(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 943**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09162508 .7**

(96) Fecha de presentación: **02.05.2006**

(97) Número de publicación de la solicitud: **2099194**

(97) Fecha de publicación de la solicitud: **09.09.2009**

(54) Título: **Aparato y método para generar y transmitir un identificador de encaminamiento anónimo para mantener la privacidad de la identidad de un agente de usuario de SIP**

(45) Fecha de publicación de la mención BOPI:

02.01.2013

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

02.01.2013

(73) Titular/es:

RESEARCH IN MOTION LIMITED (100.0%)
295 Phillip Street
Waterloo, Ontario N2L 3W8 , CA

(72) Inventor/es:

BUCKLEY, ADRIAN y
ALLEN, ANDREW

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Aparatos y método para generar y transmitir un identificador de encaminamiento anónimo para mantener la privacidad de la identidad de un agente de usuario de SIP.

La presente invención se refiere generalmente a comunicaciones en un sistema de comunicación que utiliza señalización o intercambio de señales de protocolo de inicio de sesión entre agentes de usuario que van a ser partícipes en un diálogo de comunicación, Más particularmente, la presente invención se refiere a un aparato, y a un método asociado, para generar y transmitir un GRUU anónimo (URI [Identificador de Recursos Uniformes –"Uniform Resource Identifier"] de agente de usuario susceptible de ser encaminado globalmente –"Globally Routable User agent URI") u otro identificador proporcionado a un agente de usurario con vistas a un diálogo de comunicación. Al proporcionar y utilizar un identificador anónimo, la identidad del agente de usuario no se da a conocer a un tercero u otro agente.

Antecedentes de la Invención

Los avances en las tecnologías de comunicación digital han permitido el desarrollo y el despliegue de muchos tipos nuevos de dispositivos de comunicación. Los sistemas de comunicación en los que pueden hacerse funcionar los dispositivos de comunicación, hacen posible la comunicación de datos entre conjuntos de los dispositivos de comunicación. A fin de garantizar esa operatividad de un dispositivo de comunicación en un sistema de comunicación, los protocolos y requisitos operativos son en ocasiones normalizados, tal como mediante un cuerpo de establecimiento de normativa, y el funcionamiento de un dispositivo de comunicación de conformidad con la norma operativa garantiza su operatividad con otros dispositivos de comunicación que también funcionan con arreglo a la norma.

Se enumeran normalmente en tales normas protocolos de señalización, o intercambio de señales. Los protocolos de señalización se utilizan para establecer comunicaciones entre un conjunto de dispositivos de comunicación para permitir el desempeño de una sesión de comunicación subsiguiente. Un SIP (Protocolo de Inicio de Sesión – "Session Initiation Protocol") es un protocolo de señalización proporcionado a modo de ejemplo que se utiliza con vistas al establecimiento de una llamada basado en IP (Protocolo de Internet –"Internet Protocol"), y otros esquemas de comunicación de datos en paquetes. Los dispositivos de comunicación susceptibles de ser conectados a una red troncal de datos en paquetes, tal como la Internet, que utilizan SIP incluyen, por ejemplo, los denominados teléfonos de SIP. Tales dispositivos son dispositivos entre semejantes o pares, ya que son capaces de dirigir comunicaciones a través de la red de comunicación sin requerir que la red de comunicación proporcione una capacidad funcional diferente de, por ejemplo, la comunicación y el encaminamiento de datos de comunicación.

La RFC [Petición de Comentarios –"Request For Comments"] 3261, por ejemplo, establece requisitos operativos del SIP encaminados a un establecimiento y mantenimiento de un diálogo entre un conjunto de agentes de usuario. Por lo común, los mensajes generados y comunicados con vistas al diálogo entre los agentes de usuario son comunicados entre ellos utilizando una serie de saltos de representantes a través de entidades lógicas sucesivas de la red de datos. Se hace en ocasiones referencia a la serie de saltos de representantes como un conjunto de ruta. Los mensajes son suministrados a un agente de usuario subsiguientemente a los saltos sucesivos a través de la red. Los mensajes de SIP incluyen partes de cabecera que tienen diversos campos de cabecera que incluyen, por ejemplo, un campo de cabecera de contacto. La RFC 3261 requiere que los campos de cabecera de contacto de ciertos mensajes de SIP incluyan URIs (Identificadores de Recursos Uniformes –"Uniform Resource Identifiers") que son globales. Esto es lo mismo que decir que los URIs han de ser susceptibles de ser utilizados en cualquier elemento conectado a la red. La RFC 3261 también ordena que los URIs sean válidos para peticiones enviadas fuera del diálogo en el que se ha insertado el URI de contacto. Mensajes de SIP proporcionados a modo de ejemplo y que incluyen campos de cabecera de contacto poblados u ocupados con URIs, incluyen peticiones de invitación, peticiones de registro y peticiones de referencia.

Una propuesta normativa de borrador IETF (Grupo de Trabajo de Ingeniería de Internet –"Internet Engineering Task Force"), la draft-IETF-SIP-GRUU, define un tipo de URI al que se hace referencia como un URI de agente de usuario susceptible de ser encaminado globalmente (GRUU –"globally routable user agent URI"). El GRUU tiene propiedades de pertenecer al encaminamiento a un usuario (dirección o registro) situado en un agente de usuario único o exclusivo, y de ser accesible o alcanzable desde cualquier parte. Adicionalmente, en el borrador de norma se define un nuevo mecanismo en virtud del cual un agente de usuario de SIP es capaz de obtener un GRUU desde un inventario de SIP de un proveedor de SIP con vistas a un registro. Este mecanismo permite, con ello, que el URI sea utilizado en los campos de cabecera de contacto de peticiones y respuestas de formación de diálogo, al objeto de comunicar el GRUU a otros agentes de usuario de SIP. Las propiedades del GRUU pueden ser garantizadas por el proveedor. Y, como resultado de ello, otro agente de usuario de SIP es capaz de insertar el GRUU en el URI de petición de una petición de SIP tomada como objetivo en la misma AOR específica, en una instancia de agente de usuario única, a fin de hacer posibles diversas aplicaciones que requieren que la tenencia en propiedad del GRUU, incluyendo aplicaciones de transferencia y conferencia, trabaje de forma fiable.

Los esquemas y protocolos existentes, sin embargo, no consiguen proporcionar anonimato al agente de usuario. Por ejemplo, cuando se establece una llamada, es decir, un diálogo, entre un primer agente de usuario y un segundo

agente de usuario, y la llamada ha de ser transferida desde el segundo agente de usuario a un tercer agente de usuario, la identidad del GRUU del primer agente de usuario es susceptible de ser averiguada por el tercer agente de usuario.

Se requiere, por tanto, un mecanismo que haga posible la creación de un GRUU que posibilite la persistencia y proporcione una propiedad susceptible de ser encaminada globalmente pero que también proporcione anonimato.

Es a la luz de esta información de antecedentes relacionada con el intercambio de señales o señalización de SIP y con las comunicaciones que se sirven de SIP, que se ha evolucionado a mejoras significativas de la presente invención.

Breve descripción de los dibujos

La Figura 1 ilustra un diagrama de bloques funcionales de un sistema de comunicación en el que es susceptible de hacerse funcionar una realización de la presente invención.

La Figura 2 ilustra un diagrama secuencial de mensajes representativo de la señalización o intercambio de señales proporcionado a modo de ejemplo y generado durante el funcionamiento del sistema de comunicación mostrado en la Figura 1.

La Figura 3 ilustra un mensaje de petición de registro proporcionado a modo de ejemplo, generado de conformidad al funcionamiento de una realización de la presente invención.

La Figura 4 ilustra un mensaje de respuesta de registro proporcionado a modo de ejemplo y generado de conformidad con el funcionamiento de una realización de la presente invención.

La Figura 5 ilustra un mensaje de invitación proporcionado a modo de ejemplo y generado de conformidad con el funcionamiento de una realización de la presente invención.

La Figura 6 ilustra un mensaje de conformidad doscientos generado de conformidad con el funcionamiento de una realización de la presente invención.

La Figura 7 ilustra un mensaje de referencia proporcionado a modo de ejemplo y generado de conformidad con el funcionamiento de una realización de la presente invención.

La Figura 8 ilustra un diagrama de bloques funcionales de entidades utilizadas con arreglo a una realización alternativa de la presente invención.

La Figura 9 ilustra un mensaje de invitación proporcionado a modo de ejemplo y generado de acuerdo con el funcionamiento de una realización de la presente invención.

La Figura 10 ilustra una representación de otro mensaje generado con arreglo al funcionamiento de una realización de la presente invención.

Descripción detallada

De acuerdo con ello, la presente invención proporciona, ventajosamente, un aparato, y un método asociado, por los cuales comunicarse en un sistema de comunicación que utiliza la señalización o intercambio de señales de SIP (Protocolo de Inicio de Sesión –"Session Initiation Protocol") entre agentes de usuario que toman parte en un diálogo de comunicación.

Gracias al funcionamiento de una realización de la presente invención, se proporciona una manera de generar y transmitir un GRUU (URI [Identificador de Recursos Uniformes –"Uniform Resource Identifier"] de agente de usuario susceptible de ser encaminado globalmente –"Globally Routable User agent URI") u otro identificador, proporcionado a un agente de usuario de acuerdo con un diálogo de comunicación.

En un aspecto de la presente invención, mediante el uso de un identificador anónimo, la identidad de un agente de usuario no se da a conocer a un tercero, tal como una llamada u otro agente. Y, con ello, se preserva el anonimato del agente de usuario. En el caso, por ejemplo, de la transferencia de una llamada, el agente de usuario al que se transfiere una llamada no se pone al corriente de la identidad real del otro agente de usuario que constituye un participante en la llamada.

En otro aspecto de la presente invención un agente de usuario genera un mensaje de SIP que incluye un campo poblado con un valor que identifica el agente de usuario como provisto de capacidad de identificador anónimo. El campo del mensaje está poblado, por ejemplo, con una identificación de un AGRUU (URI de agente de usuario susceptible de encaminarse globalmente y anónimo). Mediante la inclusión de dicho campo y el poblamiento o llenado del campo con el indicador o valor, el menaje alerta a un destinatario de la capacidad que tiene el agente de usuario para hacerse funcionar de manera que utilice el AGRUU u otro identificador anónimo. También notifica a un inventario de SIP que se solicita un AGRUU.

El campo de cabecera del mensaje constituye, por ejemplo, un campo de cabecera de contacto que incluye la indicación de capacidad para AGRUU. El campo de cabecera de contacto forma parte de la petición de registro, de la respuesta de registro, del 200ok [conformidad doscientos], referencia y otros mensajes de SIP. Más generalmente, el valor que ocupa el campo constituye una cadena de texto que incluye uno o más caracteres alfanuméricos.

En otro aspecto de la presente invención, un dispositivo de red, tal como un inventario de SIP, recibe el mensaje generado por el agente de usuario y es capaz de actuar sobre él. El dispositivo de red detecta el valor que ocupa el

campo del mensaje, tal como la cabecera de contacto o la parte de campo “soportada” del mensaje. Y el dispositivo de red genera una respuesta de registro para entregar de vuelta al agente de usuario. Además de la información convencionalmente incluida en la respuesta de registro, el dispositivo de red incluye un campo de contacto que incluye un valor del AGRUU anónimo para el agente de usuario que ha enviado la petición de registro. El valor del AGRUU constituye, por ejemplo, una cadena textual de caracteres alfanuméricos.

La respuesta de registro, un mensaje de conformidad 200 (“200 ok”), u otro tipo de mensaje de respuesta, también incluye valores adicionales tales como valores de un RAND-ALG (algoritmo de aleatorización –“randomizer algorithm”), un BASE-ALG (algoritmo de base –“base algorithm”), una UID [identidad de usuario –“user ID”] encriptada o cifrada y, selectivamente, un valor de AOR (dirección de registro –“address of record”) cifrado.

El agente de usuario que recibe la respuesta de registro hace uso de los valores, esto es, cadenas de texto, del campo de cabecera de contacto del mensaje de respuesta de registro.

En otro aspecto de la presente invención, un agente de usuario también incluye un aparato para generar mensajes adicionales, que hace uso de los valores contenidos en el mensaje de respuesta proporcionado al agente de usuario en respuesta a un mensaje de petición de registro. Un ejemplo de tal mensaje incluye un mensaje de invitación de SIP. El mensaje de invitación de SIP incluye una cadena de campo soportado que identifica el soporte por parte del agente de usuario de un AGRUU o de otra cadena de texto que indica que se da soporte al AGRUU anónimo. Y el mensaje de invitación también incluye un campo de cabecera de contacto que incluye un campo que identifica el AGRUU del agente de usuario. El mensaje de invitación incluye de manera adicional, selectivamente, un valor de UID cifrado. El valor de UID se cifra, por ejemplo, utilizando una clave de un valor conocido por el agente de usuario. La clave está basada, por ejemplo, en el IP, el IMSI, una indicación de posición de GPS, una indicación de la hora del día, combinaciones de los mismos, así como otros valores o sus combinaciones conocidos por el agente de usuario. Están también incluidos otros campos, tales como un ALG de base y un RAND ALG que identifican claves de encriptación o cifrado que se han utilizado para generar el GRUU Anónimo.

El agente de usuario es capaz de generar otros mensajes, incluyendo, por ejemplo, un mensaje de referencia o de transferencia. Dichos otros mensajes también incluyen campos de cabecera de contacto poblados con cadenas de datos textuales análogos a los que se acaban de describir.

En general, con arreglo al funcionamiento de una realización de la presente invención, se genera un mensaje, o se recibe, con un campo al que se da soporte. A continuación de la generación de un mensaje, el mensaje es poblado u ocupado con un AGRUU u otro valor análogo, dentro de un campo al que se da soporte, a fin de identificar el soporte del AGRUU. Y se forma un campo de contacto que incluye un valor de un AGRUU o similar y, selectivamente, también un valor de UID cifrado (EUID –“encripted UID”) y ALD de Base y RAND ALG que identifican claves de cifrado que se han utilizado para generar el GRUU Anónimo. Los campos de soporte, campos de contacto, R-URI y los campos para: (to:) se proporcionan y utilizan, todos ellos, con arreglo a una realización de la presente invención y pueden contener asimismo estos parámetros.

En otro aspecto de la presente invención, se proporciona una manera que aporta el anonimato de un agente de usuario. Cuando, por ejemplo, se transfiere un diálogo entre el agente de usuario y otro partícipe, desde ese partícipe a un partícipe o tercero subsiguiente, el partícipe o tercero subsiguiente no es capaz de obtener la identidad del agente de usuario debido a su anonimato.

En estos y otros aspectos, por lo tanto, se proporciona un aparato, y un método asociado, para un dispositivo de comunicación susceptible de hacerse funcionar de conformidad con un protocolo de interfaz de sesión. El aparato facilita el uso de un identificador susceptible de ser encaminado globalmente, al tiempo que mantiene el anonimato del dispositivo de comunicación. Un generador de mensajes se ha configurado para generar un mensaje de SIP. El mensaje se puebla u ocupa con valores que indican al menos el soporte, por parte del dispositivo de comunicación, de un identificador público susceptible de encaminarse globalmente y un identificador anónimo susceptible de ser encaminado globalmente. Se proporciona también un detector de mensaje de respuesta que funciona para detectar un mensaje de respuesta generado en respuesta al mensaje generado por el generador de mensajes.

Haciendo referencia, en primer lugar, a la Figura 1, un sistema de comunicación, mostrado generalmente con la referencia 10, hace posibles comunicaciones basadas en SIP (basadas en el Protocolo de Inicio de Sesión) entre agentes de usuario, de los cuales son representativos los agentes de usuario 12, 14 y 16. En un sistema de comunicación típico, un gran número de agentes de usuario, por ejemplo, teléfonos de SIP, están conectados a un tejido o malla de comunicación, esto es, una red, que constituye en la presente memoria una red 18 de datos conmutados en paquetes. Cuando un usuario comprende una estación móvil, la red 18 es representativa, de manera adicional, de una red de acceso por radio.

La red 18 incluye una pluralidad de entidades, a las que se hace referencia en la presente memoria genéricamente como nodos 22. Los nodos son de cualquier entidad o naturaleza funcional y física, y cada uno de ellos está identificado, por lo común, por una dirección, tal como una dirección de IP (Protocolo de Internet –“Internet Protocol”). Las comunicaciones efectuadas entre un conjunto de agentes de usuario se llevan a cabo encaminando

paquetes de datos que contienen los dato a través algunos sucesivos de los nodos. Los nodos constituyen representantes, y se hace referencia, en ocasiones, a la comunicación de los datos entre representantes sucesivos constituidos por los nodos como saltos de representante. Se hace referencia en ocasiones a la colección de los saltos de representante entre los agentes de usuario como un conjunto de ruta.

De conformidad con el funcionamiento de SIP convencional, se establece un diálogo entre agentes de usuario en respuesta a la ultimación de los procedimientos de establecimiento de llamada. Los procedimientos de establecimiento de llamada incluyen el intercambio de mensajes de señalización entre dispositivos del sistema de comunicación. Un inventario 22-1 de SIP se encuentra entre las entidades funcionales de la red de datos en paquetes, que comprenden, o constituyen una parte de, un dispositivo de nodo de la red. El inventario de SIP es susceptible de hacerse funcionar, entre otras cosas, en combinación con el intercambio de mensajes de señalización que se lleva a cabo durante el establecimiento de una llamada entre un conjunto de agentes de usuario. En la representación proporcionada a modo de ejemplo en la Figura, tanto los agentes de usuario 12, 14 y 16 como el inventario 22-1 de SIP contienen aparatos de una realización de la presente invención.

El aparato 26 se ha realizado en el agente de usuario, y el aparato 28 se ha materializado en el inventario de SIP. En otras implementaciones, el aparato y las capacidades funcionales de tal aparato se han implementado en algún otro lugar del sistema de comunicación. Los elementos de los aparatos 26 y 28 también se han representado funcionalmente y son susceptibles de implementarse de cualquier forma que se desee, incluyendo programación o software ejecutado por algoritmos, dispositivos físicos o de hardware, y combinaciones de los mismos. Mediante el funcionamiento del aparato y de las metodologías que se ponen en práctica, se proporciona una privacidad mejorada de las comunicaciones. Las implementaciones convencionales, por el contrario, no consiguen garantizar el anonimato de un agente de usuario y, por tanto, de su usuario cuando, por ejemplo, una llamada, es decir, un diálogo de un agente de usuario es transferida desde una de las partes llamantes a otra parte llamante.

Los aparatos 26 y 28 son, cada uno de ellos, susceptibles de hacerse funcionar, en la implementación proporcionada a modo de ejemplo, para generar mensajes de SIP y para recibir mensajes de SIP que se han construido de maneras que facilitan el anonimato del funcionamiento del agente de usuario. El aparato 26 incluye un generador 32 de mensajes y un receptor 34 de mensajes. Otros de los agentes de usuario incluyen elementos correspondientes. Además, el aparato 28 realizado en la práctica en el inventario 22-1 de SIP incluye un generador 36 de mensajes y un receptor 38 de mensajes. Los mensajes generados por los respectivos generadores de mensajes incluyen cualquier mensaje de SIP convencional, tal como una petición de registro, una respuesta de registro, un mensaje de conformidad 200, un mensaje de invitación y un mensaje de referencia. Detalles de los formatos generales de tales mensajes se encuentran, en general, de conformidad con los protocolos existentes.

Cuando se va a establecer un diálogo, es decir, una llamada de sesión de comunicación, el agente de usuario ha de ser primeramente registrado. Para quedar registrado, el agente de usuario genera y envía un mensaje de petición de registro.

La Figura 2 ilustra un intercambio, proporcionado a modo de ejemplo, de mensajes entre el agente de usuario 12 y el inventario o registro 22-1 de SIP con vistas al registro del agente de usuario por medio de la generación, por parte del generador 32 de mensajes, de una petición de registro. En la Figura 2, la petición de registro es indicada por el segmento 44, generado aquí por el agente 26 de usuario para su entrega al inventario 22-1 de SIP. La petición de registro, como se indica por el segmento 44, incluye una AOR (dirección de registro –“address of record”), una ID de instancia y una indicación con capacidad para AGRUU (URI de agente de usuario susceptible de ser encaminado globalmente y anónimo). El receptor del mensaje del inventario de SIP detecta el mensaje transmitido, y el generador de mensajes del mismo genera una respuesta de mensaje, aquí, un mensaje de conformidad 200, indicado por el segmento 46 para su remisión al agente de usuario. El mensaje de conformidad 200, según se indica en la Figura 2, incluye un valor de AOR que es, opcionalmente, cifrado, un algoritmo de base, un valor opaco y un valor de algoritmo RAND. El algoritmo de base identifica el esquema de cifrado o encriptación utilizado para crear la EUID, y el RAND identifica el algoritmo que el UA [agente de usuario –“user agent”] de SIP deberá utilizar para aleatorizarlo adicionalmente, si estima oportuno escogerlo así.

La Figura 3 ilustra una petición de registro 44 proporcionada a modo de ejemplo. Si bien varios de los campos se formatean y pueblan con valores que son convencionales, la petición de registro incluye un campo soportado que se ocupa, conjuntamente con una indicación de que el agente de usuario da soporte adicionalmente al AGRUU. Aquí, el campo al que se da soporte incluye dicha indicación 48 de AGRUU. Es decir, cuando un agente de usuario de SIP se registra con la red, el registro es, en la implementación proporcionada a modo de ejemplo, conforme a lo que se define en la draft-IETF-SIP-GRUU-07, e incluye la indicación de que el agente de usuario desea la asignación de un GRUU, al proporcionar una ID de instancia única o exclusiva en la etiqueta de medio de soporte “sip.instance=” (“sip.instancia=”), en la parte de cabecera de contacto del mensaje, y al incluir una etiqueta de opción “GRUU” en el campo de cabecera soportado existente en la petición. Además, como se indica por el “AGRUU” 48, el agente de usuario indica que da soporte a GRUUs anónimos al incluir también la etiqueta opcional “AGRUU” en el campo de cabecera al que se da soporte. Es posible utilizar otro valor para indicar el soporte para el AGRUU.

El inventario 22-1 de SIP que da soporte a GRUUs anónimos, al recibir la petición de registro de SIP que contiene la cabecera soportada que contiene las etiquetas de opción “GRUU” y “AGRUU” u otra indicación que señala una petición de un GRUU, genera tanto un GRUU público como un GRUU anónimo. El GRUU público es de conformidad con los GRUUs definidos en el anteriormente mencionado documento draft-IETF-SIP-GRUU. Además, tanto el GRUU público como el GRUU anónimo se proporcionan en la respuesta.

La Figura 4 ilustra una representación de un mensaje 46 de conformidad 200 proporcionado a modo de ejemplo, que forma un mensaje de respuesta de registro generado por el inventario de SIP u otro dispositivo de red. El mensaje 46 se formatea generalmente de conformidad con formatos de mensaje de conformidad 200 ya existentes, e incluye un campo 56 de contacto. Aquí, el campo de contacto se puebla con un valor opaco 56, un valor 58 de AGRUU, un valor de UID cifrado (EUID) 62, un valor de algoritmo de base 64 y un valor de algoritmo RAND 66.

El GRUU anónimo 58 contiene un NAI [identificador declarado en red –“network asserted identifier”] que es anónimo, o cifrado, y un parámetro opaco que se cifra utilizando un algoritmo de cifrado tal como el algoritmo de aleatorización (RAND-ALG) 60, mostrado en la Figura 2. Cuando se descifra, el valor del parámetro opaco cifrado devuelve el valor del parámetro opaco del GRUU público correspondiente y, también selectivamente, un identificador utilizable por los dispositivos de nodo de red que emiten el GRUU para ubicar el inventario que emitió el GRUU, o como un índice para localizar el contacto almacenado asociado con el GRUU. El parámetro opaco cifrado es un URN del formato “EUID” (identificador único cifrado), tal como se indica por la referencia 62 en la Figura 4. La porción de usuario del identificador de dirección de red es también susceptible de ser cifrada o encriptada mediante la aplicación del mismo algoritmo, en lugar de, como se muestra, utilizar una cadena fija, tal como “anónimo”.

Una ruta de servicio, tal como la identificada en la RFC 3608, se devuelve también, según se indica en la Figura 4, como ruta de servicio, e incluye la dirección de un nodo. El nodo que se identifica en el campo de ruta de servicio es un nodo que es capaz de descifrar el GRUU y resolver el GRUU. A fin de que un GRUU anónimo trabaje con verificación de ID de diálogo, las peticiones con un GRUU anónimo en el contacto para el que se requiere la verificación de ID de diálogo, incluyen el URI recibido en el campo de ruta de servicio, dentro del conjunto de ruta de una petición inicial saliente, tal como un mensaje de invitación.

El algoritmo de base 64 que se devuelve en el mensaje 46 identifica el algoritmo utilizado por el inventario para generar el valor de parámetro opaco cifrado. Los detalles específicos de este algoritmo no son necesariamente comprendidos por el agente de usuario al que es enviado el mensaje. La etiqueta que se devuelve al agente de usuario se proporciona al agente de usuario con el fin de permitir que el agente de usuario incluya la etiqueta conjuntamente con el GRUU en mensajes subsiguientes, de tal manera que los nodos de dominio doméstico se pongan al corriente de qué algoritmo ha sido utilizado para encriptar o cifrar el valor opaco y, también selectivamente, cifrar las porciones de usuario del NAI. Esta inclusión permite al dominio utilizar diferentes algoritmos para cambiar de algoritmo en el caso, por ejemplo, de que un algoritmo esté comprometido.

La etiqueta 66 del algoritmo RAND que forma parte del campo de cabecera de contacto identifica un algoritmo de cifrado conocido por el agente de usuario, que puede ser utilizado por el agente de usuario adicionalmente para aleatorizar un valor opaco cifrado recibido, según criterio por llamada. Únicamente el algoritmo de cifrado con aleatorización es conocido por el agente de usuario, y el correspondiente algoritmo de desciframiento es únicamente conocido por los nodos de red en el dominio que emite el GRUU. El algoritmo de cifrado con aleatorización tiene dos parámetros de entrada, además de la semilla del valor de parámetro opaco cifrado. Estos parámetros adicionales comprenden los parámetros “RAND” e “ID de diálogo”. El “RAND” es un valor, por ejemplo, un número aleatorio que se utiliza por el agente de usuario cuando el agente de usuario hace aleatorios los parámetros opacos cifrados del GRUU. El ID de dialogo se utiliza en asociación con el “RAND” para hacer aleatorio el parámetro opaco cifrado del GRUU. El “ID de diálogo” es una entrada que se utiliza en asociación con el “RAND” para hacer aleatorio el parámetro opaco cifrado del GRUU. El “ID de diálogo” tiene una semántica específica tal, que, a menos que su valor sea cero, su valor se deduce de uno de los parámetros que identifican el diálogo de SIP con el contacto que contiene el GRUU anónimo. En una implementación, el valor es convertido en un hexadecimal de la cadena, ya sea de la ID de llamada, de la etiqueta local o de la etiqueta remota del diálogo, dependiendo de si el GRUU anónimo pertenece a un iniciador del diálogo, o por el destinatario presente en la petición que lo creó. Haciendo referencia de nuevo a la Figura 2, la etiqueta local se indica por la referencia 72, la ID de llamada se ha designado por la referencia 74, y la etiqueta remota se indica por la referencia 75.

Tanto el algoritmo de base como el algoritmo de aleatorización tienen la propiedad de preservar la unicidad o exclusividad de la cadena de entrada dentro del dominio. El algoritmo aleatorio exhibe esta propiedad incluso por medio de los parámetros de entrada “RAND” e “ID de diálogo”, puesto que tiene que haber una determinación acerca del modo como se ha de descifrar el resultado cifrado. Los algoritmos de aleatorización pueden obtenerse por el agente de usuario de cualquiera de diversas maneras. En una implementación, por ejemplo, los algoritmos son codificados en el software y descargados al agente de usuario utilizando un mecanismo de aporte de seguridad. Alternativamente, los algoritmos se incluyen como una aplicación en un UICC o tarjeta de SIM de un agente de usuario móvil u otra memoria extraíble. O bien los algoritmos son incluidos como una aplicación en un dispositivo periférico enchufado en el agente de usuario, tal como un dispositivo conectado por USB. La codificación y el almacenamiento de tales algoritmos en el agente de usuario son, preferiblemente, resistentes a la manipulación indebida y al análisis.

Si el agente de usuario incluye un contacto que contiene un GRUU anónimo en una petición que crea un diálogo, y el agente de usuario requiere que el GRUU sea válido aproximadamente durante el periodo de tiempo que existe el diálogo, entonces, en una implementación, el agente de usuario incluye la ID de llamada (x) o la etiqueta local (X) del diálogo con el GRUU anónimo, conjuntamente con un parámetro de parrilla.

Si el agente de usuario incluye un contacto que contiene un GRUU anónimo en una respuesta a una petición que crea un diálogo, y el agente de usuario requiere que el GRUU sea válido tan solo durante el periodo de tiempo durante el que existe el diálogo, entonces el agente de usuario incluye, en una implementación, la etiqueta remota del diálogo con el GRUU anónimo, conjuntamente con el parámetro de parrilla.

La etiqueta de parrilla se adecua, por ejemplo, con la definida en la anteriormente mencionada draft-IETF-SIP-GRUU. La etiqueta de parilla es un valor generado por el agente de usuario en la implementación proporcionada a modo de ejemplo, que permite a un agente de usuario asociarse al GRUU cuando se está utilizando el GRUU. Cuando se utiliza un GRUU anónimo, el valor de etiqueta de “rejilla” se ajusta en el valor utilizado para el “RAND” con el fin de hacer aleatorio o aleatorizar el GRUU.

Si el agente de usuario no requiere que el GRUU anónimo sea válido únicamente durante un periodo de tiempo durante el que el que existe el diálogo, entonces el agente de usuario tan solo incluye la etiqueta de “parrilla” en la cabecera de contacto, y el agente de usuario no incluye una ID de llamada, una etiqueta local ni una etiqueta remota. En este escenario, el valor utilizado para la ID de diálogo a la hora de la aleatorización del GRUU es cero, y no se lleva a cabo ninguna comprobación para averiguar si el GRUU anónimo se corresponde con un diálogo existente que implique al agente de usuario al que se ha asignado el GRUU descifrado.

Cuando otro agente de usuario recibe una petición, o una respuesta, con una cabecera de contacto que contiene el GRUU anónimo, el otro agente de usuario es capaz de incluir el GRUU anónimo en el URI de petición de una petición, a fin de llegar hasta el agente de usuario que incluyó el GRUU anónimo. En una implementación, esto se lleva a cabo utilizando un mecanismo análogo al definido en la anteriormente mencionada draft-IETF-SIP-GRUU-07, y no es necesario que el receptor de la petición anónima comprenda la extensión del GRUU anónimo.

Un agente de usuario que envía una petición que contiene un GRUU anónimo en el campo de cabecera de contacto, incluye en la petición una cabecera de ruta que contiene el URI que es devuelto en la cabecera de ruta de servicio del mensaje de confirmación 200 (“200 ok”) enviado en respuesta a una petición de registro. El URI es un representante que, cuando recibe la petición y constata que hay un GRUU anónimo en el contacto que contiene un parámetro “ID de llamada” o “etiqueta local”, se incluye una cabecera de ruta de registro en la petición remitida, a fin de asegurarse de que esta se encuentra en la ruta de la totalidad de las peticiones subsiguientes para ese diálogo, al objeto de que sea capaz de verificar que existe el diálogo si el GRUU es utilizado en el URI de petición por parte de otro agente de usuario.

Si se da soporte a los GRUUs anónimos por medio de un dominio, entonces todas las peticiones entrantes han de ser encaminadas en registro también por un representante, por la razón de que, de la misma manera, una petición que contiene un GRUU anónimo con una “etiqueta remota” en el URI de petición puede ser verificado por lo que respecta al estado del diálogo.

Cuando una petición que contiene un GRUU anónimo, identificado por la etiqueta “AGRUU” u otra etiqueta, es recibido por un representante situado en el dominio que posee el GRUU, mostrado en las figuras como ejemplo.com, el representante utiliza la etiqueta “RAND-ALG” para identificar el algoritmo de aleatorización utilizado por el agente de usuario para hacer aleatorio el GRUU y, a continuación, aplicar el algoritmo al valor del parámetro opaco. Se utilizan valores con origen en la etiqueta “parrilla” y, caso de estar presente, el “ID de llamada” o “etiqueta remota”, o bien “etiqueta local”, con el GRUU anónimo. Si únicamente está presente la etiqueta “parrilla”, entonces se utiliza un valor de 0 para el parámetro de ID de diálogo del algoritmo. Una que se ha obtenido el resultado, el resultado se proporciona a un algoritmo identificado por “BASE-ALG” [algoritmo de base], a fin de devolver el valor del parámetro opaco del GRUU público correspondiente y también, ya sea el identificador para localizar el inventario que emitió el GRUU, ya sea el índice para ubicar el contacto almacenado asociado con el GRUU. Dependiendo de lo que se devuelva, el representante remite la petición al representante que actúa como el inventario que ha emitido el GRUU o algún otro representante que pueda coincidir con el contacto. El representante, en una implementación, a la hora de remitir la petición, utiliza el parámetro opaco de GRUU público descifrado con el fin de evitar un desciframiento adicional por parte del segundo representante.

Si una “ID de llamada” (74), una “etiqueta remota” (75) o una “etiqueta local” (72) está incluida en el GRUU anónimo, la petición es encaminada por medio de un dispositivo de nodo de red que tiene un estado de diálogo para el parámetro de diálogo que está incluido en la petición. El dispositivo de red comprende un representante que encamina en registro la petición original que contiene el GRUU anónimo en el campo de cabecera de contacto. El representante formado por el dispositivo de red comprueba que sigue existiendo el diálogo y seguidamente lo encamina al contacto registrado del agente de usuario utilizando procedimientos establecidos en la anteriormente mencionada draft-IETF-SIP-GRUU-07.

En un aspecto adicional de la presente invención, la parte de usuario del NA1 del GRUU anónimo es cifrado y aleatorizado adicionalmente. Cuando está cifrado y aleatorizado, el desciframiento permite a los representantes resolver el NA1 del GRUU anónimo en el NA1 del GRUU público. El manejo del representante se ve simplificado puesto que un representante no necesita almacenar ni consultar el NA1 del GRUU público basándose en un valor de parámetro opaco.

La Figura 5 ilustra una representación de un mensaje de petición de invitación proporcionado a modo de ejemplo y generado por un generador de mensajes de un agente de usuario, tal como el generador 32 de mensajes del agente 12 de usuario que se muestra en la Figura 1. El mensaje de invitación 76 se formatea también, en general, de conformidad con los protocolos de formateo de mensaje de SIP y, aquí, también incluye un campo al que se da soporte. El campo soportado incluye una etiqueta 78 de AGRUU u otra etiqueta que indique que se da soporte al GRUU anónimo. Asimismo, el mensaje de invitación incluye un campo de contacto que incluye el AGRUU 82, un valor opaco 84, un valor de parrilla 86, un valor de etiqueta local 88, un valor de algoritmo de base 92 y un algoritmo de aleatorización 94.

También, la Figura 6 ilustra una representación de otra respuesta de conformidad 200, de nuevo también formateada, en general, de conformidad con los protocolos de formateo de SIP. Nuevamente, el campo soportado incluye una etiqueta 102 de AGRUU. También, el mensaje de conformidad 200 incluye, de manera adicional, un campo de cabecera de contacto que incluye un valor opaco 104, un valor de EUID 106, un valor de parrilla 108, una etiqueta remota 112, un algoritmo de base 114 y un algoritmo de aleatorización 116.

La Figura 7 ilustra una representación de un mensaje de referencia también generado de acuerdo con el funcionamiento de una realización de la presente invención. De nuevo, el mensaje de referencia se ha construido de conformidad general con los protocolos y formatos de funcionamiento convencionalmente utilizados en la generación y la señalización de mensajes de SIP.

Aquí, de nuevo, el mensaje incluye un campo de cabecera de contacto que incluye un valor opaco 124, un valor de EUID 126, un valor de parrilla 128, un valor de etiqueta local 132, un valor de algoritmo de base 134 y un algoritmo de aleatorización 136.

Un repaso del mensaje de referencia muestra que, para el agente de usuario al que se transfiere una llamada, la identidad del otro agente de usuario es anónima. Se aporta, por lo tanto, la privacidad de las comunicaciones a través de la generación y la recepción de mensajes y de la metodología de funcionamiento de una realización de la presente invención.

La Figura 8 ilustra un agente 12 de usuario, que consiste aquí en un dispositivo inalámbrico, y un inventario 22-1 de SIP de una realización alternativa de la presente invención. El dispositivo inalámbrico puede también ser un dispositivo fijo que contenga un UA de SIP. Aquí, el agente de usuario funciona sin la asignación, por parte del inventario de SIP, de un GRUU anónimo. Aquí, en lugar de ello, el agente de usuario, a continuación de una petición de registro, sencillamente solicita la asignación de un GRUU. Y se proporciona un GRUU por parte del inventario, al agente de usuario.

Subsiguientemente, a la hora de iniciar una nueva sesión de SIP, se habrá hecho una determinación de que la identidad del usuario debe ser restringida y no proporcionarse a otro tercero, un tercero B. En el caso de que se haya construido dicha terminación, entonces el GRUU que se envía es único para el diálogo particular. Y el GRUU ha de ser anónimo para la parte llamante.

El GRUU público, aquí indicado por la referencia 142, y disponible en el agente 112 de usuario, se toma y se cifra con una clave 144 que es conocida por el agente de usuario y por el inventario 22-1. Cuando el agente de usuario forma un dispositivo de GSM / UMTS, la clave ser forma, por ejemplo, con una de las claves de AKA disponibles en el dispositivo. Además, se utiliza también un testigo de diálogo 146 para cifrar o encriptar el GRUU 142, de manera que el valor resultante, cifrado, sea válido únicamente para ese diálogo de SIP particular. El testigo constituye, por ejemplo, una ID de llamada, una etiqueta remota o una etiqueta local. Las operaciones llevadas a cabo sobre el GRUU son realizadas por un dispositivo de aporte de anonimato 148. Y, de esta forma, el valor utilizado para aleatorizar el GRUU es conocido únicamente en el agente de usuario.

Subsiguientemente al cifrado del GRUU público, se anexa una ID 152 de inventario ya sea a la parte de nombre de usuario del NAI, ya sea a la parte de dominio del NAI. El NAI resultante, un nuevo NAI, se utiliza entonces como el GRUU. Y se construye el GRUU dentro de la cabecera de contacto.

La Figura 9 ilustra un mensaje de invitación proporcionado a modo de ejemplo, representado generalmente por la referencia 156, que incluye un campo 158 de cabecera de contacto, poblado u ocupado con un valor 162, del que se indica que es un GRUU anónimo. En una implementación, el GRUU anónimo es una ID de GRUU que es reetiquetado como AGRUU, por GRUU anónimo.

En otras implementaciones, se utilizan otras variantes del valor del campo de cabecera de contacto. Por ejemplo, se utilizan home1.net@hfdshguesr98gn!scscfl.home.net, hfdshguesr98@gnscscfl.homel.net, o diversas versiones cifradas de tales valores, donde hfdshguesr98gn es la AOR cifrada, que únicamente conocida en el inventario de SIP y en el UA de SIP.

Subsiguientemente al envío y la recepción en el inventario de SIP del mensaje de invitación de SIP, el inventario examina el mensaje de SIP y detecta que la cabecera de contacto identifica el uso de un GRUU anónimo. El inventario utiliza la clave 144 que ha sido almacenada frente al agente de usuario de SIP y el testigo de diálogo 146 para descifrar el GRUU. Se crea entonces en su registro una asociación, tal como hfdshguesr98=user1_public1. Y, seguidamente, se remite el mensaje de invitación de SIP.

Adicionalmente, al recibirse el mensaje de SIP, el inventario 22-1 examina el mensaje de SIP. El inventario detecta, a partir el URI solicitado, perteneciente al mensaje, que se trata de un GRUU anónimo. Y, a continuación, el inventario toma la parte de nombre de usuario que se ha obtenido del r-URI y ubica la AOR correcta en la identificación de instancia.

LAF Figura 10 ilustra una representación, mostrada generalmente con la referencia 168, que es representativa del i-CSCF que recibe un mensaje de SIP con el URI solicitado, en cualquiera de los siguientes formatos:

< sip:hfdshguesr98gn.scscf1.home1.net@home1.net; gruu;agruu;
opaque=urn:euid: 5d47d1e1e1d410eda038faf6ba76c90f; grid=99a>
< sip: home1.net@ hfdshguesr98gn!scscf1.home1; gruu;agruu;
opaque=um:euid: 5d47d1e1e1d410eda038faf6ba76c90f; grid=99a>
< sip: hfdshguesr98gn@scsf1.home.net; gruu;agruu;
opaque=um:euid:
5d47d1e1e1d410eda038faf6ba76c90f; grid=99a>

Los valores identifican que se está utilizando un GRUU anónimo. A continuación, se examina la cabecera de contacto. Aquí, se examina la parte de nombre de usuario y se extrae la ID de inventario. En lugar de llevar a cabo una inmersión en HSS para encontrar el inventario asociado con el GRUU, la I-CSCF envía el mensaje de SIP directamente al inventario mediante la correlación de la ID de inventario con el inventario. Con ello, de nuevo, se mantiene el anonimato del agente de usuario. Y se garantiza mejor la privacidad de las comunicaciones.

Se ha proporcionado un aparato para un agente de usuario, susceptible de hacerse funcionar de acuerdo con un Protocolo de Inicio de Sesión, SIP, de tal modo que dicho aparato está destinado a facilitar el uso de un identificador susceptible de ser encaminado globalmente, al tiempo que se mantiene el anonimato del agente de usuario, comprendiendo dicho aparato: un solicitador configurado para generar una petición de registro, de tal modo que la petición se puebla o llena con valores que indican la petición de un identificador susceptible de ser encaminado globalmente y público, y de un identificador susceptible de ser encaminado globalmente y anónimo, y un detector de respuesta, configurado para detectar una respuesta retornada al agente de usuario en respuesta a la petición generada por dicho solicitador.

La petición generada por dicho solicitador puede comprender una petición de Registro de SIP, que contiene una parte de cabecera. La parte de cabecera de la petición de Registro de SIP generada por dicho solicitador puede comprender una etiqueta de opción que identifica o indica la petición de un URI, identificador de recursos uniformes, de agente de usuario susceptible de ser encaminado globalmente y público. Alternativamente, la parte de cabecera de la petición de Registro de SIP generada por dicho solicitador puede comprender una etiqueta de opción que identifica la petición de un URI, identificador de recursos uniformes, de agente de usuario susceptible de ser encaminado globalmente y anónimo.

El aparato puede comprender, de manera adicional, un generador de valor de identificación de diálogo, de tal modo que dicho generador de valor de identificación de diálogo está configurado para generar un valor de identificación de diálogo que se utiliza por parte del agente de usuario con vistas a una operación de aleatorización.

El agente de usuario puede comprender un dispositivo inalámbrico, de tal manera que la petición es comunicada a través de una interfaz aérea por radio.

Se ha proporcionado también un aparato para un inventario de Protocolo de Inicio de Sesión, SIP, de tal manera que dicho aparato está destinado a actuar sobre una petición de registro referida a un identificador susceptible de ser encaminado globalmente, comprendiendo dicho aparato: un detector, configurado para recibir una indicación de la petición de registro, de tal modo que dicho receptor está configurado para detectar si la petición incluye la petición de una operación anónima, un dispositivo de asignación de identificador susceptible de ser encaminado globalmente, susceptible de hacerse funcionar en respuesta a la petición detectada por dicho detector, de tal manera que dicho dispositivo de asignación de identificador susceptible de ser encaminado globalmente se ha configurado para asignar un identificador susceptible de ser encaminado globalmente y anónimo.

El identificador susceptible de ser encaminado globalmente y anónimo asignado por dicho dispositivo de asignación de identificador susceptible de ser encaminado globalmente, puede comprender un identificador de recursos uniformes, URI, de agente de usuario susceptible de ser encaminado globalmente y anónimo. El URI de agente de usuario susceptible de ser encaminado globalmente y anónimo puede comprender un identificador declarado en red, NAI ["network asserted identifier"], anónimo. El URI de agente de usuario susceptible de ser encaminado globalmente y anónimo puede comprender un identificador declarado en red, NAI, cifrado. El URI de agente de usuario susceptible de ser encaminado globalmente y anónimo puede comprender un parámetro opaco cifrado.

El aparato puede comprender, de manera adicional, un generador de etiqueta de identidad de algoritmo de base, configurado para generar una etiqueta de identidad de algoritmo de base que identifica un tipo de algoritmo que se utiliza para formar el parámetro opaco cifrado.

El aparato puede comprender, de manera adicional, un generador de etiqueta de identidad de algoritmo aleatorio, configurado para generar una etiqueta de identidad de algoritmo aleatorio que identifica un tipo de algoritmo disponible para su uso a la hora de aleatorizar adicionalmente el parámetro opaco cifrado.

Al menos parte del identificador susceptible de ser encaminado globalmente y anónimo puede ser encriptado o cifrado, y el aparato puede comprender, adicionalmente, un identificador de ruta de servicio configurado para proporcionar una dirección que identifica una posición nodal capaz de descifrar la parte del identificador susceptible de ser encaminado globalmente y anónimo que está cifrada.

Se ha proporcionado también un método para facilitar el uso de un identificador susceptible de ser encaminado globalmente y que se utiliza con vistas a las comunicaciones de un agente de usuario de Protocolo de Inicio de Sesión, SIP, al tiempo que se mantiene el anonimato del agente de usuario, de tal manera que dicho método comprende las operaciones de: generar, en el agente de usuario, una petición poblada u ocupada con un valor que indica la petición de un identificador susceptible de ser encaminado globalmente y de un identificador susceptible de ser encaminado globalmente y anónimo; y detectar una respuesta retornada al agente de usuario en respuesta a la petición generada durante dicha operación de generación.

El método puede comprender, adicionalmente, las operaciones, en el inventario de SIP, de: detectar la petición generada durante dicha operación de generación y, una vez detectada, si la petición incluye el identificador susceptible de ser encaminado globalmente y anónimo; asignar un identificador susceptible de ser encaminado globalmente y anónimo para identificar el agente de usuario; y enviar el identificador susceptible de ser encaminado globalmente y anónimo al agente de usuario.

El método puede comprender, de manera adicional, la operación de encriptar o cifrar una porción del identificador susceptible de ser encaminado globalmente y anónimo, asignado durante dicha operación de asignación. El método puede comprender, de manera adicional, la operación de descifrar la porción del identificador susceptible de ser encaminado globalmente y anónimo, cifrado subsiguientemente a dicha operación de envío.

Se ha proporcionado también un aparato para un agente de usuario, que comprende: un detector de GRUU público, configurado para detectar la entrega al usuario del GRUU público; un dispositivo de aporte de anonimato, concebido para recibir el GRUU público detectado por dicho detector, de tal modo que dicho dispositivo de aporte de anonimato está configurado para alterar los valores del GRUU público. El dispositivo de aporte de anonimato puede haberse dispuesto para alterar los valores del GRUU público utilizando un valor conocido en el agente de usuario.

Se ha proporcionado también un aparato para un sistema de comunicación de Protocolo de Inicio de Sesión, SIP, de tal modo que dicho aparato facilita el uso de un identificador susceptible de ser encaminado globalmente, al tiempo que preserva el anonimato de su identidad, de manera que dicho aparato comprende: un primer detector de mensaje, configurado para recibir un primer mensaje que indica una capacidad de funcionamiento anónimo del nodo de envío; y un segundo generador de mensaje, susceptible de hacerse funcionar en respuesta a la detección del primer mensaje por dicho primer detector de mensaje, de tal manera que dicho segundo generador de mensaje está configurado para generar un segundo mensaje, incluyendo el segundo mensaje un identificador susceptible de ser encaminado globalmente y anónimo, que proporciona la capacidad del nodo de envío que preserva el anonimato de la identidad.

Las descripciones anteriores lo son de ejemplos preferidos para implementar la invención, y el ámbito de la invención no ha de estar necesariamente limitado por esta descripción. El ámbito de la presente invención se define por las siguientes reivindicaciones.

REIVINDICACIONES

1.- Un método para facilitar una comunicación de Protocolo de Inicio de Sesión (SIP) por un agente (12) de usuario, al tiempo que mantiene el anonimato del agente (12) de usuario, de tal manera que dicho método comprende:

enviar una petición de registro que comprende un campo de cabecera de soporte poblado u ocupado con un valor que indica una petición de un identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y público, y de un identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo; y

recibir una respuesta (46) que comprende el identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y público, y un único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo (58).

2.- El método de acuerdo con la reivindicación 1, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo (58) está incluido dentro de un campo de cabecera de contacto de dicha respuesta (46).

3.- El método de acuerdo con la reivindicación 1 o la reivindicación 2, que comprende adicionalmente identificar el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo (58).

4.- El método de acuerdo con una de las reivindicaciones 1-3, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo es identificado por una cadena de texto de caracteres alfanuméricos.

5.- El método de acuerdo con la reivindicación 1, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo contiene un Identificador de Dirección de Red, “NAI”.

6.- El método de acuerdo con una de las reivindicaciones 1-5, que comprende, de manera adicional, generar un mensaje de SIP que comprende un único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo, recibido.

7.- El método de acuerdo con la reivindicación 6, en el cual el mensaje de SIP comprende un mensaje de petición de invitación de SIP.

8.- El método de acuerdo con la reivindicación 6, en el cual el mensaje de SIP comprende un mensaje de referencia de SIP.

9.- El método de acuerdo con la reivindicación 6, en el cual el mensaje de SIP comprende un mensaje de respuesta de registro de SIP.

10.- El método de acuerdo con una de las reivindicaciones 6-9, en el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo, recibido, se incluye en un campo de cabecera de contacto de dicho mensaje de SIP.

11.- El método de acuerdo con cualquiera de las reivindicaciones 1-5, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo comprende una parte de nombre de usuario y una parte de dominio.

12.- El método de acuerdo con la reivindicación 11, en el cual al menos parte del identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo es encriptada o cifrada.

13.- El método de acuerdo con una cualquiera de las reivindicaciones 1-5, en el cual la petición de registro es una petición de Registro de SIP y la respuesta es una respuesta de Registro de SIP.

14.- El método de acuerdo con una cualquiera de las reivindicaciones 11-13, en el cual la parte de nombre de usuario del único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo, es cifrada.

15.- Un método para que un Inventario de Protocolo de Inicio de Sesión (SIP) facilite la comunicación de SIP por parte de un agente (12) de usuario, al tiempo que se mantiene el anonimato del agente (12) de usuario, de tal manera que el método comprende:

recibir una petición de registro que comprende un campo de cabecera al que se da soporte y que es poblado u ocupado con un valor que indica una petición de un identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y público, y de un identificador de recursos uniformes de

agente de usuario susceptible de ser encaminado globalmente y anónimo; y
enviar una respuesta (46) que comprende el identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y público, y un único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo (58).

16.- El método de acuerdo con la reivindicación 15, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo (58) está incluido dentro de un campo de cabecera de contacto de dicha respuesta (46).

17.- El método de acuerdo con una de las reivindicaciones 15-16, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo es identificado por una cadena de texto de caracteres alfanuméricos.

18.- El método de acuerdo con la reivindicación 15, en el cual el único identificador de recursos uniformes de agente de usuario susceptible de ser encaminado globalmente y anónimo contiene un Identificador de Dirección de Red, “NAI”.

19.- Un aparato de agente de usuario configurado para implementar el método de acuerdo con una cualquiera de las reivindicaciones 1-18.

20.- El aparato de agente de usuario de acuerdo con la reivindicación 19, de tal manera que el aparato de agente de usuario comprende un dispositivo inalámbrico, y de modo que la petición y la respuesta de registro son comunicadas a través de una interfaz aérea por radio.

21.- Un nodo de red que comprende un Inventario de Protocolo de Inicio de Sesión (SIP), de tal manera que el nodo de red está configurado para implementar el método de acuerdo con una cualquiera de las reivindicaciones 15-18.

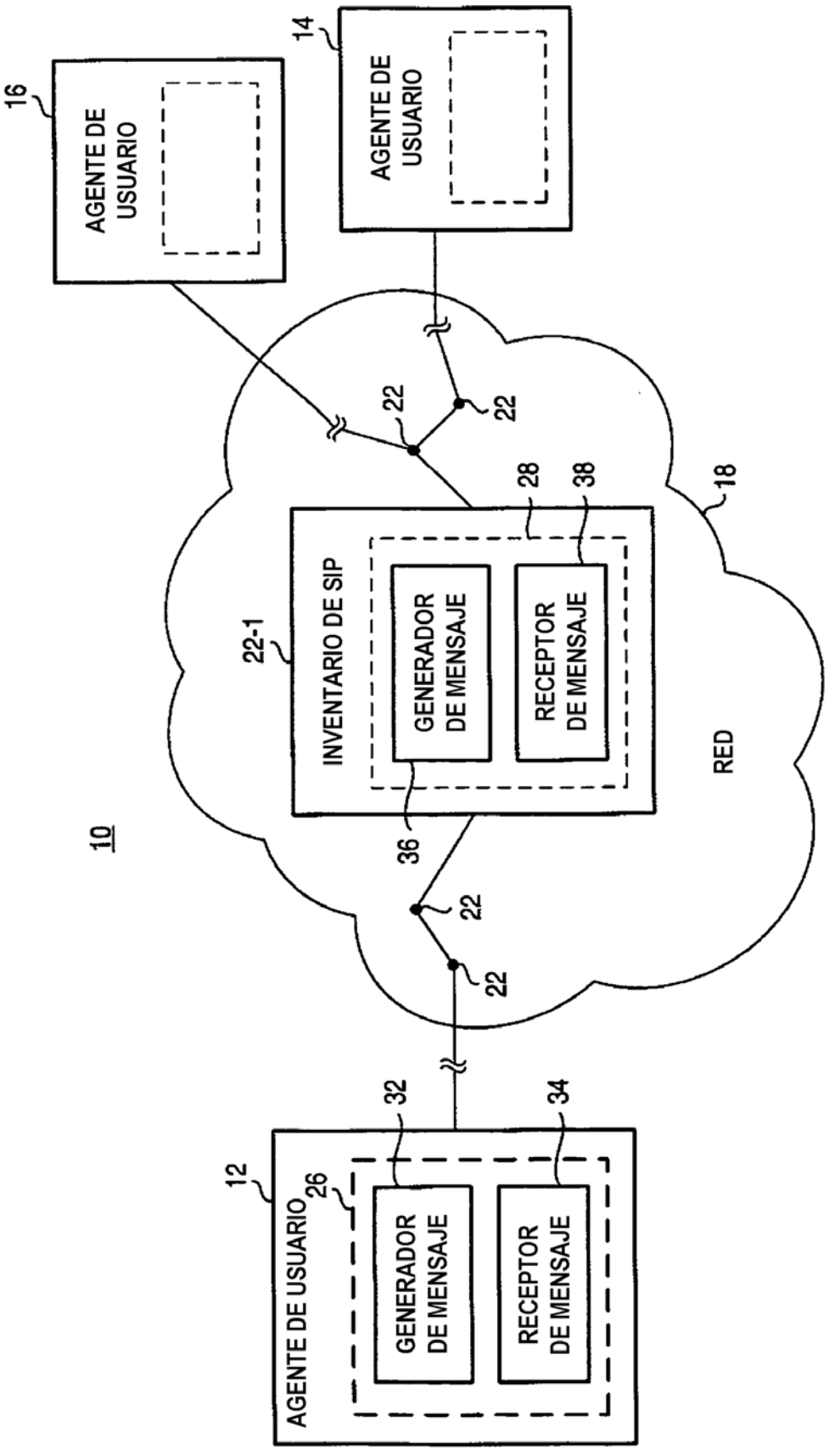
10
16
AGENTE DE USUARIO
14
AGENTE DE USUARIO
22
22
22
22
22
18
RED
22-1
INVENTARIO DE SIP
28
GENERADOR DE MENSAJE
38
RECEPTOR DE MENSAJE
36
12
AGENTE DE USUARIO
26
32
GENERADOR DE MENSAJE
34
RECEPTOR DE MENSAJE

FIG. 1

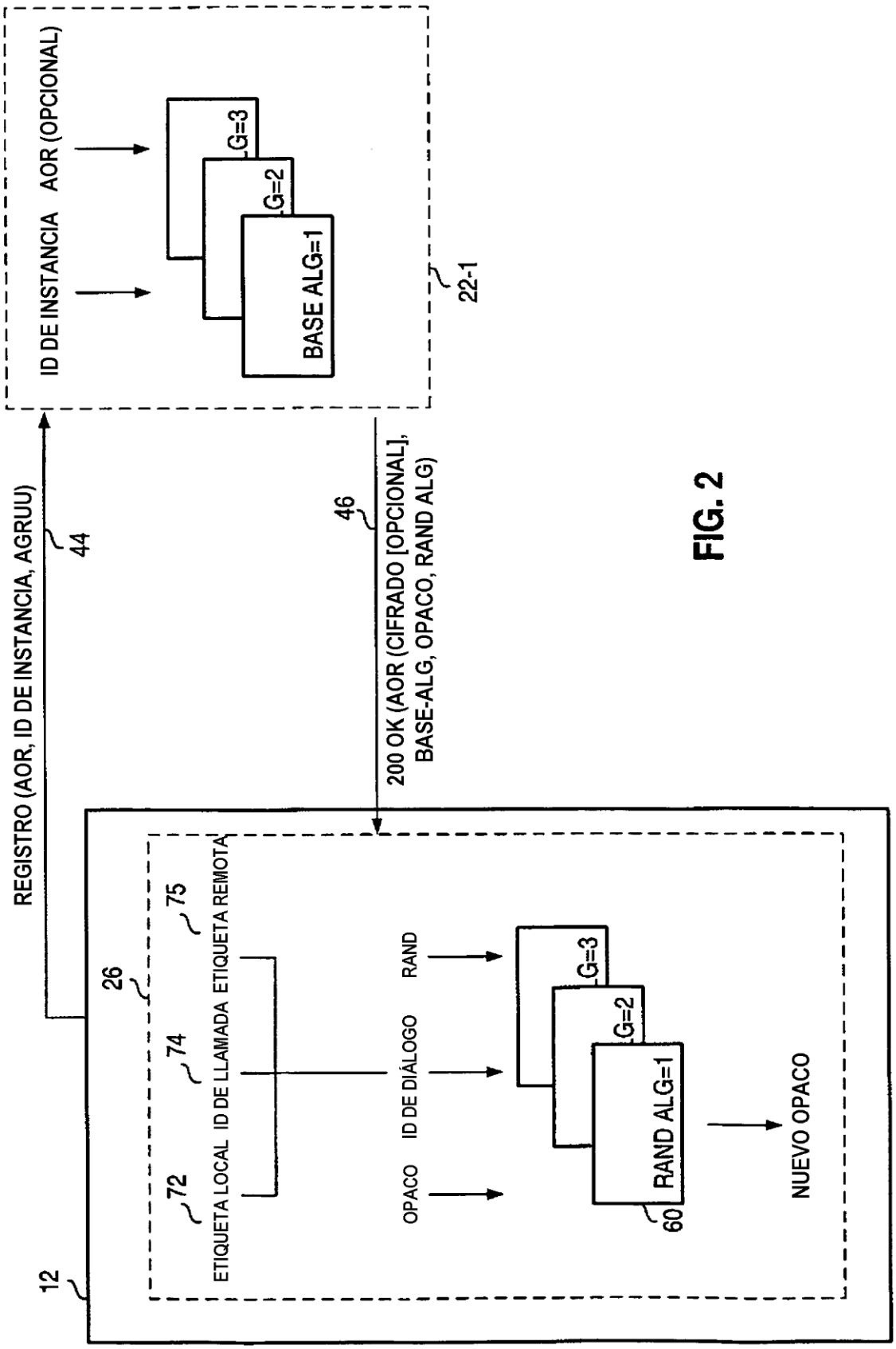
ID DE INSTANCIA
AOR (OPCIONAL)
G=3
G=2
BASE ALG=1
22-1
REGISTRO (AOR, ID DE INSTANCIA, AGRUU)
44
46
200 OK (AOR (CIFRADO [OPCIONAL], BASE-ALG, OPACO, RAND ALG)
12
26
75
ETIQUETA REMOTA
74
ID DE LLAMADA
72
ETIQUETA LOCAL
RAND
ID DE DIÁLOGO
OPACO
G=3
G=2
RAND ALG=1
60
NUEVO OPACO

FIG. 2

44

```
REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1;branch=z9hG4bKnashds7
Max-Forwards: 70
From: Callee <sip:callee@example.com>;tag=a73kszlfl
Supported: gruu, agruu                                  48
To: Callee <sip:callee@example.com>
Call-ID: 1j9FpLxk3uxtm8tn@192.0.2.1
CSeq: 1 REGISTER
Contact: <sip:callee@192.0.2.1>
;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
Content-Length: 0
```

FIG. 3

46

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.2.1;branch=z9hG4bKnashds7
From: Callee <sip:callee@example.com>;tag=a73kszlfl
To: Callee <sip:callee@example.com> ;tag=b88sn
Call-ID: 1j9FpLxk3uxtm8tn@192.0.2.1
CSeq: 1 REGISTER
Service-Route: <sip:s-cscf1.example.com;lr>
<allOneLine>
54  Contact: <sip:callee@192.0.2.1>
    ;gruu="sip:callee@example.com;gruu;
56  opaque=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
58  ;agruu="sip:anonymous@example.com;agruu;
    opaque=urn:euid:5d47d1e1e1d410eda038faf6ba76c90f7d15ef80e7014ea2316
64  base-alg=11;rand-alg=2;"                    62
    ;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
                                                66
    ;expires=3600
    </allOneLine>
    Content-Length: 0
```

FIG. 4

76

```
INVITE  .sip:callee.example.com SIP/2.0
From: Anonymous <sip:anonymous@example.com>;tag=n88ah
To: Callee <sip:callee@example.com>
Route: <sip: s-cscf1.example.com;lr>
Max-Forwards: 70
Call-ID: 1j9FpLxk3uxtma7@host.example.com
CSeq: 1 INVITE
Supported: gruu; agruu ~78
Allow: INVITE, OPTIONS, CANCEL, BYE, ACK
<allOneLine>
Contact:
<sip:anonymous@example.com;gruu;agruu ~82
84 ~ ;opaque=
urn:euid:5d47d1e1e1d410eda038faf6ba76c90f7d15ef80e7014ea2316;
86 ~ grid=99a;local-tag= n88ah;base-alg=11;rand-alg=2>
</allOneLine>      88      92      94
Content-Length: --
Content-Type: application/sdp
```

FIG. 5

98

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP proxy.example.com;branch=z9hG4bKnaa8
Via: SIP/2.0/UDP host.example.com;branch=z9hG4bK99a
From: Anonymous <sip:anonymous@example.com>;tag=n88ah
To: Callee <sip:callee@example.com> ;tag=a0z8
Call-ID: 1j9FpLxk3uxtma7@host.example.com
CSeq: 1 INVITE
Supported: gruu; agruu ~102
Allow: INVITE, OPTIONS, CANCEL, BYE, ACK
<allOneLine>
Contact:
<sip:anonymous@example.com;gruu;agruu
104 ~ ;opaque=          ~106
urn:euid:5d47d1e1e1d410eda038faf6ba76c90f7d15ef80e7014ea2316;
108 ~ grid=99a;remote-tag= a0z8;base-alg=11;rand-alg=2>
</allOneLine>      112      114      116
Content-Length: --
Content-Type: application/sdp
```

FIG. 6

122

```
  <allOneLine>
  REFER  . sip:anonymous@example.com;gruu;agruu
  ;opaque= urn:euid:
eda038faf6ba765d47d1e1e1d410c90f7d15ef80e7014ea2316;
grid=36a789a;remote-tag= a0z8;base-alg=11;rand-alg=2 SIP/2.0
  </allOneLine>
  From: Anonymous <sip:anonymous@example.com>;tag=a56781
  To: Anonymous <sip:anonymous@example.com>
  Max-Forwards: 70
  Call-ID: 1j9FpLxk3uxtma7@host.example.com
  CSeq: 2 REFER
  Supported: gruu
  Allow: INVITE, OPTIONS, CANCEL, BYE, ACK
  <allOneLine>
  Refer-To: <sip:anonymous@example.com;gruu;agruu
  ;opaque= urn:euid:5d47d1e1e1ef80e701038faf6ba76c90f7d 4ea2316;
 grid=99a;local-tag= n88ah;base-alg=11;rand-alg=2>
  Contact:
  <sip:anonymous@example.com;gruu;agruu
  ;opaque=
urn:euid:50e7014ea2347d1e1e1d410eda038faf6ba76c90f7d15ef816;
grid=9389b;local-tag= a56781;base-alg=11;rand-alg=2>
  </allOneLine>
  Content-Length: 0
```

124 126 128 132 134 136

FIG. 7

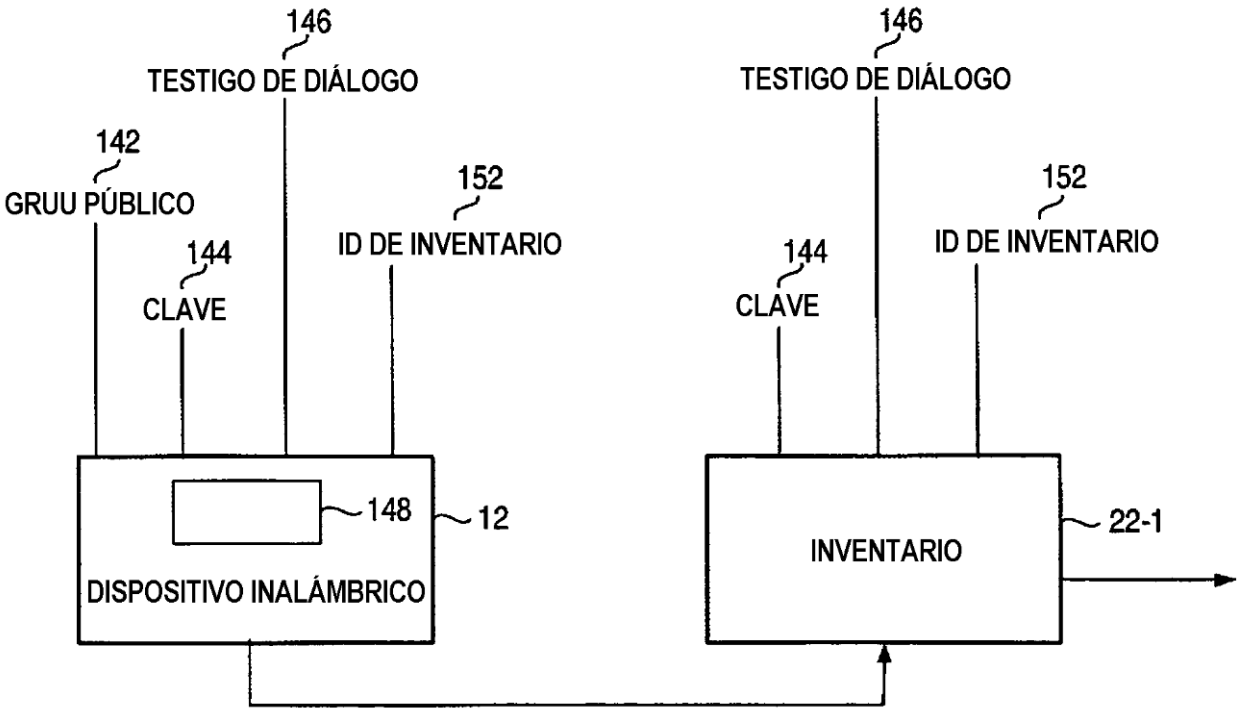
146
TESTIGO DE DIÁLOGO
142
GRUU PÚBLICO
144
CLAVE
152
ID DE INVENTARIO
148
12
DISPOSITIVO INALÁMBRICO
146
TESTIGO DE DIÁLOGO
144
CLAVE
152
ID DE INVENTARIO
INVENTARIO
22-1

FIG. 8

```
INVITE tel:+1-212-555-3333 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd] :1357; comp=sigcomp;
branch=z9hG4bKnashds7
Max-Forwards: 70
Route: sip:pcscf1.home1.net:7531; lr; comp=sigcomp>,
<sip:orig@scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: Critical
From: <anonymous>; tag=171828
To: <tel:+1-212-555-3333>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Supported: 100rel; precondition; agruu
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi=87654321;
port1=7531
Contact: < sip:hfdshguesr98gn.scscf1.home1.net@home.net;gruu; agruu;
opaque=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6; grid=99a;base-
alg=11;rand-alg=2>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
Content-Type: application/sdp
Content-Length:  (...)

v=0
o=- 2987933615  2987933615  IN  IP6  5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=rtpmap:96 telephone=event
a=maxptime:20
```

156

158

162

FIG. 9

168

```
INVITE sip:hfdshgesr98gn.scscf1.home1.net@home1.net; gruu; agruu;
opaque=urn:euid:
5d47d1e1e1d410eda038faf6ba76c90f; grid=99a:base-alg=11;rand-alg=2 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd] :1357; comp=sigcomp;
branch=z9hG4bKnashds7
Max-Forwards: 70
Route:  sip:pcscf1.home2.net:7531; lr; comp=sigcomp>,
<sip:orig@scscf1.home2.net;lr>
P-Asserted-Identity: "Andrew Allen" <sip:user1_public1@home2.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home2.net>; tag=171828
To: <tel:+1-212-555-3333>
Call-ID: cb93a0s09a9sdfg9kj490456
Cseq: 127 INVITE
Supported: 100rel; precondition; gruu; agruu
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi=87654321;
port1=7531
Contact: <tel:+1-212-555-3333>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
Content-Type: application/sdp
Content-Length:  (…)

v=0
o=- 2987933615  2987933615  IN  IP6  5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=rtpmap:96 telephone=event
a=maxptime:20
```

FIG. 10