obstáculo para cada potencial transacción. Cada vez

que el usuario desea obtener un servicio, debe evaluar si confía en el proveedor del servicio, para datos financieros tales como detalles de la tarjeta de crédito. Además, existe la incomodidad de los procedimientos de manipulación constante de una ID de usuario, una contraseña y detalles de pago para cada transacción. La incomodidad puede reducirse utilizando PKI, OpenID y servicios de pago tales como Paypal. Sin embargo, en los casos en los que el operador IMS tiene ya una relación comercial con el cliente en forma de un servicio móvil, fijo o de acceso a internet, existe un potencial para reducir la incomodidad para los clientes de IMS en la realización de transacciones por los servicios.

El documento US 2006/089999 describe un método de cobro por servicios, pero solamente puede funcionar en caso de que la red en la que está registrado el usuario tenga una relación de confianza con la red en la que está situado el servidor que proporciona los servicios. Los documentos WO 03/105031 y US 2004/147245 tampoco permitirían el cobro por servicios, en caso de que la red en la que está registrado el usuario no tenga una relación de confianza con la red en la que está situado el servidor que proporciona los servicios.

COMPENDIO

Los usuarios IMS llevan a cabo transacciones con proveedores remotos sin que se requiera que el usuario o el proveedor remoto estimen la fiabilidad de la otra parte, o pasen por prolongados procedimientos de autenticación. Un operador IMS es un proveedor de servicios de pago que permite que se cobren servicios ordinarios basados en web, del mismo modo que los servicios IMS, tal como los números de acceso de tarifa superior o los servicios SMS en redes fijas y móviles.

De acuerdo con un primer aspecto de la invención, se da a conocer un método de cobro por servicios en una red de comunicación basada en SIP. Un servidor que proporciona un servicio recibe de un usuario un primer mensaje de solicitud, incluyendo el mensaje de solicitud un identificador del usuario utilizado para el registro con la red de comunicación. En respuesta, el servidor envía al usuario una dirección restringida a través de la cual pueden obtenerse servicios. El usuario envía un segundo mensaje de solicitud a una red intermedia, incluyendo el segundo mensaje de solicitud la dirección restringida. Debe observarse que la red intermedia tiene una relación de confianza con el servidor, y es una red IMS que tiene una relación de confianza con otra red IMS en la que está registrado el usuario. El identificador del usuario es autenticado en la red intermedia, que a continuación envía al servidor una tercera solicitud, comprendiendo ésta una identidad del usuario y la dirección restringida. El servidor envía un mensaje de respuesta, que incluye credenciales que el usuario puede utilizar para obtener el servicio solicitado, a partir de la dirección restringida. La red intermedia cobra al usuario por el servicio solicitado, y envía las credenciales al usuario, permitiendo de ese modo que el usuario acceda al servicio. Esto permite que la red intermedia cobre al usuario, sin que éste tenga que establecer una relación con el servidor.

En una realización opcional, la red de comunicación es una red de comunicación basada en SIP. Cuando la red intermedia es una red IMS que tiene una relación de confianza con otra red IMS en la que está registrado el usuario, la invención funciona con el servidor incluso cuando la red local del usuario no tiene una relación de confianza con el servidor. La red IMS y la otra red IMS en la que está registrado el usuario comunican opcionalmente con un operador intermedio.

Como opción, el método comprende, en respuesta a la primera solicitud, enviar desde el servidor al usuario información de cobro además de la dirección restringida, y utilizar la información de cobro para cobrar al usuario.

Además, para autenticar al usuario, el método incluye opcionalmente llevar a cabo una verificación del crédito relativa al usuario, para asegurar que el usuario tiene fondos suficientes para pagar los servicios del servidor.

Opcionalmente, las credenciales enviadas desde el servidor tienen una duración predeterminada.

En una realización opcional, el segundo mensaje de solicitud es un mensaje SIP, y el tercer mensaje de solicitud es un mensaje de protocolo de transporte de hipertexto (HTTP, Hypertext Transport Protocol). Sin embargo, como una opción alternativa, el segundo y el tercer mensaje de solicitud son ambos mensajes HTTP.

De acuerdo con un segundo aspecto de la invención, se da a conocer un dispositivo de usuario para utilizar en una red de comunicación. Se dispone un primer transmisor para enviar a un servidor de prestación de servicios un primer mensaje de solicitud que incluye un identificador de usuario utilizado para registrarse con la red de comunicación. Asimismo, se dispone un primer receptor para recibir desde el servidor un primer mensaje de respuesta, que incluye una dirección restringida a través de la cual pueden obtenerse los servicios solicitados. Se utiliza un segundo transmisor para enviar a un nodo intermedio de la red una segunda solicitud que incluye la dirección restringida. El nodo intermedio de la red está situado en una red IMS que tiene una relación de confianza con otra red IMS en la que el usuario está registrado. Se dispone un segundo receptor para recibir desde el nodo intermedio de la red una segunda respuesta que incluye credenciales que autentican el identificador del usuario. Se dispone un tercer transmisor para enviar una solicitud de servicios a la dirección restringida, la solicitud de servicios incluyendo las credenciales que demuestran al servidor que el usuario ha sido cobrado por los servicios y que puede acceder a la zona restringida del servidor utilizando la dirección restringida.

De acuerdo con un tercer aspecto la invención, se da a conocer un servidor para utilizar en una red de comunicación. Se dispone un primer servidor para recibir de un usuario una primera solicitud de servicios, incluyendo la solicitud un identificador del usuario utilizado para registrarse con la red de comunicación. Se dispone un primer transmisor para enviar al usuario un mensaje que incluye una dirección restringida a través de la cual pueden obtenerse los servicios. Se dispone un segundo receptor para recibir, desde una red intermedia con la que el servidor tiene una relación de confianza, otra solicitud que incluye una identidad del usuario, la dirección restringida y una indicación de que el identificador del usuario está autenticado por la red intermedia. El nodo intermedio de la red está situado en una red IMS que tiene una relación de confianza con otra red IMS en la que el usuario está registrado. Se dispone un segundo transmisor para enviar a la red intermedia un mensaje de respuesta, incluyendo el mensaje de respuesta información de cobro y credenciales utilizables para obtener el servicio solicitado desde la dirección restringida. Se dispone un tercer receptor para recibir del usuario un mensaje de solicitud de servicios, incluyendo el mensaje de solicitud de servicios la dirección restringida y las credenciales. Un procesador determina que la dirección restringida, la identidad del usuario y las credenciales sean válidas. En caso de que se determinen como válidas, el servicio es proporcionado.

De acuerdo con un tercer aspecto de la invención, se da a conocer un nodo para utilizar en una red de comunicación intermedia que tiene una relación de confianza con otra red IMS en la que está registrado el usuario. Se dispone un primer receptor para recibir de un usuario un mensaje de solicitud, incluyendo el mensaje de solicitud una dirección restringida para una zona restringida de un servidor que tiene una relación de confianza con la red de comunicación intermedia. Se dispone un primer procesador para autenticar un identificador de usuario asociado con el usuario, y se dispone un primer transmisor para enviar al servidor una tercera solicitud, incluyendo la tercera solicitud una identidad del usuario y la dirección restringida, y una indicación de que el identificador del usuario está autenticado. Se dispone un segundo receptor para recibir del servidor un mensaje de respuesta, incluyendo el mensaje de respuesta credenciales utilizables para obtener de la dirección restringida el servicio solicitado. Se dispone una función de cobro para cobrar al usuario, y se dispone un segundo transmisor para enviar al usuario las credenciales utilizables para acceder a los servicios a través de la dirección restringida.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 muestra esquemáticamente, en un diagrama de bloques, una red IMS en asociación con una arquitectura de red móvil de una red de acceso del servicio general de radiocomunicaciones por paquetes (GPRS);

la figura 2 muestra esquemáticamente, en un diagrama de bloques, una arquitectura de red acorde con una realización de la invención;

la figura 3 es un diagrama de señalización que muestra la señalización entre nodos de red, de acuerdo con la realización de la invención;

la figura 4 es un diagrama de flujo que muestra las etapas de una realización de la invención;

la figura 5 muestra esquemáticamente, en un diagrama de bloques, un dispositivo de usuario acorde con una realización de la invención;

la figura 6 muestra esquemáticamente, en un diagrama de bloques, un servidor acorde con una realización de la invención; y

la figura 7 muestra esquemáticamente, en un diagrama de bloques, un nodo intermedio acorde con una realización de la invención.

DESCRIPCIÓN DETALLADA

Haciendo referencia a la figura 2, se muestra un dispositivo 8 de usuario final. El dispositivo puede ser cualquier dispositivo adecuado, tal como un ordenador personal o un dispositivo móvil. El dispositivo 8 tiene un navegador web 9, y tiene instalado un cliente 10 de agente de usuario SIP (SIP UAC, SIP User Agent Client) con IMS habilitado. El cliente 10 está registrado como un usuario con el operador IMS C 11. Esto significa que el cliente 10 y el operador 11 se han puesto de acuerdo sobre la ID de usuario del cliente, la contraseña o equivalentes, para que el operador 11 autentique al usuario y viceversa.

En el servidor 12 funciona un proveedor de servicio que proporciona algún tipo de servicio. El proveedor de servicio tiene un acuerdo con el operador IMS S 13. En este ejemplo, el operador IMS C 11 y el operador IMS S 13 se muestran como dos operadores IMS independientes, pero la invención aplica igualmente si los operadores IMS C y S son el mismo operador IMS. En este ejemplo, el operador IMS C 11 y el operador IMS S 13 son operadores diferentes, y existe un acuerdo entre ambos que define de qué manera confían entre ellos y cómo realizar contabilidad y liquidaciones de pago entre ellos, de acuerdo con procedimientos IMS normales. En un escenario probable, los operadores IMS S 13 y C 11 no tienen una relación directa, sino que colaboran a través de un operador intermedio IMS 14.

El proveedor de servicio 12 y el operador IMS S 13 tienen un acuerdo sobre cómo confían entre ellos. Esto puede ser mediante métodos PKI, cortafuegos de la capa 3 o combinaciones de los mismos. Asimismo, tienen un acuerdo comercial que define cargos por servicios concretos.

Antes de que el dispositivo 8 de usuario pueda comunicar con el servicio en el servidor 12, el SIP UAC 10 se registra con el IMS C 11. Esto es necesario para que el SIP UAC 10 envíe mensajes Invite SIP al IMS C 11.

A continuación haciendo referencia a la figura 3, se ilustra un diagrama de señalización que muestra la señalización necesaria para obtener un servicio para el que se ha realizado un cobro, de acuerdo con una realización de la invención. La numeración siguiente corresponde a la numeración de la figura 3.

S1. El usuario utiliza su navegador web 9 para visitar la zona abierta del servidor 12 del proveedor del servicio. El usuario selecciona una opción para comprar servicios y por lo tanto acceder a una zona restringida del servidor 12.

S2. Un cuerpo de mensaje codificado MIME es enviado desde el servidor 12 al navegador web 9 del cliente. Este cuerpo de mensaje contiene una dirección para la zona restringida, una dirección para un punto de recuperación de credenciales en el que pueden ser obtenidas credenciales para acceder a la zona restringida, y una dirección para la red S 13 IMS.

S3. La codificación MIME es registrada mediante el SIP UAC 10 del usuario en el navegador web 9 del usuario, de manera que cuando se recibe un cuerpo de mensaje de este tipo en el dispositivo 8 del usuario el cuerpo de mensaje es trasladado al SIP UAC 10.

S4. El SIP UAC 10 envía un mensaje INVITE para el IMS C 13 (la red IMS con la que está registrado el usuario), dirigido al IMS S 11. La invitación contiene el cuerpo de mensaje MIME. El mensaje INVITE es autenticado mediante el IMS C 11 como enviado desde el cliente 10 utilizando procedimientos IMS normales. En esta etapa, puede llevarse el control de crédito con la cuenta de prepago del cliente.

S5. El IMS C 11 envía el mensaje INVITE al IMS S 13. A continuación, el ID del cliente es enviado en una cabecera de identidad-declarada-P del mensaje INVITE. Utilizando disposiciones de seguridad IMS normales, el IMS S 13 confía en que el mensaje procede del IMS C 11.

S6. El IMS S 13 envía una solicitud HTTP o HTTPS al punto de la recuperación de credenciales del servidor 12. La solicitud incluye información relacionada con el ID 10 del cliente y la dirección de la zona restringida solicitada. Contiene asimismo una indicación sobre si la etapa S4 de control del crédito ha sido o no satisfactoria. El servidor 12 determina si el usuario tiene ya credenciales de una transacción anterior (revisitada o fallida). Si éste fuera el caso, entonces las credenciales pueden ser proporcionadas sin cargo, y la transacción puede permitirse incluso si ha fallado el control de crédito en S4. De lo contrario, el servidor 12 lleva a cabo una autorización en base al ID del cliente.

S7. El servidor 12 devuelve al IMS S13 un cuerpo de mensaje MIME que contiene un URL de la zona protegida. Este URL incluye credenciales generadas por el servidor 12 y será utilizado en la etapa S12 para autenticar la solicitud para la zona protegida. El cuerpo de mensaje contiene asimismo información que será utilizada mediante el IMS S 13 para cobrar al usuario.

S8a. El IMS S13 envía en un mensaje SIP 200 OK al IMS C 11 el URL recibido en el cuerpo de mensaje. El IMS S 13 incluye asimismo información de cobro en el mensaje. La información de cobro puede ser igual que la recibida desde servidor 12, o puede ser recalculada o remapeada en función de los acuerdos entre los IMS C 11 y S 13.

S8b. El IMS C 11 envía en un mensaje SIP 200 OK al SIP UAC 10 el URL que incluye las credenciales recibidas en el cuerpo de mensaje. El IMS C 11 puede incluir información de cobro en el mensaje. Esta información de cobro puede ser igual que la recibida desde el IMS S 13, o puede ser recalculada o remapeada en función de los acuerdos entre el IMS C 11 y el cliente 10.

S9a. El SIP UAC 10 envía un ACK al IMS C 11 para acusar que ha sido recibido el URL (que incluye las credenciales).

S9b. El IMS C 11 envía un ACK al IMS S 13 para acusar que ha sido recibido el URL (que incluye las credenciales).

S10. El SIP UAC 10 activa el navegador web 9 del cliente utilizando el URL recibido.

S11a. El navegador web 9 es activado.

S11b. Para concluir la sesión SIP, el SIP UAC 10 envía un mensaje BYE al IMS C 11.

S11c. El IMS C 11 finaliza la sesión SIP y genera información de cobro utilizando su sistema de cobro, y envía un mensaje 200 OK al SIP UAC 10. Asimismo, el IMS C 11 puede utilizar información de contacto obtenida a partir del perfil de usuario del cliente, para notificar mediante la dirección de correo electrónico del cliente o por SMS, que se ha producido la transacción. Este mensaje puede incluir el URL (incluyendo las credenciales).

S11d. El IMS C 11 envía un mensaje BYE al IMS S13.

S11e. El IMS S 13 finaliza la sesión SIP y genera información de cobro utilizando su sistema de cobro, y envía un 200 OK al IMS C 11.

S12. A continuación, el usuario puede acceder a la zona restringida del servidor 12 utilizando directamente el navegador web 9.

S13. Cuando el navegador web del usuario ha proporcionado las credenciales correctas, el servidor 12 proporciona el servicio solicitado.

Debe observarse que el IMS C 11 y el IMS S 13 pueden colaborar a través de un intermediario 14. En este caso, la señalización entre el IMS C 11 y el IMS S 13 pasará a través del intermediario 14, o bien las liquidaciones de cobro pueden ser realizadas por el intermediario.

Una vez que ha sido entregado al navegador 9 el URL que incluye las credenciales, la comunicación puede realizarse directamente entre el navegador 9 y el servidor 12, sin ninguna otra implicación de los operadores IMS.

El proveedor del servicio decide la duración para la que serán válidas las credenciales. La política que controla esto puede estar ubicada en el servidor 12. Son ejemplos de políticas los siguientes:

- Un servicio de descarga de música puede proporcionar un URL que autoriza al cliente a descargar un archivo específico cualquier número de veces. Alternativamente, puede proporcionarse un URL que permita al cliente de descargar el archivo solamente una vez.

- Para comercio electrónico con entrega física, el servicio puede proporcionar un URL que autoriza al cliente a revisar una cesta de compras. El URL puede incluir la cesta junto con las credenciales.

- En un servidor de comunidad social o de sitio comercial "mis páginas", el URL proporcionado puede o no ser sin cargo, y sirve como un vale de "inicio de sesión único". Esto significa que el operador IMS proporciona un servicio de autenticación y el servidor puede, a través del URL, asegurarse de que el usuario es quien dice ser.

El usuario puede ser cobrado de forma segura después de la etapa S8, una vez que el IMS C 11 ha recibido el URL. Esto se debe a que después de esta etapa, el usuario puede obtener de nuevo las credenciales, incluso si no fueron entregadas satisfactoriamente al navegador web 9. Por lo tanto, el cobro no depende del comportamiento fiable del soporte lógico en el dispositivo 8 del cliente.

A continuación haciendo referencia a la figura 4, se muestra un diagrama de flujo que ilustra las etapas, de acuerdo con una realización de la invención. La numeración siguiente corresponde a las etapas mostradas en las figuras 3 y 4:

S1. El navegador web 9 del usuario envía una solicitud de los servicios del servidor 12, incluyendo la solicitud un identificador para el usuario.

S2. El servidor 12 responde al navegador web, incluyendo la respuesta la dirección para una zona restringida del servidor desde la cual puede obtenerse el servicio solicitado.

S3. El SIP UAC 10 del usuario envía Invite SIP al IMS C 11, Invite SIP que incluyen la dirección para la zona restringida y el identificador del usuario.

S14. El IMS C 11 autentica el identificador de usuario asociado con el usuario. En este momento, el IMS C 11 puede asimismo llevar a cabo una verificación de crédito del usuario.

S6. El IMS S, que tiene una relación de confianza con el IMS C, envía una solicitud al punto de recuperación de crédito del servidor 12, incluyendo la solicitud un ID para el usuario y la dirección para la zona restringida. La solicitud incluye asimismo una indicación de que el identificador del usuario ha sido autenticado. El IMS S y el servidor tienen una relación de confianza.

S7. El servidor 12 responde con un mensaje que incluye información de cobro por el servicio y credenciales para obtener el servicio solicitado.

S15. El IMS C cobra al usuario.

S8b. El IMS C envía al usuario el URL que incluye las credenciales.

S12. En este momento, el usuario tiene las credenciales para acceder al servicio, y la dirección para la zona restringida. Con esta información, el usuario contacta con el servidor 12 para obtener el servicio.

Debe observarse que la descripción anterior asume dos redes IMS, si bien es posible que la red local del usuario, IMS C 11, tenga una relación de confianza con el servidor 12, en cuyo caso puede contactar directamente con servidor 12.

A continuación haciendo referencia a la figura 5, se muestra un dispositivo 8 de usuario. El dispositivo 8 de usuario está dotado de un primer transmisor 15 para enviar un mensaje de solicitud al servidor 12, y de un primer receptor 16 para recibir una respuesta del servidor, incluyendo la respuesta la dirección para la zona restringida a través de la cual pueden obtenerse los servicios solicitados. Se dispone un segundo transmisor 17 para enviar al IMS C 11 un mensaje Invite SIP que incluye la dirección de la zona restringida. Se dispone un segundo receptor 18 para recibir del IMS C 12 un mensaje 200 OK SIP, incluyendo el 200 OK SIP un URL y credenciales que autentican al usuario. Se dispone un tercer transmisor 19 para enviar una solicitud de servicios a la dirección restringida el servidor 12, la solicitud de servicios incluyendo las credenciales. Se dispone un procesador 20 para controlar la señalización. Se apreciará que los receptores pueden realizarse en un solo receptor, y que los transmisores pueden realizarse en un solo transmisor.

Haciendo referencia a la figura 6, se muestra un servidor 12 acorde con una realización de la invención. El servidor 12 comprende un primer receptor 21 para recibir una solicitud de servicios desde el dispositivo 8 de usuario, y un primer transmisor 22 para enviar al usuario 8 una de respuesta que incluye la dirección para la zona restringida desde la que pueden obtenerse los servicios. Se dispone un segundo receptor 23 para recibir desde el IMS S 13 otra solicitud que incluye una identidad del usuario, la dirección restringida y una indicación de que el identificador del usuario está autenticado por la red intermedia. Se dispone un segundo transmisor 24 para enviar al IMS S 13 un mensaje de respuesta, incluyendo el mensaje respuesta información de cobro y credenciales utilizables para obtener de la dirección restringida el servicio solicitado. Se dispone un tercer receptor 25 para recibir del dispositivo 8 de usuario un mensaje de solicitud de servicios. Este mensaje incluye la dirección restringida y las credenciales. Se dispone un procesador 26 para determinar que la dirección restringida, la identidad del usuario y las credenciales son válidas y, en caso de que se determine que lo son, proporcionar el servicio solicitado. Se apreciará que los receptores pueden realizarse en un solo receptor, y que los transmisores pueden realizarse en un solo transmisor.

La figura 7 muestra un nodo 26 para utilizar en una red de comunicación. El nodo 26 está dotado de un primer receptor 27 para recibir del dispositivo 28 de usuario un mensaje de solicitud que incluye una dirección restringida para una zona restringida del servidor 12. Se dispone un primer procesador 28 para autenticar el identificador del usuario, y se dispone un primer transmisor 29 para enviar al servidor 12 una solicitud que incluye una identidad del usuario y la dirección restringida, y una indicación de que el identificador del usuario está autenticado. Se dispone un segundo receptor 30 para recibir del servidor 12 un mensaje de respuesta. El mensaje de respuesta incluye información de cobro y credenciales utilizables para obtener de la dirección restringida el servicio solicitado. Se dispone una función de cobro 31 para cobrar al usuario de acuerdo con la información de cobro recibida. Se dispone un segundo transmisor 32 para enviar al dispositivo de usuario 8 las credenciales utilizables para acceder a los servicios a través de la dirección restringida. Las diversas características de este nodo pueden estar ubicadas en un solo nodo, en una serie de nodos, e incluso en una serie de nodos situados en redes diferentes, pero la funcionalidad básica se mantiene igual.

La invención permite a los usuarios mantener una relación comercial solamente con su propio operador IMS, en lugar de mantenerla con cada proveedor de servicio. Por lo tanto, no es necesario exponer detalles de las tarjetas de crédito a nuevos proveedores de servicios, ni autorizar a nuevos proveedores de servicios a cobrar con la tarjeta de crédito del usuario o en un servicio de pago. Solamente se requiere un punto de contacto para cuestiones de reclamaciones y responsabilidad. Otra ventaja de la invención es que el usuario requiere solamente una única identidad, un solo método de autenticación y claves/contraseña únicas. El usuario no necesita utilizar IDs y contraseñas independientes para muchos servidores. Además, si el usuario mantiene una cuenta de prepago con su operador IMS, se minimizan entonces cualesquiera potenciales pérdidas debidas a fraude.

Los expertos en la materia apreciarán que pueden realizarse diversas modificaciones a las realizaciones descritas anteriormente, sin apartarse del alcance de la presente invención. Por ejemplo, la descripción anterior se refiere a una red IMS, si bien resultará evidente que la invención podría modificarse para funcionar en cualquier red de comunicación que utilice señalización basada en SIP o arquitectura genérica de autenticación o de procedimientos de puesta en marcha.

REIVINDICACIONES

1. Un método de cobro por servicios en una red de comunicación, comprendiendo el método:

en un servidor que proporciona un servicio, recibir (S1) de un usuario una primera solicitud de servicios, incluyendo la solicitud un identificador del usuario utilizado para registrarse con la red de comunicación;

en respuesta a la primera solicitud, enviar (S2) al usuario una dirección restringida a través de la cual pueden ser obtenidos los servicios;

estando el método **caracterizado por**, en el dispositivo del usuario, enviar (S3) a una red intermedia un segundo mensaje de solicitud, siendo la red intermedia una red de subsistema multimedia IP que tiene una relación de confianza con otra red de subsistema multimedia IP en la cual está registrado el usuario, incluyendo el segundo mensaje de solicitud la dirección restringida, teniendo la red intermedia una relación de confianza con el servidor;

en la red intermedia, autenticar (S14) el identificador del usuario;

enviar (S6) una tercera solicitud desde la red intermedia al servidor, incluyendo la tercera solicitud una identidad del usuario y la dirección restringida;

recibir (S7) en la red intermedia un mensaje de respuesta procedente del servidor, incluyendo el mensaje de respuesta credenciales utilizables para obtener desde la dirección restringida el servicio solicitado;

en la red intermedia, cobrar (S15) al usuario por el servicio solicitado; y

enviar (S8b) al usuario las credenciales utilizables para acceder a los servicios a través de la dirección restringida.

2. El método acorde con la reivindicación 1, en el que la red de comunicación es una red de comunicación basada en protocolo de inicio de sesión.

3. El método acorde con la reivindicación 1, en el que la red de subsistema multimedia IP y la otra red de subsistema multimedia IP en la que está registrado el usuario comunican a través de un operador intermediario.

4. El método acorde con cualquiera de las reivindicaciones 1 a 3, que comprende además, en respuesta a la primera solicitud, enviar desde el servidor al usuario información de cobro además de la dirección restringida, y utilizar la información de cobro para cobrar al usuario.

5. El método acorde con cualquiera de las reivindicaciones 1 a 4, que comprende, además de autenticar al usuario, llevar a cabo una comprobación de crédito relativa al usuario.

6. El método acorde con cualquiera de las reivindicaciones 1 a 5, en el que las credenciales enviadas desde el servidor tienen una duración predeterminada.

7. El método acorde con cualquiera de las reivindicaciones 1 a 6, en el que el segundo mensaje de solicitud es un mensaje de protocolo de inicio de sesión, y el tercer mensaje de solicitud es un mensaje de protocolo de transporte de hipertexto.

8. El método acorde con cualquiera de las reivindicaciones 1 a 7, en el que el segundo y el tercer mensaje de solicitud son ambos mensajes de protocolo de transporte de hipertexto.

9. Un dispositivo (8) de usuario para utilizar en una red de comunicación, comprendiendo el dispositivo de usuario:

un primer transmisor (15) para enviar a un servidor (12) un primer mensaje de solicitud de prestación de servicios, incluyendo el primer mensaje de solicitud un identificador de usuario utilizado para registrarse con la red de comunicación;

un primer receptor (16) para recibir del servidor un primer mensaje de respuesta, incluyendo el mensaje de respuesta una primera dirección restringida a través de la cual pueden ser obtenidos los servicios solicitados;

el dispositivo de usuario, estando **caracterizado por** un segundo transmisor (17) para enviar una segunda solicitud a un nodo intermedio de la red, incluyendo la segunda solicitud la dirección restringida, estando situado el nodo intermedio de la red en una red de subsistema multimedia IP que tiene una relación de confianza con otra red de subsistema multimedia IP en la cual está registrado el usuario;

un segundo receptor (18) para recibir una segunda respuesta desde el nodo intermedio de la red, incluyendo la segunda respuesta credenciales que autentican el identificador de usuario;

un tercer transmisor (19) para enviar una solicitud de servicios a la dirección restringida, la solicitud de servicios incluyendo las credenciales.

10. Un servidor (12) para su utilización en una red de comunicación, comprendiendo el servidor:

un primer receptor (21) para recibir de un usuario una primera solicitud de servicios proporcionados por el servidor, incluyendo la solicitud un identificador del usuario utilizado para registrarse con la red de comunicación;

un primer transmisor (22) para enviar al usuario un mensaje que incluye una dirección restringida a través de la cual pueden obtenerse los servicios;

el servidor estando **caracterizado por** un segundo receptor (23) para recibir, desde una red intermedia con la cual el servidor tiene una relación de confianza, otra solicitud que incluye una identidad del usuario, la dirección restringida y una indicación de que el identificador de usuario está autenticado mediante la red intermedia, en el que la red intermedia es una red de subsistema multimedia IP que tiene una relación de confianza con otra red de subsistema multimedia IP en la cual está registrado el usuario;

un segundo transmisor (24) para enviar un mensaje de respuesta a la red intermedia, incluyendo el mensaje de respuesta credenciales utilizables para obtener de la dirección restringida el servicio solicitado;

un tercer receptor (25) para recibir del usuario un mensaje de solicitud de servicios, incluyendo el mensaje de solicitud de servicios la dirección restringida y las credenciales;

un procesador (26) para determinar si la dirección restringida, la identidad del usuario y las credenciales son válidas y, en caso de que se determine que lo son, proporcionar el servicio.

11. Un nodo (26) para utilizar en una red de comunicación intermedia que tiene una relación de confianza con otra red de subsistema multimedia IP en la cual está registrado el usuario, el nodo estando **caracterizado por que** comprende:

un primer receptor (27) para recibir del usuario un mensaje de solicitud, incluyendo el mensaje de solicitud una dirección restringida para una zona restringida de un servidor, teniendo el servidor una relación de confianza con la red de comunicación intermedia;

un primer procesador (28) para autenticar un identificador de usuario asociado con el usuario;

un primer transmisor (29) para enviar al servidor una tercera solicitud, incluyendo la tercera solicitud una identidad del usuario y la dirección restringida, y una indicación de que el identificador el usuario está autenticado;

un segundo receptor (30) para recibir del servidor un mensaje de respuesta, incluyendo el mensaje de respuesta información de cobro y credenciales utilizables para obtener de la dirección restringida el servicio solicitado;

una función (31) de cobro para cobrar al usuario en función de la información de cobro recibida; y

un segundo transmisor (32) para enviar al usuario las credenciales utilizables para acceder a los servicios a través de la dirección restringida.

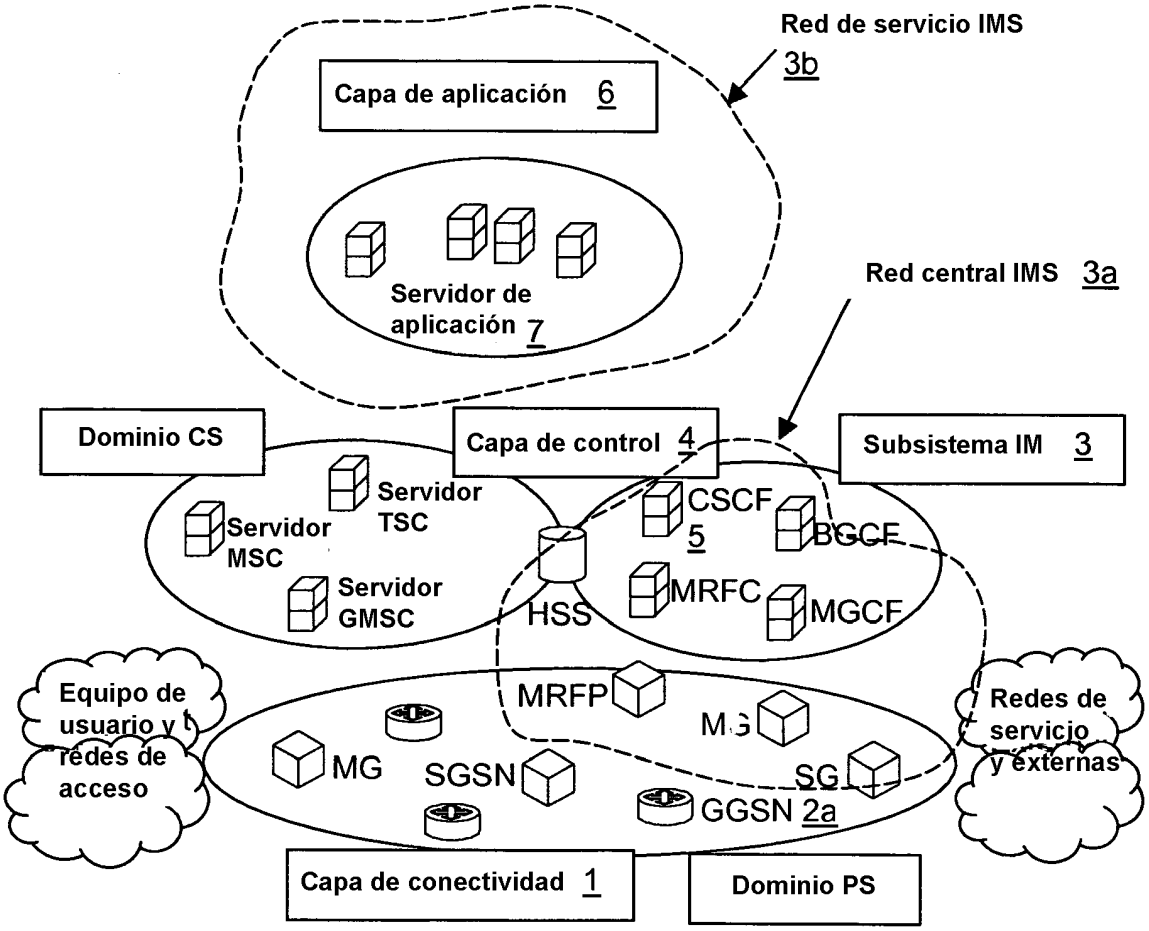

Figura 1 (técnica anterior)

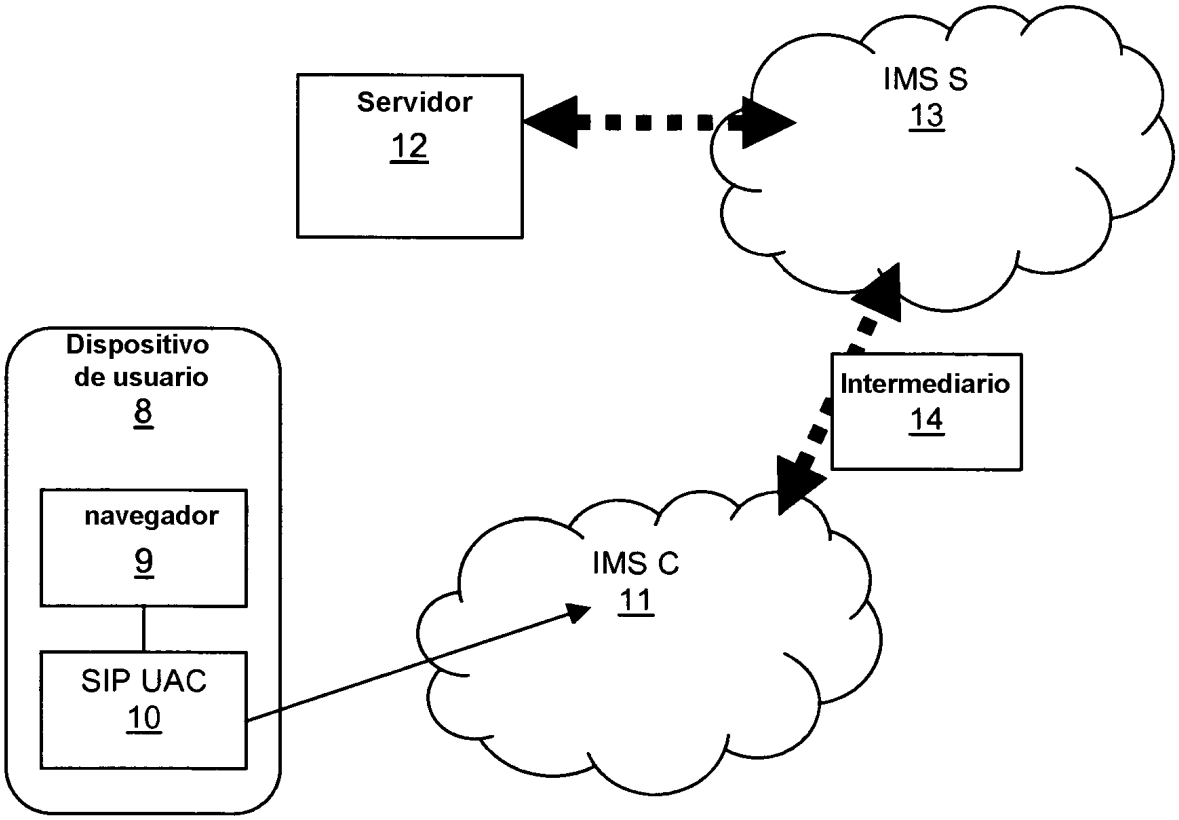
Servidor
12
IMS S
13
Dispositivo
de usuario
8
Intermediario
14
navegador
9
IMS C
11
SIP UAC
10

Figura 2

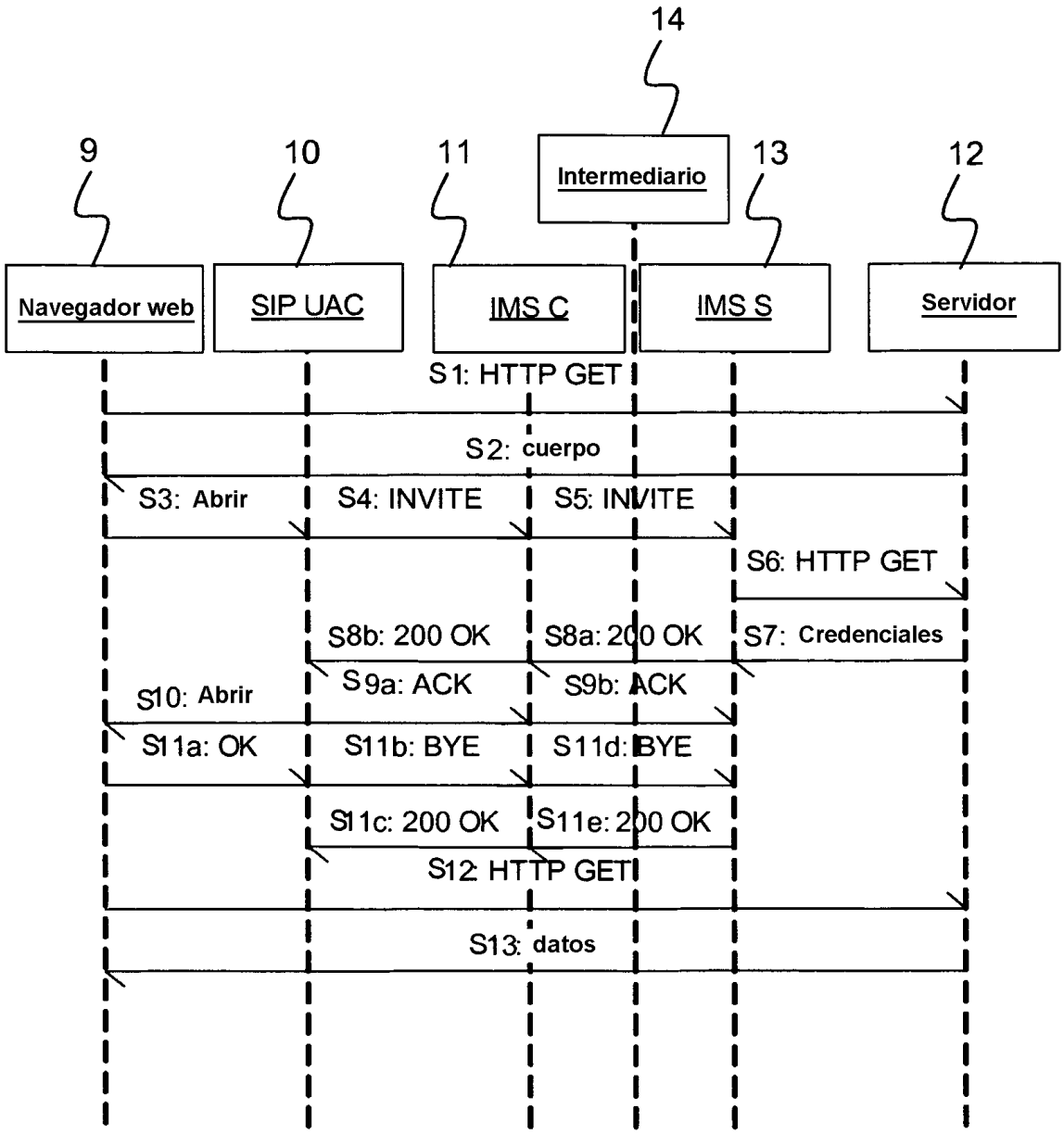
14
9
10
11
Intermediario
13
12
Navegador web
SIP UAC
IMS C
IMS S
Servidor
S1: HTTP GET
S2: cuerpo
S3: Abrir
S4: INVITE
S5: INVITE
S6: HTTP GET
S8b: 200 OK
S8a: 200 OK
S7: Credenciales
S9a: ACK
S9b: ACK
S10: Abrir
S11a: OK
S11b: BYE
S11d: BYE
S11c: 200 OK
S11e: 200 OK
S12: HTTP GET
S13: datos

Figura 3

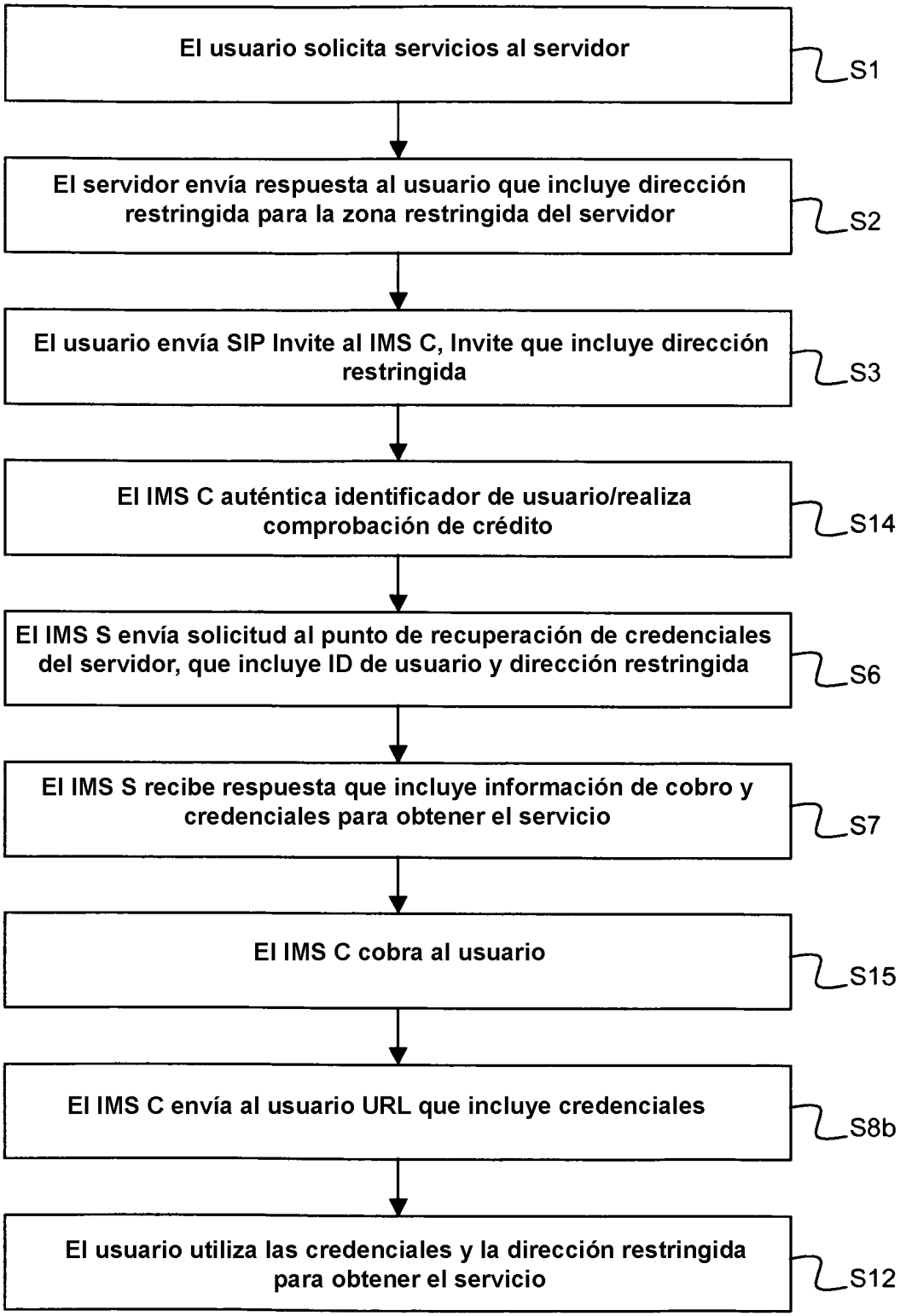
El usuario solicita servicios al servidor
S1
El servidor envía respuesta al usuario que incluye dirección restringida para la zona restringida del servidor
S2
El usuario envía SIP Invite al IMS C, Invite que incluye dirección restringida
S3
El IMS C auténtica identificador de usuario/realiza comprobación de crédito
S14
El IMS S envía solicitud al punto de recuperación de credenciales del servidor, que incluye ID de usuario y dirección restringida
S6
El IMS S recibe respuesta que incluye información de cobro y credenciales para obtener el servicio
S7
El IMS C cobra al usuario
S15
El IMS C envía al usuario URL que incluye credenciales
S8b
El usuario utiliza las credenciales y la dirección restringida para obtener el servicio
S12

Figura 4

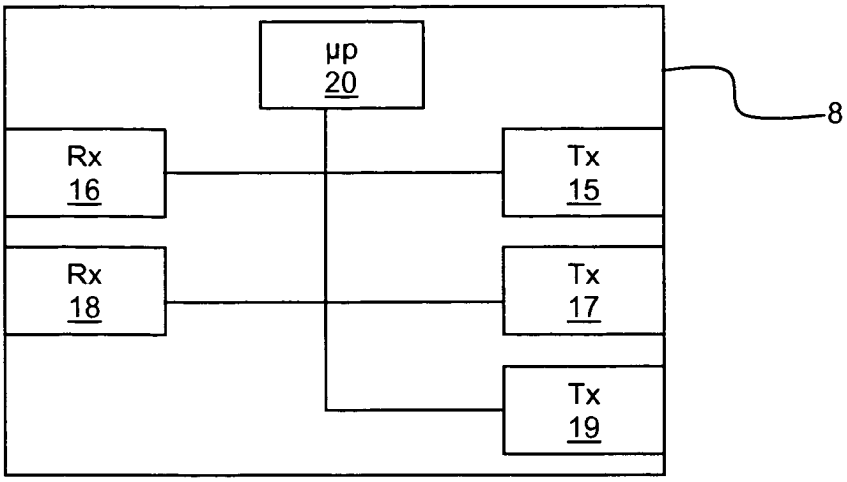

Figura 5

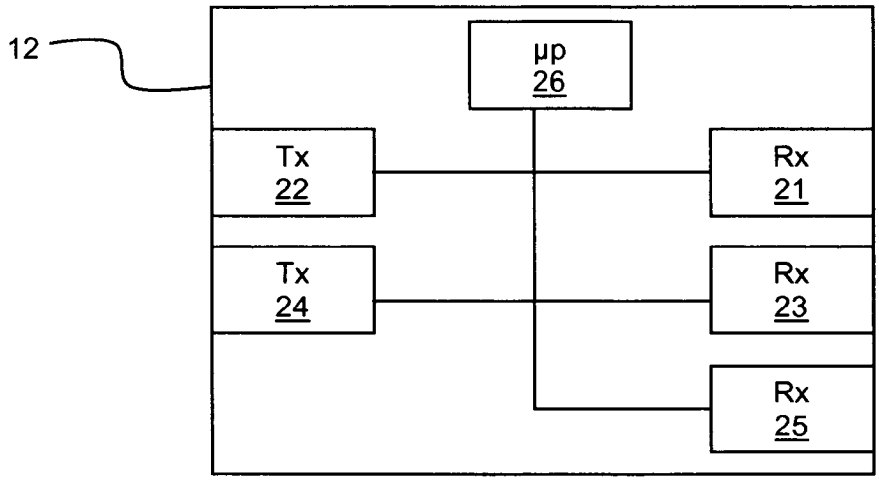

Figura 6

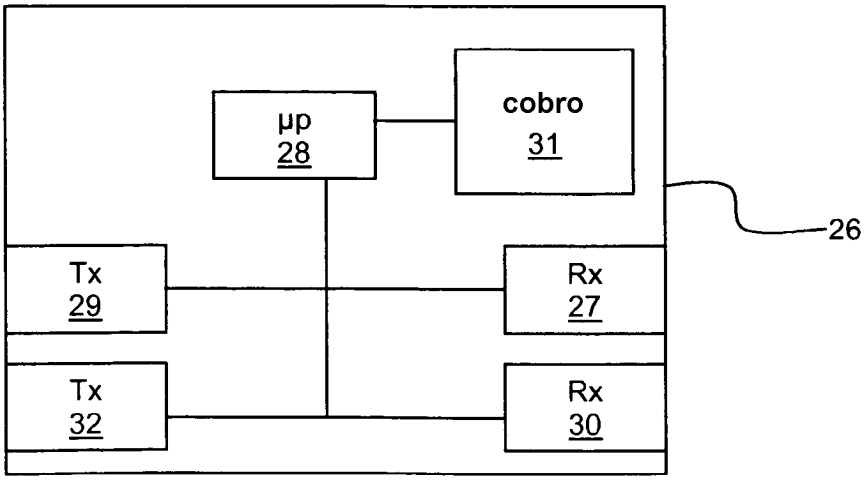

Figura 7