(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 524**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.01.2004 E 04703857 (5)**

(97) Fecha y número de publicación de la concesión europea: **25.02.2015 EP 1590914**

(54) Título: **Método y aparato para autorizar acceso a información de usuario en una red**

(30) Prioridad:

04.02.2003 US 444687 P
19.12.2003 US 739138

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2015

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

KISS, KRISZTIAN;
TUOHINO, MARKKU y
WESTMAN, IKKA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y aparato para autorizar acceso a información de usuario en una red

Campo técnico

Esta invención se refiere a redes, y más específicamente a autorizar acceso a información de usuario en una red o sistema.

Técnica antecedente

Los dispositivos y entidades en redes generalmente se comunican entre sí regularmente, enviando instrucciones y/o datos. Para que un primer dispositivo de red envíe información a un segundo dispositivo de red, el primer dispositivo de red debe conocer que el segundo dispositivo de red está realmente conectado a la red y puede recibir la información. En algunas redes, los dispositivos de red deben registrarse con una entidad de red, por lo tanto, esta entidad de red envía información acerca del dispositivo de red y su registro actual con la red. Los dispositivos de red que desean enviar información al dispositivo de red registrado pueden a continuación acceder a la entidad de red que contiene la información para determinar que el dispositivo de red registrado está realmente registrado, antes de intentar enviar la información del dispositivo de red registrado. Además, la entidad de red puede realizar un proceso de verificación y/o un proceso de autenticación en el cual se verifica un dispositivo de red que solicita la información de otro dispositivo de red para determinar que el dispositivo de red solicitante está autorizado a recibir la información del segundo dispositivo de red. Si el primer dispositivo de red no está autorizado, entonces la entidad de red no puede enviar al primer dispositivo de red información en relación con el segundo dispositivo de red. Si el primer dispositivo de red está autorizado a recibir información del segundo dispositivo de red, la entidad de red puede a continuación reenviar esta información al primer dispositivo de red. El primer dispositivo de red puede a continuación comenzar la comunicación con o enviar información al segundo dispositivo de red. Sin embargo, surgen problemas cuando la red o el sistema únicamente permiten acceso a la información de usuario mediante el usuario real u otras identidades del usuario.

Un ejemplo de esto está en las redes de la versión 5 del Subdominio Multimedia del Protocolo de Internet de Abonado Móvil Internacional del Proyecto Común de Tecnologías Inalámbricas de la Tercera Generación (3GPP IMS) que usan el lote de evento de estado de registro del Protocolo de Iniciación de Sesión (SIP) para informar a dispositivos de red acerca del estado del registro de los suscriptores al lote de evento. La Versión 5 del IMS del 3GPP usa el lote de evento de estado de registro de SIP para informar acerca del estado de registro a los suscriptores del lote de evento. Todos los lotes de evento de SIP, incluyendo el lote de evento de estado de registro, requieren autenticación y autorización de las solicitudes SUSCRIBIR de SIP (SIP SUBSCRIBE) antes de aceptarlas por el notificador (receptor de la solicitud). En redes/sistemas actuales tales como estos, la autenticación se resuelve durante el registro, la Función de Control de Estado de Llamada de Intermediario (P-CSCF) siempre inserta una identidad confiable del usuario a todas las solicitudes SIP posteriores.

Sin embargo, las redes/sistemas de la Ver-5 actuales no proporcionan ninguna solución de autorización para el lote de evento de estado de registro. Las especificaciones de la Ver-5 restringen la lista de suscriptores autorizados a que sean el usuario cuyo estado de registro está en cuestión y la P-CSCF a través de la que se transfiere toda la comunicación SIP del usuario particular. La solución real de cómo decide la Función de Control de Estado de Llamada Servidora (S-CSCF) (notificador del lote de evento), si la fuente de la solicitud SUSCRIBIR de SIP se autoriza, queda indefinida. Sin autorización, cualquier usuario puede suscribirse al estado de registro de alguien cualquiera y recibir el estado de todas las identidades de usuario públicas de ese usuario particular.

El documento "3rd Generation Varnisher Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SPD; stage 3 (Release 5)", 3GPP standard; 3GPP TS 24.229, 3rd Generation Partnership Project (3GPP), Mobile Competent Sensor; 650 Route des lucioles; F-06921 Sophia-Antipolis CDEX; Francia, Nº V 5.3.0, 20 de diciembre de 2012, analiza en la sección 5.4.2.1 suscripciones a eventos de S-CSCF. Cuando llega una solicitud SUSCRIBIR entrante dirigida a la S-CSCF que contiene el encabezamiento de evento (Event) con el lote de evento de registro, la S-CSCF deberá: comprobar, si basándose en política local, la solicitud se generó mediante un usuario que está autorizado a suscribirse a estos estados de registro de usuario y generar una respuesta 2xx que realiza acuse de recibo a la solicitud SUSCRIBIR y que indica que la subscripción autorizada fue satisfactoria como se describe en draft-letf-sipping-reg-event-00[43].

Divulgación de la invención

La presente invención es como se expone en las reivindicaciones independientes.

La presente divulgación se refiere a un método y sistema para autorizar acceso a información de un usuario. El sistema incluye una primera entidad de red y una segunda entidad de red. La primera entidad de red envía una solicitud para información de un usuario a la segunda entidad de red. La segunda entidad de red recibe la solicitud para información del usuario, verifica que la primera entidad de red está autorizada a recibir la información solicitada,

y genera una respuesta que autoriza la solicitud si la primera entidad de red está autorizada a recibir la información. La verificación puede incluir comparar la primera entidad de red frente a todas las identidades de usuario públicas no prohibidas del usuario, comparando la primera entidad de red frente a todas las entidades de red identificadas en una solicitud anterior, y comparar la primera entidad de red frente a todos los servidores de aplicación que no pertenecen a proveedores de terceros fuera de una red a la que el usuario está conectado.

Breve descripción de los dibujos

La presente invención se describe adicionalmente en la descripción detallada que sigue en referencia a la pluralidad de dibujos indicada a modo de ejemplos no limitantes de realizaciones de la presente invención en las que números de referencia similares representan partes similares a lo largo de todas las varias vistas de los dibujos y en las que:

La Figura 1 es un sistema para autorizar acceso a información de usuario de acuerdo con una realización de ejemplo de la presente invención;
La Figura 2 es un diagrama de flujo de un proceso de ejemplo para autorizar acceso a información de usuario en una red de acuerdo con una realización de ejemplo de la presente invención;
La Figura 3 es un diagrama de señalización de equipo de usuario que realiza una solicitud para información de usuario de acuerdo con una realización de ejemplo de la presente invención;
La Figura 4 es un diagrama de señalización de equipo de usuario que envía una solicitud para información de usuario mediante un intermediario de acuerdo con una realización de ejemplo de la presente invención;
La Figura 5 es un diagrama de señalización de un intermediario que envía una solicitud para información sobre un usuario de acuerdo con una realización de ejemplo de la presente invención;
La Figura 6 es un diagrama de señalización de un servidor de aplicación que envía una solicitud para información de usuario de acuerdo con una realización de ejemplo de la presente invención;
La Figura 7 es un diagrama de señalización para autorizar acceso a información de usuario en una red IMS del 3GPP de acuerdo con una realización de ejemplo de la presente invención; y
La Figura 8 es un diagrama de flujo de un proceso de ejemplo para autorizar a suscriptores para un lote de evento de estado de registro de un usuario de acuerdo con una realización de ejemplo de la presente invención.

Mejor modo para llevar a cabo la invención

Las particularidades mostradas en el presente documento son a modo de ejemplo y para fines de análisis ilustrativo de las realizaciones de la presente invención. La descripción tomada con los dibujos hace evidente para los expertos en la materia cómo la presente invención puede realizarse en la práctica.

Además, pueden mostrarse disposiciones en diagramas de bloques para evitar oscurecer la invención, y también en vista del hecho de que detalles específicos con respecto a la implementación de tales disposiciones de diagramas de bloques son altamente dependientes de la plataforma en la que se ha de implementar la presente invención, es decir, los detalles específicos deberían estar bien dentro del ámbito de un experto en la materia. Cuando se exponen detalles específicos (por ejemplo, circuitos, diagramas de flujo) para describir realizaciones de ejemplo de la invención, debería ser evidente para un experto en la materia que la invención puede ponerse en práctica sin estos detalles específicos. Finalmente, debería ser evidente que cualquier combinación de circuitería de cableado permanente e instrucciones de software puede usarse para implementar realizaciones de la presente invención, es decir, la presente invención no está limitada a ninguna combinación específica de circuitería de hardware ni instrucciones de software.

Aunque pueden describirse realizaciones de ejemplo de la presente invención usando un diagrama de bloques de sistema de ejemplo en un entorno de unidad anfitrión de ejemplo, la práctica de la invención no está limitada a lo mismo, es decir, la invención puede ponerse en práctica con otros tipos de sistemas, y en otros tipos de entornos.

La referencia en la memoria descriptiva a "una realización" significa que un rasgo, estructura o característica particular descrito en relación con la realización se incluye en al menos una realización de la invención. Las apariciones de la frase "en una realización" en diversos lugares en la memoria descriptiva no se refieren todas necesariamente a la misma realización.

La presente invención se refiere al método y sistema para autorizar acceso a información de un usuario. El equipo de usuario del usuario puede conectarse a una red o sistema con otros dispositivos de red y entidades de red. Los dispositivos o entidades de red pueden ser cualquier tipo de dispositivos de red tales como otro equipo de usuario, servidores, intermediarios, pasarelas, enrutadores, terminales, etc. Una o más entidades de red en la red pueden contener información en relación con usuarios y/o equipo de usuario en la red. Otros dispositivos de red o entidades pueden desear obtener la información acerca de un usuario particular y, por lo tanto, pueden solicitar acceso a esta información desde una entidad de red servidora que contiene (por ejemplo, almacena) la información de usuario. La entidad de red servidora puede a continuación verificar que la fuente de la solicitud está autorizada a recibir la información del usuario, y si es así, la entidad de red servidora puede a continuación generar una respuesta que autoriza la solicitud y proporcionar la información de usuario para el dispositivo o entidad de red solicitante. La autorización puede incluir comparar información en la solicitud que identifica al solicitante con información

almacenada en la entidad de red servidora de los dispositivos/entidades de red autorizados a acceder a la información del usuario particular. La información de los dispositivos/entidades de red autorizados a acceder a la información del usuario particular puede cargarse y almacenarse inicialmente en la entidad de red servidora durante la inicialización de la red/sistema o la inicialización de la entidad de red y/o puede enviarse dinámicamente a la entidad de red servidora y/o modificarse durante la operación de la red/sistema.

El equipo de usuario puede ser cualquier tipo de dispositivo de red, fija o inalámbrica, que pueda tener un usuario asociado tal como, por ejemplo, un terminal, ordenador, teléfono inalámbrico, servidor, Asistente Digital Personal (PDA), ordenador portátil, etc. Además, la información del usuario puede incluir muchos tipos de información, por ejemplo, información de registro, identificaciones de usuario, localización de usuario, tipo de equipo de usuario, capacidades de equipo de usuario, etc.

La Figura 1 muestra un sistema para autorizar acceso a información de usuario de acuerdo con una realización de ejemplo de la presente invención. El sistema incluye una entidad de red 10 servidora que puede recibir y almacenar información en relación con uno o más usuarios, y recibir solicitudes para esta información. El sistema puede incluir también muchos otros tipos de dispositivos de red o de sistema que pueden enviar o solicitar información desde la entidad de red 10 servidora tal como, por ejemplo, equipo de usuario 12, equipo de usuario 14, 16 a través de intermediarios 16, 17, servidores de aplicación u otros servidores 18, 20, u otras entidades de red 22, 24.

El equipo de usuario 12 puede desear acceder a información en relación con sí mismo u otro usuario, por ejemplo, el equipo de usuario 14. El equipo de usuario 12 puede a continuación solicitar esta información desde la entidad de red 10 servidora, en la cual la entidad de red 10 servidora verifica que el equipo de usuario 12 está autorizado a recibir la información del equipo de usuario 14, y si es así, reenvía la información al equipo de usuario 12. En algunos sistemas, puede haber equipo de usuario que únicamente hace de interfaz a la entidad de red 10 servidora a través de un intermediario u otro dispositivo 16. En este escenario de ejemplo, el equipo de usuario 14 que desea información de usuario de otro usuario, o de sí mismo, puede enviar una solicitud al intermediario 16 que a continuación reenvía la solicitud a la entidad de red 10 servidora. La entidad de red 10 servidora, después de verificar que el equipo de usuario 14 está autorizado a recibir la información solicitada, puede a continuación reenviar la información solicitada al intermediario 16 que a continuación a su vez la reenvía al equipo de usuario 14. De manera similar, los servidores de aplicación 18, 20 u otras entidades de red 22, 24 pueden desear información de otro o de su propio usuario y reenviar una solicitud directamente a la entidad de red 10 servidora en la cual su solicitud se verifica como que está autorizada a recibir la información, y si está autorizada, la información solicitada se reenvía al servidor de aplicación o entidad de red en consecuencia.

La Figura 2 muestra un diagrama de flujo de un proceso de ejemplo para autorizar acceso a información de usuario en una red de acuerdo con una realización de ejemplo de la presente invención. Se recibe S1 una solicitud para información de un usuario. La fuente de la solicitud puede compararse frente a entidades de red y/o identificaciones de usuario autorizadas a recibir la información solicitada del usuario S2. Puede a continuación determinarse si la fuente está autorizada a recibir la información solicitada S3 y si no, puede generarse una respuesta denegando acceso a la información solicitada del usuario S4. Si la fuente está autorizada, puede generarse una respuesta que autoriza la solicitud S5 y reenviarse la información solicitada a la fuente de la solicitud S6.

La Figura 3 muestra un diagrama de señalización de equipo de usuario que realiza una solicitud para información de usuario de acuerdo con una realización de ejemplo de la presente invención. El equipo de usuario 12 puede enviar una solicitud a una entidad de red 10 que solicita información de un usuario. La entidad de red 10 puede enviar a continuación un mensaje de acuse de recibo al equipo de usuario 12 que realiza acuse de recibo de la recepción de la solicitud. La entidad de red 10 puede verificar que el equipo de usuario 12 está autorizado a recibir la información solicitada comparando información en la solicitud con información almacenada en la entidad de red 10 servidora. Si está autorizado, la entidad de red 10 puede enviar una respuesta que notifica al equipo de usuario 12 de este hecho y puede enviar también la información de usuario solicitada mediante la respuesta y/o una respuesta separada. El equipo de usuario 12 puede a continuación realizar acuse de recibo de la recepción de la respuesta.

La Figura 4 muestra un diagrama de señalización de equipo de usuario que envía una solicitud para información de usuario mediante un intermediario de acuerdo con una realización de ejemplo de la presente invención. En esta realización de ejemplo, el equipo de usuario 14 puede hacer de interfaz con la entidad de red 10 servidora mediante una entidad de red intermediaria 16. Por lo tanto, el equipo de usuario 14 puede enviar una solicitud para información de usuario a la entidad de red intermediaria 16, que a continuación a su vez reenvía esta solicitud a la entidad de red 10 servidora. La entidad de red 10 servidora puede a continuación enviar un mensaje de acuse de recibo al equipo de usuario 14 a través de la entidad de red intermediaria 16 que realiza acuse de recibo de la recepción de la solicitud para información. La entidad de red 10 servidora comprueba para observar si el equipo de usuario 14 está autorizado a recibir la información de usuario comparando información en la solicitud con información almacenada en la entidad de red 10 servidora, y puede enviar una respuesta al equipo de usuario 14 mediante la entidad de red intermediaria 16 concediendo o denegando el acceso a la información. Si se concede el acceso, la respuesta puede incluir también alguna o toda la información solicitada. El equipo de usuario 14 puede a continuación enviar un acuse de recibo a la entidad de red 10 servidora a través de la entidad de red intermediaria 16 realizando acuse de recibo de la recepción de la respuesta.

La Figura 5 muestra un diagrama de señalización de un intermediario que envía una solicitud para información sobre un usuario de acuerdo con una realización de ejemplo de la presente invención. La entidad de red intermediaria 17 puede enviar una solicitud a una entidad de red 10 que solicita información de un usuario. La entidad de red 10 puede a continuación enviar un mensaje de acuse de recibo a la entidad de red intermediaria 17 que realiza acuse de recibo de la recepción de la solicitud. La entidad de red 10 puede verificar que la entidad de red intermediaria 17 está autorizada a recibir la información solicitada comparando información en la solicitud con información almacenada en la entidad de red 10 servidora. Si está autorizada, la entidad de red 10 puede enviar una respuesta que notifica a la entidad de red intermediaria 17 de este hecho y puede enviar también la información de usuario solicitada mediante la respuesta y/o una respuesta separada. La entidad de red intermediaria 17 puede a continuación realizar acuse de recibo de la recepción de la respuesta.

La Figura 6 muestra un diagrama de señalización de un servidor de aplicación que envía una solicitud para información de usuario de acuerdo con una realización de ejemplo de la presente invención. El servidor de aplicación 18 puede enviar una solicitud a una entidad de red 10 que solicita información de un usuario. La entidad de red 10 puede a continuación enviar un mensaje de acuse de recibo al servidor de aplicación 18 que realiza acuse de recibo de la recepción de la solicitud. La entidad de red 10 puede verificar que el servidor de aplicación 18 está autorizado a recibir la información solicitada comparando información en la solicitud con información almacenada en la entidad de red 10 servidora. Si está autorizado, la entidad de red 10 puede enviar una respuesta que notifica al servidor de aplicación 18 de este hecho y puede enviar también la información de usuario solicitada mediante la respuesta y/o una respuesta separada. El servidor de aplicación 18 puede a continuación realizar acuse de recibo de la recepción de la respuesta.

La Figura 7 muestra un diagrama de señalización para autorizar acceso a información de usuario en una red de IMS del 3GPP de acuerdo con una realización de ejemplo de la presente invención. En esta realización de ejemplo, el equipo de usuario puede enviar una solicitud a una identidad de red servidora que es una Función de Control de Sesión de Llamada Servidora (S-CSCF) mediante una Función de Control de Sesión de Llamada de Intermediario (P-CSCF). En esta realización de ejemplo de la presente invención, la solicitud puede ser una solicitud para suscripción a un lote de evento de estado de registro de un usuario. El equipo de usuario puede realizar esta solicitud, una P-CSCF puede realizar esta solicitud por sí misma, o un servidor de aplicación u otra entidad de red pueden realizar esta solicitud a la S-CSCF.

Tras recibir la solicitud para información de suscripción, una función de control de estado de llamada servidora puede a continuación enviar un mensaje de acuse de recibo al equipo de usuario mediante la recepción de acuse de recibo de la solicitud de la función de control de estado de llamada de intermediario. La función de control de estado de llamada servidora puede a continuación verificar que el equipo de usuario está autorizado a recibir el lote de evento de estado de registro del usuario solicitado. En esta realización de ejemplo de la presente invención, las fuentes autorizadas de la solicitud pueden incluir todas las ID de usuario públicas no prohibidas del usuario, todas las entidades que se han incluido en un encabezamiento de TRAYECTORIA (PATH) anteriormente enviado a la función de control de estado de llamada servidora en una solicitud de REGISTRO (REGISTER) anterior, y a todos los servidores de aplicación que no pertenecen a proveedores de terceros. Estos servidores de aplicación pueden también coincidir con un perfil del usuario para el evento. La autorización de la solicitud para información de suscripción mediante la S-CSCF puede incluir comparar información en la solicitud con las fuentes autorizadas.

Si la fuente de la solicitud no está autorizada, la función de control de estado de llamada servidora puede prohibir acceso a la información de suscripción del usuario. Si la fuente de la solicitud está autorizada, la función de control de estado de llamada servidora puede generar una respuesta que realiza acuse de recibo de la solicitud de suscripción y que indica que la suscripción autorizada fue satisfactoria. Adicionalmente, la respuesta puede incluir un encabezamiento de Expiración (Expires) que contiene el mismo o un valor disminuido que un encabezamiento de Expiración en la solicitud de suscripción, y/o un encabezamiento de Contacto (Contact) que es un identificador generado en la función de control de estado de llamada servidora que ayuda a correlacionar refrescos para la suscripción. Posteriormente, la función de control de estado de llamada servidora puede realizar los procedimientos para notificación acerca del estado de registro como se han descrito en las especificaciones del IMS del 3GPP.

Los servidores de aplicación autorizados pueden incluir servidores de aplicación mencionados en un criterio de filtro asociados con una solicitud de REGISTRO anterior. Los criterios de registro pueden ser una regla, parte de una información de suscriptor usada para elegir o seleccionar aquellos servidores de aplicación que se visitan por el usuario. La función de control de estado de llamada servidora puede conocer todas las ID de usuario públicas no prohibidas de cada usuario, entidades incluidas en encabezamientos de TRAYECTORIA recibidos y todos los servidores de aplicación que no pertenecen a proveedores de terceros, antes de recibir ninguna solicitud para el lote de evento de estado de registro de un usuario. Además, la función de control de estado de llamada servidora puede conocer también otras ID de usuario no registradas de un usuario.

Por lo tanto, en esta realización de ejemplo de la presente invención, todas las subscripciones de lote de evento SIP (SUSCRIBIR de SIP) pueden necesitar autenticarse y autorizarse antes de que se acepten mediante el notificador (es decir, la S-CSCF). De acuerdo con un método propuesto, de acuerdo con qué entidades de red (por ejemplo, servidores) que están permitidos a suscribir el lote de evento de estado de registro pueden recogerse desde un

encabezamiento de Trayectoria de una solicitud de REGISTRO del Protocolo de Iniciación de Sesión (SIP). Se supone que estas entidades/servidores necesitan recibir comunicación SIP hacia el usuario y debería autorizarse, por lo tanto, a suscribirse al lote de evento de estado de registro.

De acuerdo con esta realización de la presente invención, la S-CSCF puede usar ciertos elementos del registro SIP para los fines de autorización del lote de evento de estado de registro. Los elementos pueden incluir la identidad de usuario pública del usuario y la lista de Trayectoria recibida en la solicitud de REGISTRO. La lista de trayectoria representa aquellos servidores en la trayectoria de la solicitud de REGISTRO de SIP, que están interesados en recibir comunicación SIP futura hacia el usuario. Por lo tanto, aquellos servidores pueden almacenar información relacionada con el registro del usuario. Como consecuencia, los servidores, parte de la lista de trayectoria, deberían autorizar a los suscriptores del lote de evento de estado de registro del usuario.

Por lo tanto, esta realización de la presente invención proporciona autorización del lote de evento de estado de registro para una S-CSCF cuando el notificador (es decir el elemento que enviará el respectivo NOTIFICAR (NOTIFY) al SUSCRIBIR, es decir la S-CSCF) recibe la solicitud de SUSCRIBIR para un lote de evento de estado de registro de usuario particular. Después de verificar la fuente de la solicitud de SUSCRIBIR (por medio de comprobar el campo de encabezamiento P-Identidad-Aseverada (P-Asserted-Identity)) el notificador puede comprobar la fuente de la solicitud de SUSCRIBIR frente a la lista de trayectoria y a las identidades de usuario públicas del usuario. Se autoriza la suscripción únicamente si existe una coincidencia.

La Figura 8 muestra un diagrama de flujo de un proceso de ejemplo para autorizar suscriptores para un lote de evento de estado de registro de un usuario de acuerdo con una realización de ejemplo de la presente invención. Se recibe una solicitud de suscripción desde una fuente en una función de control de estado de llamada servidora S10. La función de control de estado de llamada servidora compara información en la solicitud con información almacenada de suscriptores autorizados (es decir, entidades de red e identidades de usuario) S11. Los suscriptores autorizados pueden incluir todas las identidades de usuario públicas no prohibidas que el usuario de la fuente de la solicitud posee y que la S-CSCF conoce, todas las entidades identificadas mediante un encabezamiento de TRAYECTORIA enviado en una solicitud de REGISTRO anterior, o todos los servidores de aplicación que no pertenecen a proveedores de terceros. Se determina si la fuente de la solicitud es una identidad de usuario pública no prohibida S12, una entidad identificada mediante un encabezamiento de TRAYECTORIA enviado en una solicitud de REGISTRO de SIP anterior S13, o unos servidores de aplicación que no pertenecen a proveedores de terceros S14. Si la fuente de la solicitud no es ninguna de estas, la fuente no está autorizada a recibir la información solicitada, y la función de control de estado de llamada servidora puede enviar una respuesta que indica que la autorización de suscripción ha fallado S15. Si la fuente de la solicitud es una de estas, la función de control de estado de llamada servidora puede generar una respuesta que realiza acuse de recibo de la solicitud de suscripción y que indica que la suscripción autorizada fue satisfactoria S16 y a continuación realizar procedimientos para notificación acerca del registro S17.

La presente invención es ventajosa puesto que permite rendimiento de una decisión de autorización basándose en datos dinámicos almacenados en la S-CSCF, y no requiere tablas de dirección estática pre-configuradas (por ejemplo, la dirección de todas las P-CSCF de los asociados en itinerancia). Además, la presente invención permite autorización a información de un usuario a otras entidades de red y no solamente otras identidades de usuario públicas del usuario.

Se indica que los ejemplos anteriores se han proporcionado meramente para el fin de explicación y de ninguna manera deben interpretarse como limitantes de la presente invención. Aunque se ha descrito la presente invención con referencia a una realización preferida, se entiende que las palabras que se han usado en el presente documento son palabras de descripción e ilustración, en lugar de palabras de limitación. Pueden realizarse cambios en el ámbito de las reivindicaciones adjuntas, como actualmente establecidas y como modificadas, sin alejarse del alcance de la presente invención en sus aspectos. Aunque se ha descrito la presente invención en el presente documento con referencia a métodos, materiales, y realizaciones particulares, la presente invención no pretende limitarse a las particularidades desveladas en el presente documento, sino únicamente al alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método que comprende:

recibir una solicitud en una entidad de red (10) desde una fuente (12) para información de registro de un usuario;
verificar que la fuente (12) está autorizada a recibir la información, comprendiendo la verificación adicionalmente:

comparar la fuente (12) de la solicitud frente a todas las identidades de usuario públicas no prohibidas del usuario, y
comparar la fuente (12) de la solicitud frente a todas las entidades de red identificadas en un encabezamiento de Trayectoria contenido en una solicitud de Registro anterior relacionada con el usuario; y

generar una respuesta que autoriza la solicitud si la fuente (12) está autorizada a recibir la información, en donde la fuente (12) está autorizada a recibir la información si existe una coincidencia en cualquiera de las comparaciones.

2. El método de acuerdo con la reivindicación 1, que comprende adicionalmente verificar que la entidad de red (10) está autorizada a recibir la información basándose en información dinámica almacenada en la entidad de red e información en la solicitud.

3. El método de acuerdo con la reivindicación 1, en el que la solicitud comprende una solicitud para suscripción a un lote de evento de estado de registro.

4. El método de acuerdo con la reivindicación 1, en el que el encabezamiento de Trayectoria incluye dispositivos de Función de Control de Sesión de Llamada de Intermediario (32) a los que el usuario está unido.

5. El método de acuerdo con la reivindicación 1, comprendiendo la verificación adicionalmente comparar la fuente (12) de la solicitud frente a todos los servidores de aplicación (18, 20) que coinciden con un Criterio de Filtro de perfil del usuario para un evento de Registro asociado a la solicitud.

6. El método de acuerdo con la reivindicación 1, en el que la respuesta comprende adicionalmente información de expiración de registro de usuario.

7. El método de acuerdo con la reivindicación 6, comprendiendo la información de expiración de registro de usuario un mismo valor o un valor disminuido de la segunda información de expiración de registro de usuario contenida en la solicitud.

8. El método de acuerdo con la reivindicación 1, comprendiendo la respuesta adicionalmente un encabezamiento de Contacto generado por la entidad de red (10), comprendiendo el encabezamiento de Contacto un identificador que ayuda a correlacionar refrescos para la solicitud.

9. El método de acuerdo con la reivindicación 1, que comprende adicionalmente realizar procedimientos de notificación de estado de registro por parte de la entidad de red (10) después de la generación de la respuesta.

10. El método de acuerdo con la reivindicación 1, en el que la entidad de red (10) es una Función de Control de Sesión de Llamada Servidora (34).

11. Una entidad de red (10) configurada para:

recibir una solicitud desde una fuente (12) para información de registro de un usuario;
verificar que la fuente (12) está autorizada a recibir la información, comprendiendo la verificación:

comparar la fuente (12) de la solicitud frente a todas las identidades de usuario públicas no prohibidas del usuario,
comparar la fuente (12) de la solicitud frente a todas las entidades de red identificadas en un encabezamiento de Trayectoria contenido en una solicitud de Registro anterior relacionada con el usuario; y

generar una respuesta que autoriza la solicitud si la fuente (12) está autorizada a recibir la información, en donde la fuente (12) está autorizada a recibir la información si existe una coincidencia en cualquiera de las comparaciones.

12. La entidad de red (10) de acuerdo con la reivindicación 11, en donde la entidad de red (10) es una Función de Control de Sesión de Llamada Servidora (34).

13. La entidad de red (10) de acuerdo con la reivindicación 11, en donde la entidad de red (10) está configurada adicionalmente para comparar la fuente (12) de la solicitud frente a todos los servidores de aplicación (18, 20) que

coinciden con un Criterio de Filtro de perfil del usuario para un evento de Registro asociado con la solicitud.

14. Un sistema que comprende:

una primera entidad de red, la primera entidad de red configurada para enviar una solicitud para información de registro de un usuario; y
una segunda entidad de red (10), estando configurada la segunda entidad de red para:

recibir la solicitud para información del usuario, verificar que la primera entidad de red está autorizada a recibir la información solicitada, comprendiendo la verificación adicionalmente:

comparar la fuente (12) de la solicitud frente a todas las identidades de usuario públicas no prohibidas del usuario, y
comparar la fuente (12) de la solicitud frente a todas las entidades de red identificadas en un encabezamiento de Trayectoria contenido en la solicitud de Registro anterior relacionada con el usuario; y

generar una respuesta que autoriza la solicitud si la primera entidad de red está autorizada a recibir la información, en donde la primera entidad de red está autorizada a recibir la información si existe una coincidencia en cualquiera de las comparaciones.

15. Un programa informático que, cuando se ejecuta en un ordenador (10), realiza el método de una cualquiera de las reivindicaciones anteriores 1 a 10.

FIG. 1

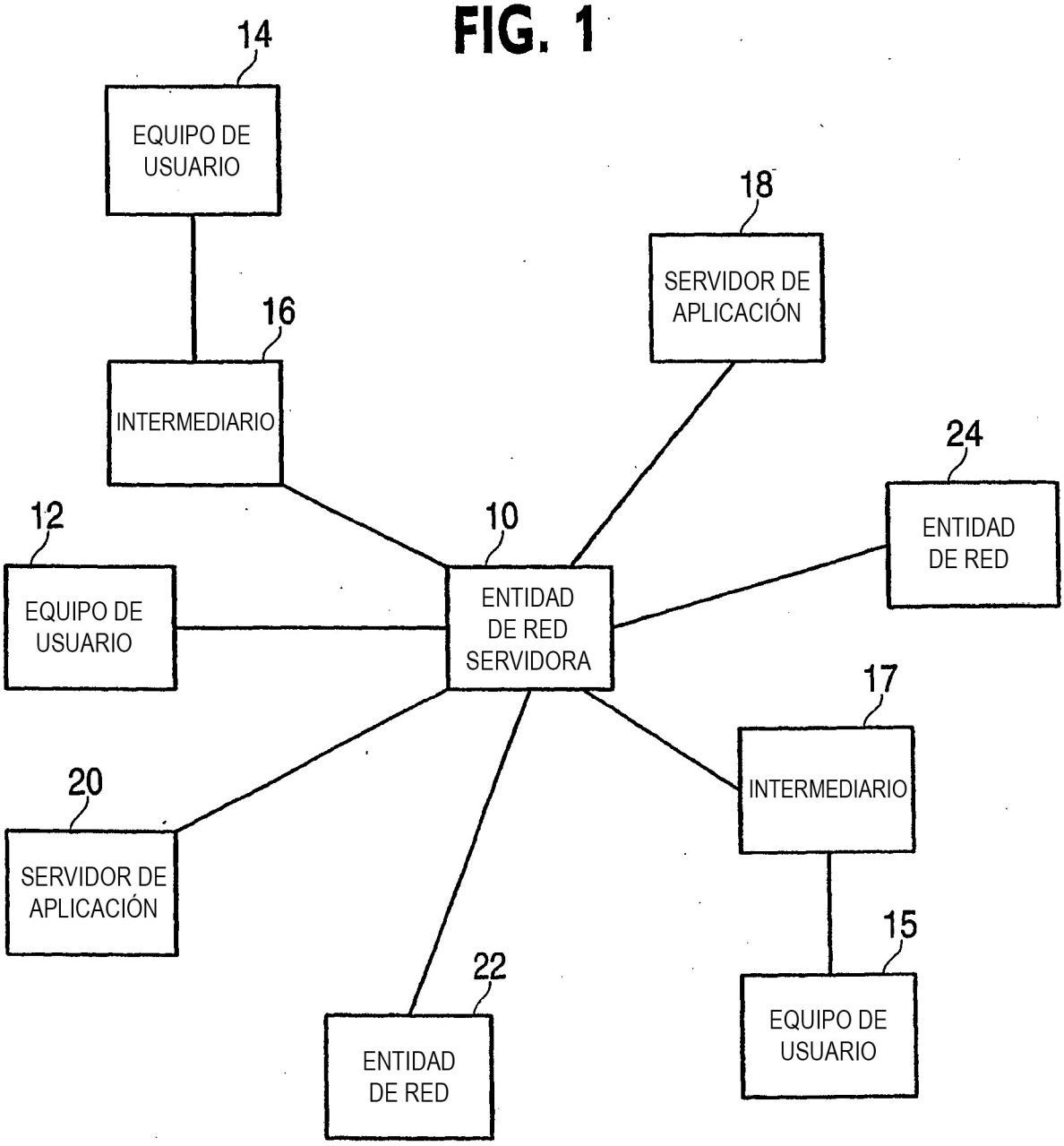

14
EQUIPO DE USUARIO
18
SERVIDOR DE APLICACIÓN
16
INTERMEDIARIO
24
ENTIDAD DE RED
12
10
EQUIPO DE USUARIO
ENTIDAD DE RED SERVIDORA
17
INTERMEDIARIO
20
SERVIDOR DE APLICACIÓN
15
22
ENTIDAD DE RED
EQUIPO DE USUARIO

FIG. 2

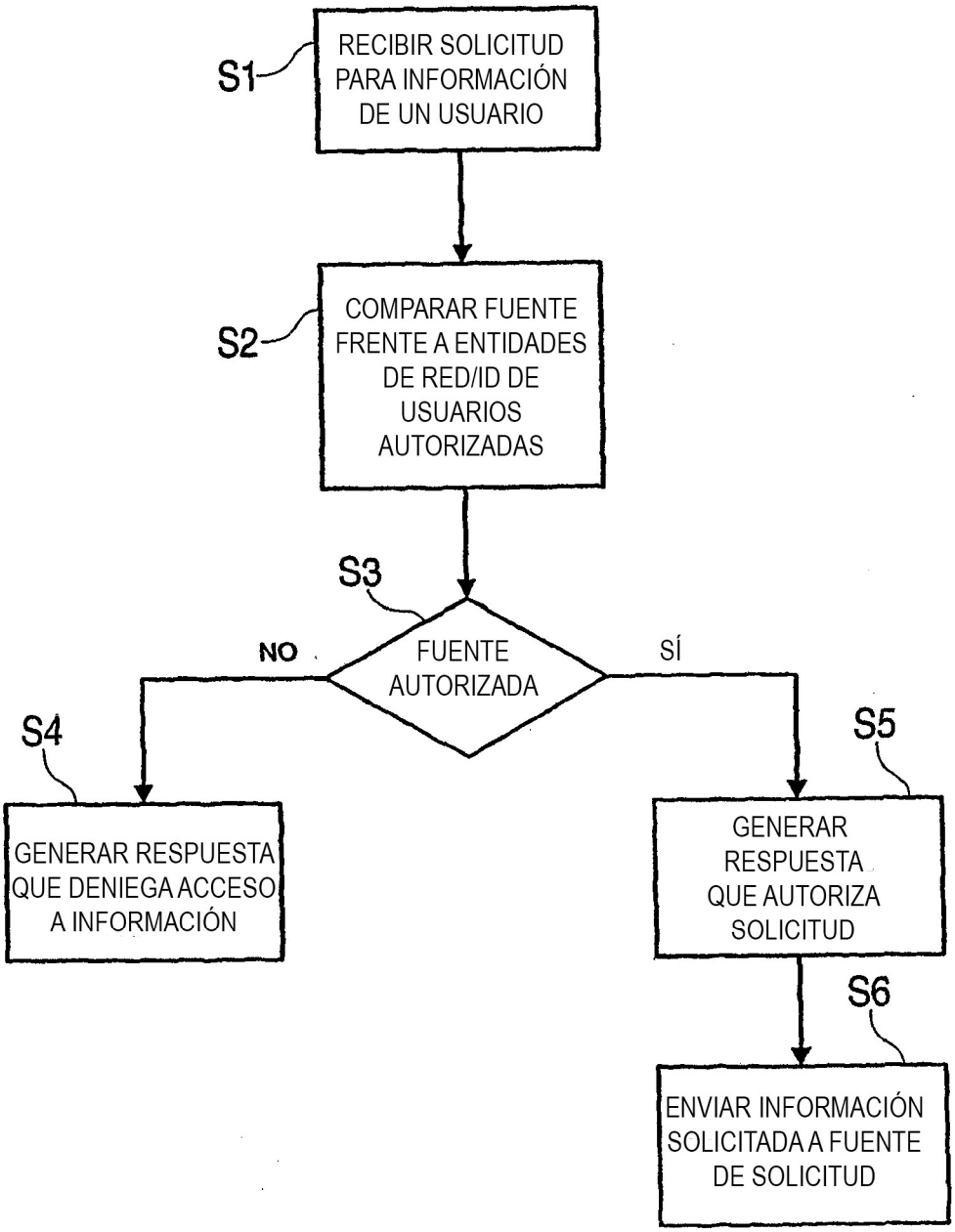

S1
RECIBIR SOLICITUD PARA INFORMACIÓN DE UN USUARIO
S2
COMPARAR FUENTE FRENTE A ENTIDADES DE RED/ID DE USUARIOS AUTORIZADAS
S3
FUENTE AUTORIZADA
NO
SÍ
S4
GENERAR RESPUESTA QUE DENIEGA ACCESO A INFORMACIÓN
S5
GENERAR RESPUESTA QUE AUTORIZA SOLICITUD
S6
ENVIAR INFORMACIÓN SOLICITADA A FUENTE DE SOLICITUD

FIG. 3

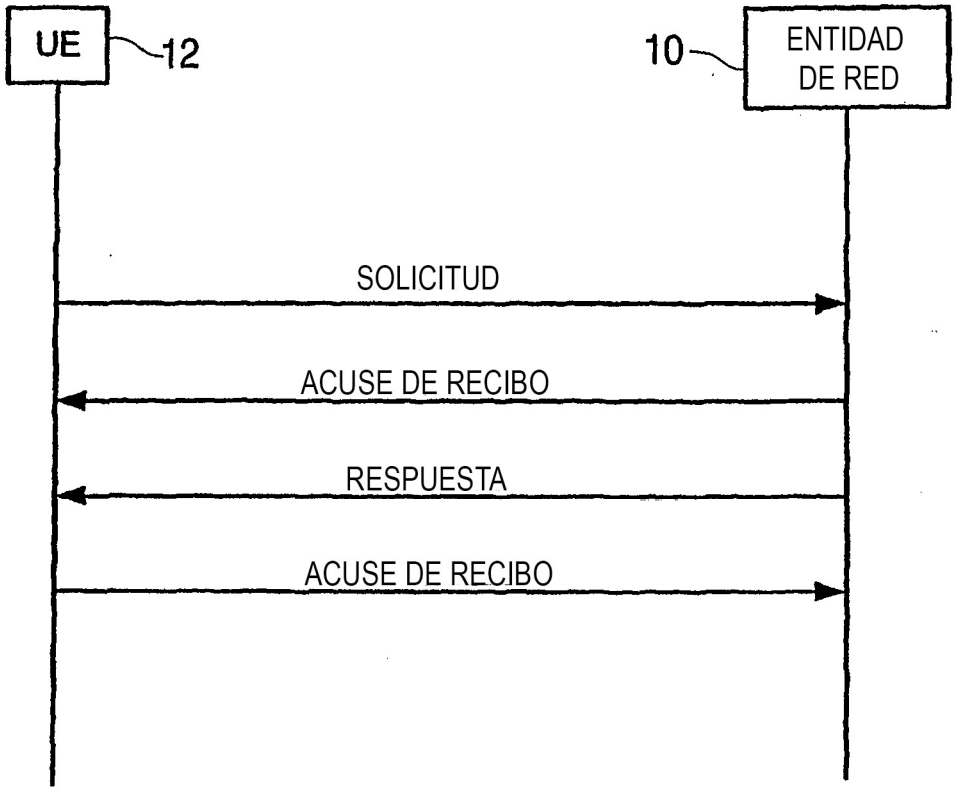

UE
12
10
ENTIDAD DE RED
SOLICITUD
ACUSE DE RECIBO
RESPUESTA
ACUSE DE RECIBO

FIG. 4

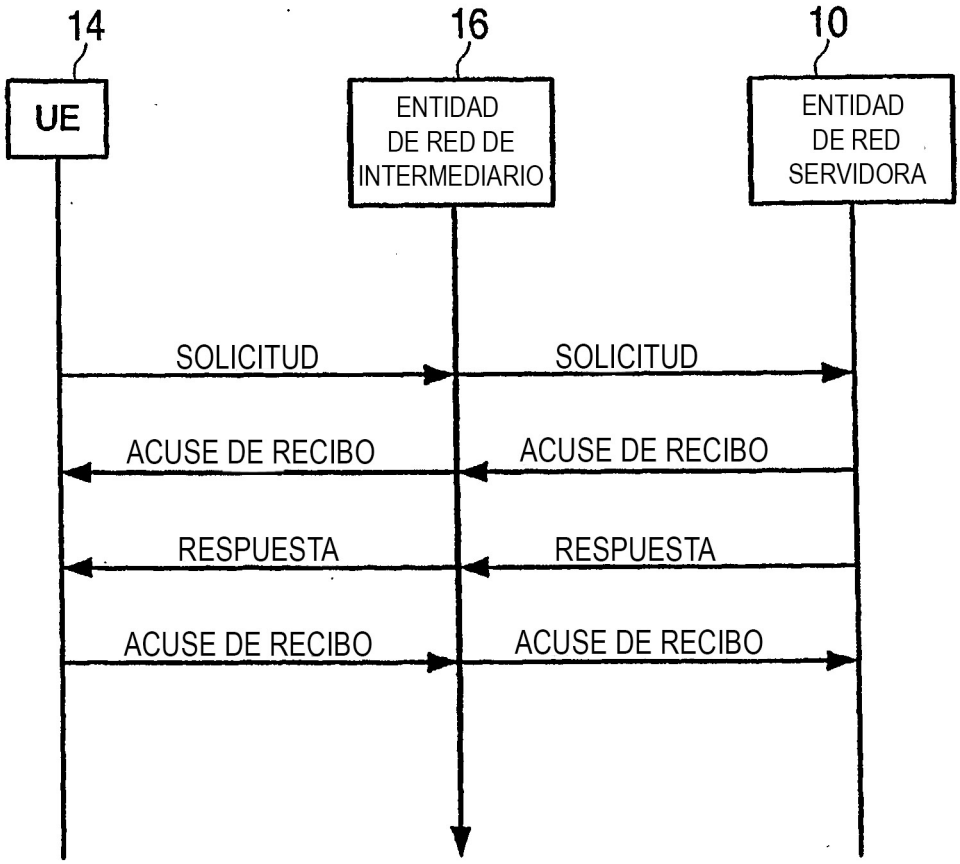

14
16
10
UE
ENTIDAD DE RED DE INTERMEDIARIO
ENTIDAD DE RED SERVIDORA
SOLICITUD
SOLICITUD
ACUSE DE RECIBO
ACUSE DE RECIBO
RESPUESTA
RESPUESTA
ACUSE DE RECIBO
ACUSE DE RECIBO

FIG. 5

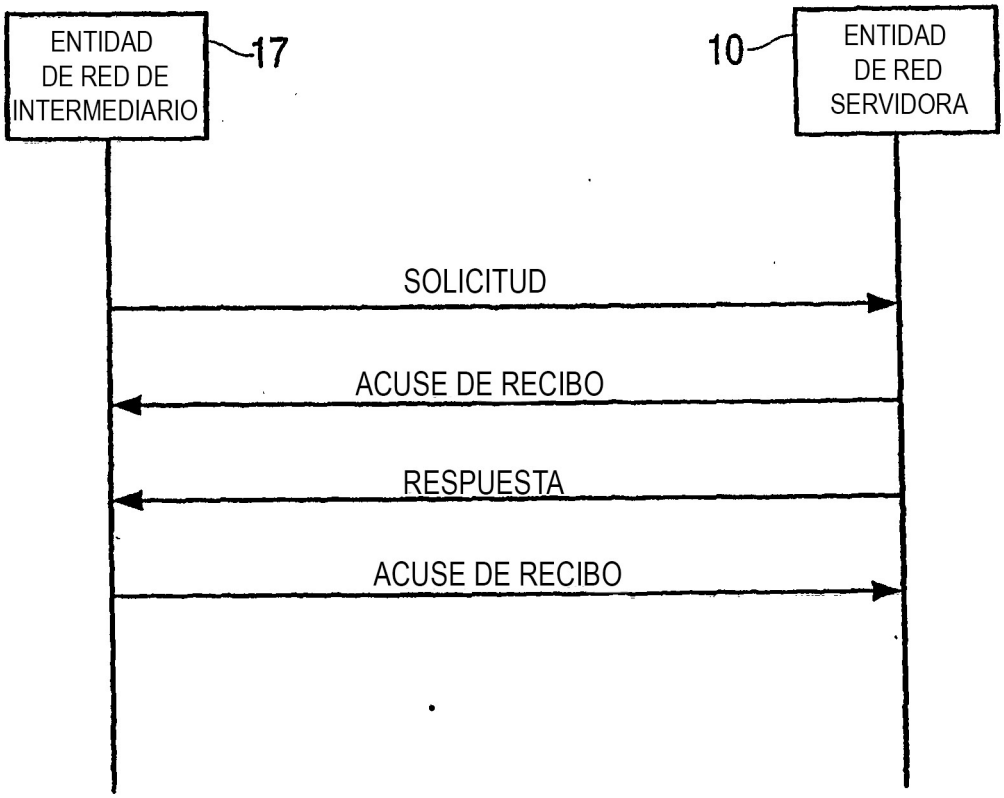

ENTIDAD DE RED DE INTERMEDIARIO
17
10
ENTIDAD DE RED SERVIDORA
SOLICITUD
ACUSE DE RECIBO
RESPUESTA
ACUSE DE RECIBO

FIG. 6

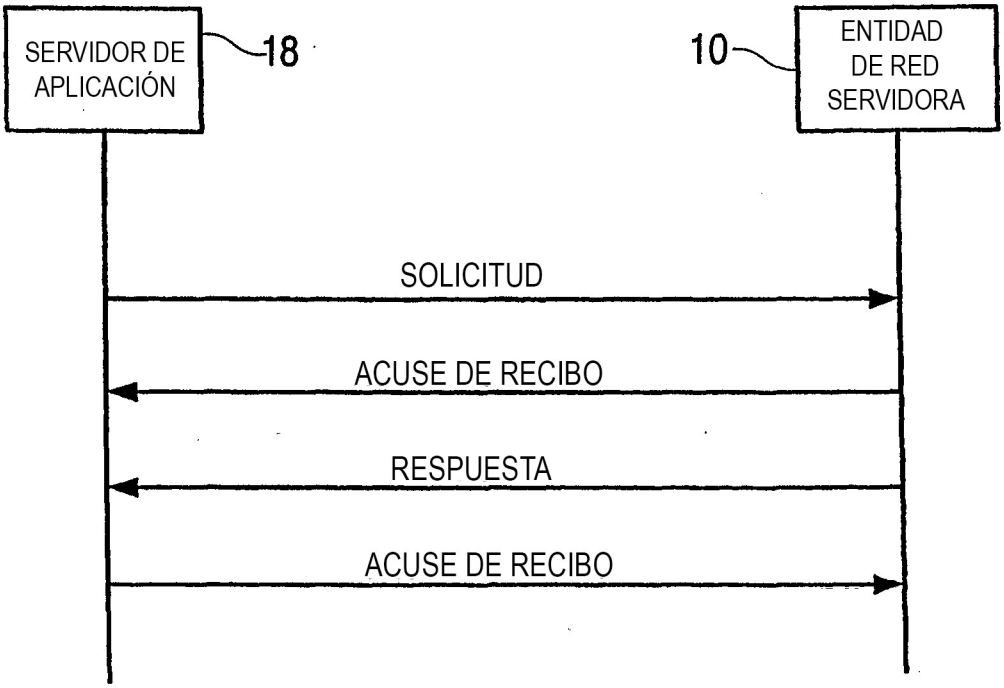

SERVIDOR DE APLICACIÓN
18
10
ENTIDAD DE RED SERVIDORA
SOLICITUD
ACUSE DE RECIBO
RESPUESTA
ACUSE DE RECIBO

FIG. 7

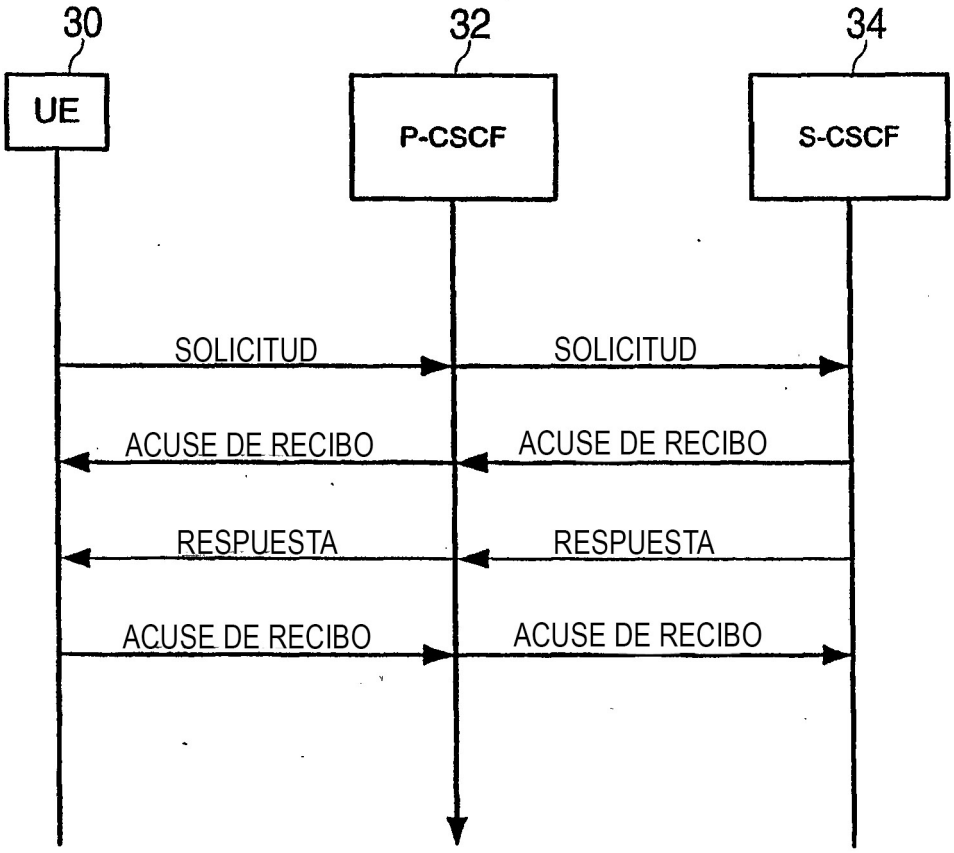
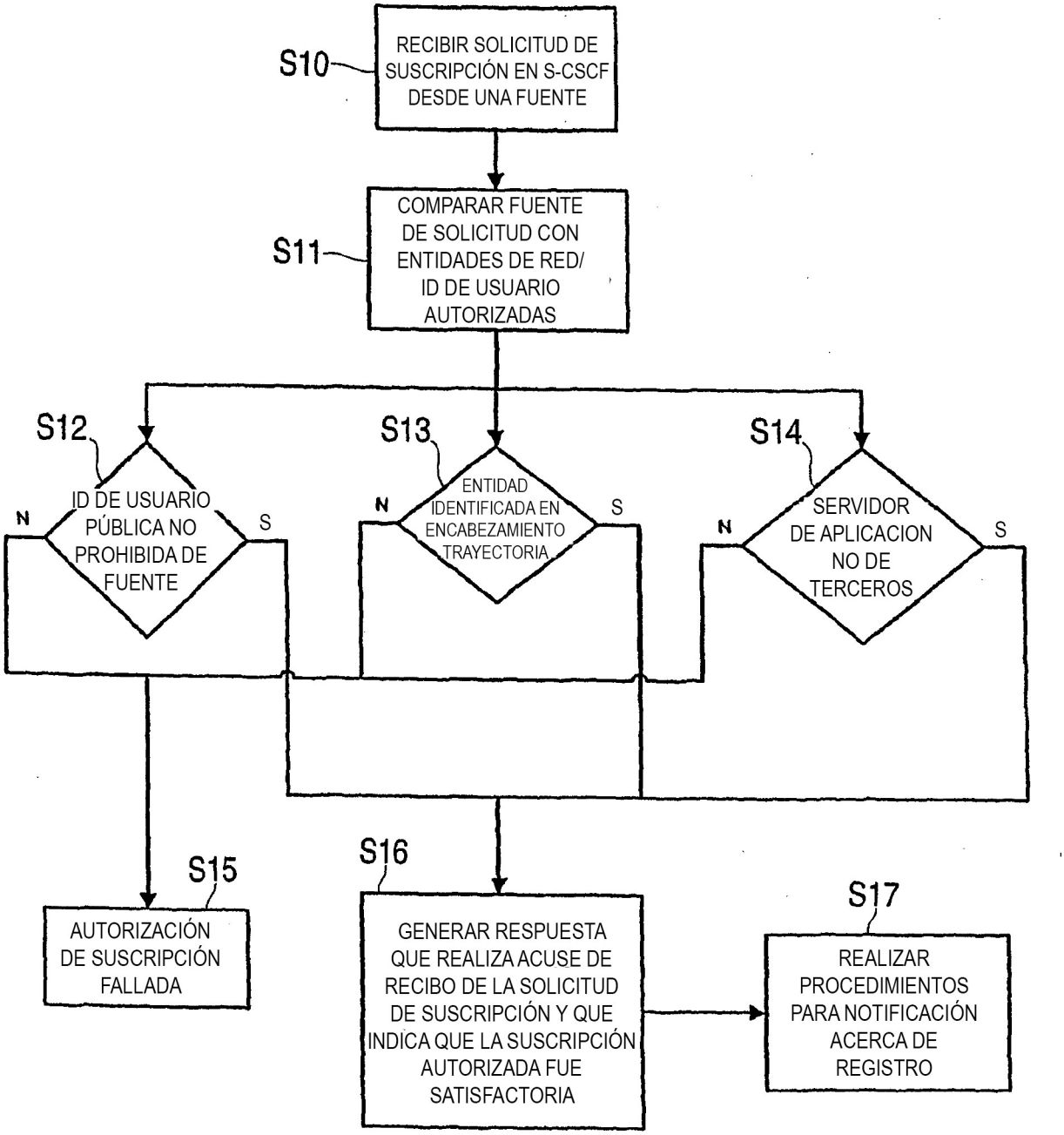

30
32
34
UE
P-CSCF
S-CSCF
SOLICITUD
SOLICITUD
ACUSE DE RECIBO
ACUSE DE RECIBO
RESPUESTA
RESPUESTA
ACUSE DE RECIBO
ACUSE DE RECIBO

FIG. 8


S10
RECIBIR SOLICITUD DE SUSCRIPCIÓN EN S-CSCF DESDE UNA FUENTE
S11
COMPARAR FUENTE DE SOLICITUD CON ENTIDADES DE RED/ ID DE USUARIO AUTORIZADAS
S12
ID DE USUARIO PÚBLICA NO PROHIBIDA DE FUENTE
N
S
S13
ENTIDAD IDENTIFICADA EN ENCABEZAMIENTO TRAYECTORIA
N
S
S14
SERVIDOR DE APLICACION NO DE TERCEROS
N
S
S15
AUTORIZACIÓN DE SUSCRIPCIÓN FALLADA
S16
GENERAR RESPUESTA QUE REALIZA ACUSE DE RECIBO DE LA SOLICITUD DE SUSCRIPCIÓN Y QUE INDICA QUE LA SUSCRIPCIÓN AUTORIZADA FUE SATISFACTORIA
S17
REALIZAR PROCEDIMIENTOS PARA NOTIFICACIÓN ACERCA DE REGISTRO