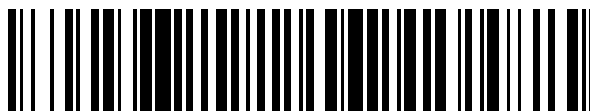


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 701 433**

51 Int. Cl.:

H04W 12/02 (2009.01)

H04L 29/12 (2006.01)

H04L 29/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **07.07.2009 PCT/IB2009/006188**

87 Fecha y número de publicación internacional: **14.01.2010 WO10004411**

96 Fecha de presentación y número de la solicitud europea: **07.07.2009 E 09785994 (6)**

97 Fecha y número de publicación de la concesión europea: **12.09.2018 EP 2311242**

54 Título: **Método y aparato para el identificador de instancia basado en un único identificador de dispositivos**

30 Prioridad:

09.07.2008 US 79293

16.09.2008 US 211607

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

22.02.2019

73 Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
(100.0%)
164 83 Stockholm, SE**

72 Inventor/es:

**SCHNEYER, SEAN, KENDALL;
LINDHOLM, FREDRIK y
HEIDERMARK, ALF**

74 Agente/Representante:

LINAGE GONZÁLEZ, Rafael

ES 2 701 433 T3

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

DESCRIPCIÓN

Método y aparato para el identificador de instancia basado en un único identificador de dispositivos

5 La presente invención se refiere a sistemas de comunicación y datos basados en SIP. Las abreviaturas usadas en el presente documento tendrán los siguientes significados:

- CS: Conmutación de circuitos
- CSCF: Función de control de sesión de llamada
- DevID: Identificador de dispositivo
- ESN: Número de serie electrónico
- GRUU: URI de agente de usuario (UA) enrutable globalmente
- HSS: Servidor local de abonado
- I-CSCF: CSCF de interrogación
- ICS: Servicios centralizados IMS
- ID: Identificador
- IMEI: Identidad internacional de equipos móviles
- IMS: Subsistema multimedia IP
- IP: Protocolo de Internet
- MEID: Identificador de equipo móvil
- MSC: Centro de conmutación móvil
- NAI: Identificador de acceso a la red
- P-CSCF: Proxy CSCF
- PS: Conmutación de paquetes
- S-CSCF: CSCF de servicio
- SCC AS: Servidor de aplicaciones de continuidad y centralización de servicios
- SIP: Protocolo de inicio de sesión
- SNR: Número de serie
- TAC: Código de asignación de tipo
- UA: Agente de usuario
- UE: Equipo de usuario
- URI: Identificadores de recursos uniformes
- URN: Nombre de recursos uniforme
- UUID: Identificador universal único

10 En sistemas basados en SIP, como IMS, sería ventajoso poder dirigir una solicitud a un dispositivo específico, como un dispositivo móvil, un dispositivo de línea fija o una instancia de un cliente basado en software. Un cliente basado en software no está directamente vinculado a un dispositivo físico específico y puede ejecutarse sobre cualquier plataforma adecuada, como un ordenador personal o un dispositivo móvil avanzado. Por ejemplo, al transferir una llamada, uno puede desear dirigirse a un dispositivo específico como el dispositivo móvil de un usuario.

15 Para lograr este objetivo, un URN de agente de usuario (UA) enrutable globalmente (GRUU) es asignado al dispositivo móvil por el registrador (que es el S-CSCF en un sistema IMS). Para asignar correctamente el GRUU, el registrador usa un ID de instancia proporcionado por el dispositivo móvil durante el registro.

20 Las especificaciones actuales asumen que el dispositivo al que se apunta con el GRUU siempre será el que está realizando el registro. Sin embargo, con la introducción de los servicios centralizados (ICS) de IMS, es posible que la red se registre (en IMS) en nombre del dispositivo cuando el dispositivo usa el acceso por conmutación de circuitos (CS). En el caso de ICS, el servidor MSC es la entidad de red que se registra en nombre del abonado de CS.

25 Dado que un dispositivo ICS también puede registrarse directamente (en IMS) cuando usa el acceso por conmutación de paquetes (PS), es deseable que el ID de instancia que usa la red sea idéntica al ID de instancia que usa el dispositivo al realizar el registro. Esto asegurará que se asigne el mismo GRUU al dispositivo.

30 Las especificaciones actuales de IMS (como 24.229) no proporcionan ninguna guía específica sobre cómo el dispositivo o la red deben crear el ID de instancia. La única guía que se proporciona es que el ID de instancia debe coincidir con el formato descrito en el proyecto de salida de IETF. Por lo tanto, las especificaciones actuales no garantizan que el ID de instancia usado por la red coincida con el ID de instancia usado por el dispositivo.

35 Un posible ID de instancia sería usar directamente una identidad de equipo existente desde el dispositivo o terminal, como la IMEI. De manera desventajosa, esta identidad se transmitirá en texto plano en la señalización que se transportará tanto a la red como a los dispositivos del usuario final. Exponer la identidad del equipo de esta manera podría considerarse una violación de la privacidad, ya que revela información que puede correlacionarse con el usuario final. Además, la exposición de la identidad del equipo plantea un riesgo de seguridad, ya que esta información podría usarse para clonar el equipo. Por lo tanto, usar directamente una identidad de dispositivo

existente como la IMEI es problemático desde el punto de vista de la privacidad y la seguridad. La presente invención proporciona una solución alternativa.

5 En "Identificadores de instancia para agentes de usuario SIP", proyecto de trabajo estándar IETF, grupo de trabajo de ingeniería de Internet, ch. nº 1, 13 de julio de 2005, Jennings, Cisco Systems et al describen el objetivo de proporcionar un identificador estable a largo plazo para un agente de usuario particular en un sistema de comunicaciones basado en SIP. Con este propósito, el citado documento enseña a emplear una etiqueta de encabezado de contacto que comprende un URN de UUID.

10 En "Opciones DHCP para características del sistema huésped", proyecto de trabajo estándar IETF, grupo de trabajo de ingeniería de Internet, ch. nº 3, 22 de febrero de 1999, Mike Henry, Intel Corp describe la mejora de la interoperabilidad de servicios de configuración basándose en el protocolo de configuración host dinámico. A este respecto, el documento se refiere a tener clientes que transmitan información adicional y que tengan servidores que reconozcan esta información. Como parte de esta información adicional, D2 sugiere emplear un único identificador de clientes de manera que el servidor esté provisto de un identificador único y estático para la plataforma de clientes. Este único identificador de clientes se describe en un formato UUID de 128 bits.

15 El documento "Clarificación de que debería usarse GRUU", proyecto 3GPP, S2-082804-23, 10 de abril de 2008 se refiere a GRUU como una combinación de AOR e ID de instancia, donde el ID de instancia identifica de manera única el equipo.

20 El documento Montemurro M et al.: "Un espacio de nombres de nombre de recursos uniforme para la asociación GSM (GSMA) y la identidad de equipo de estación móvil internacional (IMEI)", IETF, 2 de febrero de 2007, se refiere a un espacio de nombres de nombre de recursos uniforme para la GSMA y subespacios de nombres para la IMEI, y para la IMEISV. La IMEI tiene una longitud de 15 dígitos decimales y la IMEISV tiene una longitud de 16 dígitos decimales y ambos están codificados usando decimal codificado binario.

25 Sería ventajoso tener un método y un aparato para un ID de instancia basado en un único identificador de dispositivo que supere las desventajas de la técnica anterior. La presente invención proporciona tal método y aparato.

30 **Sumario**

En una realización, la presente invención es un método para crear los ID de instancia que garantizan que los ID de instancia sean coherentes, ya sea que los cree el dispositivo o la red. Al mismo tiempo, la invención protege la privacidad del usuario. Para garantizar la coherencia, la creación del ID de instancia se basa en los siguientes principios:

35 el uso de un identificador único que pertenece al dispositivo pero que también es conocido en la red (denominado en el presente documento DevIID);

40 el uso de un hash para proteger el DevIID; y

45 el uso de un espacio de nombres compartido que usan tanto la red como el dispositivo al codificar el DevIID en un ID de instancia.

Breve descripción de los dibujos

En la siguiente sección, la invención se describirá con referencia a realizaciones de ejemplo ilustradas en las figuras, en las cuales:

50 la figura 1 es una Tabla 100 que muestra una representación de cadena de UUID;

la figura 2 es una Tabla 200 que muestra una definición de espacio de nombres para IMEI u otra creación de UUID basada en ID de dispositivo;

55 la figura 3 ilustra los elementos de una estructura IMEI 300;

la figura 4 ilustra los elementos de una estructura IMEISV 400;

60 la figura 5 ilustra los elementos de una estructura MEID 500;

la figura 6 es un diagrama 600 de mensajería que ilustra el registro del dispositivo;

65 la figura 7 es un encabezado 700 de mensaje que muestra un REGISTRO de ejemplo con ID de instancia (sip.instance);

la figura 8 es un diagrama 800 de mensajería que ilustra los mensajes/comandos que ocurren durante el registro de la red en nombre de un UE de CS; y

5 la figura 9 es un encabezado 900 de mensaje que ilustra el REGISTRO de ejemplo y el ID de instancia ID (sip. instance).

Descripción detallada

10 La realización descrita en el presente documento proporciona detalles específicos para la creación de un ID de instancia que garantiza la unicidad del ID, al tiempo que garantiza la privacidad de las identidades de los equipos existentes. La presente invención también proporciona un mecanismo para garantizar que la red (por ejemplo, un servidor MSC) y el dispositivo creen identificadores de instancia idénticos que se usan en la creación de un GRUU. En una realización, la presente invención hace uso del formato UUID definido en la RFC la 4122.

15 Se supone que el dispositivo descrito con respecto a una realización de la presente invención es un dispositivo móvil 3GPP que soporta los GRUU y la creación de un ID de instancia. Sin embargo, la presente invención es aplicable a cualquier dispositivo donde la red y el dispositivo compartan el conocimiento de un identificador específico del dispositivo. En el caso de un dispositivo móvil compatible con 3GPP, el DevID puede derivarse de la IMEI. En un ejemplo útil para entender la presente invención, para un dispositivo compatible con 3GPP2, el DevID puede derivarse del MEID o ESN.

20 Para clientes de software y clientes que no cumplen con los estándares móviles, es posible que la IMEI (o equivalente) no esté disponible. Por lo tanto, en un ejemplo útil para entender la invención, el DevID se crea basándose en la identidad de usuario privada del terminal. En tal escenario, un dispositivo puede estar representado por varias identidades de usuario privadas hacia el registrador, como por ejemplo una del UE como tal en el acceso PS, y una del servidor MSC que se registra en nombre del usuario. Para garantizar un comportamiento coherente, tanto el UE como la red que realiza el registro seleccionan el DevID basándose en el ID privado usado por la red. Una ventaja de usar el ID privado de la red como DevID es que se vuelve indiferente con respecto al tipo de acceso CS usado.

30 El método para la creación de ID de instancia de acuerdo con una primera realización de la presente invención es el siguiente:

35 en esta realización, la versión basada en el nombre del UUID se usa como se describe en la RFC 4122. Se puede usar la versión 3 o la versión 5; la única diferencia es el tipo de hashing que se usa (MD5 y SHA-1, respectivamente).

40 Como se ve en la Tabla 100 de la figura 1, el ID de instancia se construye como un URI de UUID usando la representación de cadena de un UUID como se describe en la RFC 4122.

Para crear el ID de instancia final, se requiere un ID de espacio de nombres. La Tabla 200 de la figura 2 proporciona la definición de un espacio de nombres que se usa como ejemplo en esta realización.

45 El siguiente método se utiliza para crear un ID de instancia que usa un ID específico del dispositivo, en este ejemplo usando la IMEI como se define en 3GPP:

elegir un algoritmo hash (MD5 o SHA-1); para este ejemplo, MD5. La red y el dispositivo deben usar el mismo algoritmo hash;

50 crear un DevID extrayendo el TAC y el SNR de la IMEI. Una estructura IMEI 300 se ilustra en la figura 3. Se usan el TAC y el SNR y se omite el dígito de reserva para un total de 14 dígitos usados. Al omitir el dígito de reserva, esta técnica también es aplicable a la IMEISV donde se omite el SVN como se ve en la figura 4. En un ejemplo útil para entender la presente invención, en el caso de dispositivos no 3GPP en los que se usa algo distinto de la IMEI, el único criterio para el DevID es que es exclusivo del dispositivo y también es conocido por la red;

55 colocar el ID de espacio de nombres (el ID de espacio de nombres se define en la Tabla 200 de la figura 2) y el DevID en orden de bytes de red;

concatenar el ID de espacio de nombres y el DevID;

60 calcular el hash de la cadena concatenada usando el algoritmo de hash preseleccionado;

establecer los campos UUID como se especifica en la subcláusula 4.3 de la RFC 4122 usando el hash tal como se calculó anteriormente y crear la representación de cadena como se muestra en la cláusula 3 de la RFC; y

65

ES 2 701 433 T3

colocar la representación de cadena en forma de urna anteponiendo "urn: uuid" a la cadena anterior. Ejemplo: urn:uuid: 3647f493-4948-abe2-6599-7c295ab29804.

5 Este URN de UUID es el ID de instancia que se usará para este dispositivo y por la red cuando se registre en nombre de este dispositivo.

Se pueden desarrollar identificadores únicos de dispositivos basándose en los diversos foros de estandarización.

10 En 3GPP, la IMEI se compone de los siguientes elementos (cada elemento constará de dígitos decimales solamente):

código de asignación de tipo (TAC). Su longitud es de 8 dígitos;

15 número de serie (SNR) es un número de serie individual que identifica de manera única a cada equipo dentro del TAC. Su longitud es de 6 dígitos; y

dígito de reserva (dígito de control): este dígito se usa como un dígito de suma de comprobación de Luhn y no se transmite con la IMEI.

20 La IMEI (14 dígitos) se complementa con un dígito de control. El dígito de control no es parte de los dígitos transmitidos.

Un ejemplo de derivación de DevID es el siguiente:

25 IMEI 3GPP:

TAC: 35196500

30 SNR: 718917

Dígito de control: 7

$$\text{DevID} = \text{TAC} + \text{SNR} = 35196500718917$$

35 La IMEISV se compone de los siguientes elementos (cada elemento constará de dígitos decimales solamente):

código de asignación de tipo (TAC). Su longitud es de 8 dígitos;

40 número de serie (SNR) es un número de serie individual que identifica de manera única a cada equipo dentro de cada TAC. Su longitud es de 6 dígitos;

número de versión de software (SVN) identifica el número de versión de software del equipo móvil. Su longitud es de 2 dígitos.

45 Un ejemplo de derivación de DevID es el siguiente:

EMEISV 3GPP:

50 TAC: 35196500

SNR: 718917

SVN: 04

55
$$\text{DevID} = \text{TAC} + \text{SNR} = 35196500718917$$

En 3GPP2, para el MEID, todos estos campos se definen como valores hexadecimales con el siguiente intervalo válido.

60 NN - intervalo válido AO - FF - administrado globalmente

TTTTTT - intervalo válido 000000 - FFFFFFFF

ZZZZZZ - intervalo válido 000000 - FFFFFFFF

65

CD - intervalo válido 0. F - El dígito de control (CD) no forma parte del MEID y no se transmite cuando se transmite el MEID.

Un ejemplo de derivación de DevID es el siguiente:

5
MEID 3GPP2:
TAC: A1000000
10 SNR: 3F0D50
CD:

DevID = TAC + SNR = A10000003F0D50

15 Se puede generar una alternativa de identificador adicional para dispositivos sin los ID de dispositivo únicos.

En un ejemplo útil para entender la presente invención de una solución de ID privada (acceso indiferente), puede que no haya un ID específico del dispositivo, como una IMEI, disponible para el cliente. Este sería el caso cuando se usa un cliente de software, por ejemplo. En este caso, la identidad privada puede ser usada en su lugar.

20 La identidad privada toma la forma de un identificador de acceso a la red (NAI) como se define en la RFC 4282. Un ejemplo de identidad privada para IMS es: user1_private@home1.net.

25 Un ejemplo de derivación de DevID es el siguiente:

ID privado:

ID privado: user1_private@home1.net

30 DevID = ID privado = user1_private@home1.net

35 Las figuras 6 y 8 ilustran los flujos de llamadas usando el método de la presente invención. Estos flujos de llamadas de ejemplo muestran una arquitectura de red basada en IMS, sin embargo, la presente invención también se aplica a arquitecturas que no son IMS.

La figura 6 ilustra un flujo 600 de llamadas cuando el dispositivo móvil se registra directamente en IMS (hacia el registrador) usando el acceso PS. Con referencia ahora a la figura 6, se muestra el flujo de registro básico en una realización de ejemplo de la presente invención. Como se ve allí, el flujo de señalización es el siguiente:

- 40 1. ID de instancia de construcción: UE A crea un ID de instancia derivado de su IMEI como se describe en el presente documento;
- 45 2. Solicitud de REGISTRO (UE A a P-CSCF): (como se ve en la figura 7);
3. Solicitud de REGISTRO (P-CSCF a I-CSCF): la P-CSCF reenvía la solicitud a la I-CSCF;
- 50 4. Cx: procedimiento de consulta del estado de registro del usuario: la I-CSCF realiza una solicitud de información relacionada con el estado de registro del abonado mediante el envío de la identidad del usuario privado, la identidad del usuario público y el nombre de dominio visitado al HSS. El HSS devuelve las capacidades requeridas de S-CSCF y la I-CSCF usa esta información para seleccionar una S-CSCF adecuada;
- 55 5. Solicitud de REGISTRO (I-CSCF a S-CSCF): la I-CSCF reenvía la solicitud de REGISTRO a la S-CSCF seleccionada;
6. 401 (No autorizado) (S-CSCF a I-CSCF): la S-CSCF impugna la solicitud de registro;
7. 401 (No autorizado) (I-CSCF a P-CSCF): la I-CSCF reenvía la respuesta a la P-CSCF;
- 60 8. 401 (No autorizado) (P-CSCF a UE A): la P-CSCF reenvía la respuesta al UE A;
9. Solicitud de REGISTRO (UE A a P-CSCF): el UE A reenvía la solicitud de REGISTRO (referida en el paso 2), esta vez con credenciales de autenticación;
- 65 10. Solicitud de REGISTRO (P-CSCF a I-CSCF): la P-CSCF reenvía la solicitud a la I-CSCF;

11. Cx: procedimiento de consulta del estado de registro del usuario: la I-CSCF realiza una solicitud de información relacionada con el estado de registro del abonado mediante el envío de la identidad del usuario privado, la identidad del usuario público y el nombre de dominio visitado al HSS. El HSS devuelve las capacidades requeridas de S-CSCF y la I-CSCF usa esta información para seleccionar una S-CSCF adecuada;
- 5 12. Solicitud de REGISTRO (I-CSCF a S-CSCF): la I-CSCF reenvía la solicitud de REGISTRO a la S-CSCF seleccionada;
- 10 13. Cx: notificación de registro de S-CSCF: la S-CSCF informa al HSS que el usuario ha sido registrado. Cuando sea solicitado por la S-CSCF, el HSS también incluirá el perfil del usuario en la respuesta enviada a la S-CSCF;
14. Construir GRUU: la S-CSCF (que actúa como registrador) construye un GRUU basándose en el ID de instancia que se creó en el paso 1. El GRUU se construye como se define en draft-ietf-sip-gruu;
- 15 15. 200 (OK) (S-CSCF a I-CSCF): la S-CSCF envía una respuesta 200 (OK) a la I-CSCF que indica que el registro se realizó correctamente. La respuesta 200 (OK) incluye el GRUU que se creó en el paso anterior;
16. 200 (OK) (I-CSCF a P-CSCF): la I-CSCF reenvía la respuesta 200 (OK) a la P-CSCF que indica que el registro se realizó correctamente; y
- 20 17. 200 (OK) (P-CSCF a UE A): la P-CSCF reenvía la respuesta 200 (OK) a UE A indicando que el registro se realizó correctamente.
- La figura 8 ilustra un flujo 800 de llamadas cuando la red se registra en nombre de un dispositivo que está usando el acceso CS. La funcionalidad de la presente invención mejora el flujo descrito en 3GPP TS 24.292:
- 25 1. Conexión CS (UE A a MSC);
- 30 2. Ubicación de autenticación y actualización (MSC/MLR a HLR/HSS);
3. Aceptar conexión CS (MSC a UE A);
- 35 4. Evaluación de registro de IMS: el servidor de MSC evalúa si necesita realizar el registro con IMS. Esto puede basarse en los datos del abonado recibidos del HSS/HLR;
5. Descubrimiento de direcciones IMS: el servidor MSC deriva un nombre de dominio de red doméstica. El dominio de red doméstica se usa para realizar consultas de DNS para ubicar la I-CSCF en la red doméstica;
- 40 6. ID de instancia de construcción: el servidor MSC crea un ID de instancia derivado de la IMEI del UE A como se describe en esta invención;
7. Solicitud de REGISTRO (servidor MSC a I-CSCF): el propósito de esta solicitud es registrar una identidad de usuario privada y una identidad de usuario pública temporal derivada para este abonado en nombre del usuario con una S-CSCF en la red doméstica. Esta solicitud se enruta a la I-CSCF en la red doméstica;
- 45 8. Cx: procedimiento de consulta del estado de registro del usuario: la I-CSCF realiza una solicitud de información relacionada con el estado de registro del abonado mediante el envío de la identidad del usuario privado, la identidad del usuario público y el nombre de dominio visitado al HSS. El HSS devuelve las capacidades requeridas de S-CSCF y la I-CSCF usa esta información para seleccionar una S-CSCF adecuada;
- 50 9. Solicitud de REGISTRO (I-CSCF a S-CSCF): la I-CSCF reenvía la solicitud de REGISTRO a la S-CSCF seleccionada;
10. Cx: notificación de registro de S-CSCF: la S-CSCF informa al HSS que el usuario ha sido registrado. Cuando sea solicitado por la S-CSCF, el HSS también incluirá el perfil del usuario en la respuesta enviada a la S-CSCF;
- 55 11. Construir GRUU: la S-CSCF, actuando como el registrador, construye un GRUU basándose en el ID de instancia que se creó en el paso 6. El GRUU se construye como se define en draft-ietf-sip-gruu. Debido a que esta ID de instancia usada era la misma que el dispositivo habría generado, el GRUU que se crea también será idéntico a uno que se devolvería a un dispositivo que se registra directamente;
- 60 12. 200 (OK) (S-CSCF a I-CSCF): la S-CSCF envía una respuesta 200 (OK) a la I-CSCF que indica que el registro se realizó correctamente. La respuesta 200 (OK) incluye el GRUU que se creó en el paso anterior; y
- 65 13. 200 (OK) (I-CSCF a servidor MSC): la I-CSCF envía la respuesta 200 (OK) al MSC Server indicando que el registro se realizó correctamente.

La presente invención tiene numerosas ventajas. Asegura que cualquier ID de instancia creado por una red será idéntico a un ID de instancia creado por el dispositivo. Esto, a su vez, hace que se defina el mismo GRUU independientemente de cómo se registró el dispositivo (directamente o por la red). La presente invención proporciona pasos específicos para definir la creación del ID de instancia, particularmente en el caso de un sistema IMS. De esta manera, llena un vacío en las especificaciones 3GPP existentes. La presente invención asegura así un comportamiento consistente para servicios basados en IMS tales como ICS. Además, el uso de un hash para derivar el ID de instancia protege el identificador específico del dispositivo, como la IMEI y el MEID, que a su vez protege la integridad de este identificador específico del dispositivo, mejorando así la seguridad.

Como reconocerán los expertos en la técnica, los conceptos innovadores descritos en la presente solicitud pueden modificarse y variarse en una amplia gama de solicitudes. Por consiguiente, el alcance de la materia patentada no debe limitarse a ninguna de las enseñanzas de ejemplo específicas discutidas anteriormente, sino que se define mediante las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método para usar en una red de comunicaciones, el método realizado por un dispositivo móvil o un equipo de usuario o realizado por un centro de conmutación móvil, MSC, comprendiendo el método el paso de:
- 5 crear un identificador de instancia, ID, para identificar de manera única el dispositivo móvil o el equipo de usuario, UE, en la red de comunicaciones mientras se asegura la privacidad del dispositivo móvil o identidades del UE existentes, en el que la creación del identificador de instancia se basa en:
- 10 seleccionar un algoritmo hash de uno de MD5 o SHA-1;
- crear un identificador único que pertenece al dispositivo móvil o al UE y es conocido para la red, DevID, extrayendo un código de asignación de tipo, TAC, y un número en serie, SNR, de una identidad de equipo móvil internacional, IMEI, del dispositivo móvil o UE;
- 15 cuando se usa el TAC y el SNR omitir el dígito de reserva de la IMEI por un total de 14 dígitos;
- colocar un ID de espacio de nombres y el DevID en orden de bytes de red;
- 20 concatenar el ID de espacio de nombres y el DevID;
- calcular un hash de la cadena concatenada usando el algoritmo hash seleccionado;
- establecer campos de un identificador único universalmente, UUID, usando el hash y crear una representación de cadena; y
- 25 colocar la representación de cadena en forma de urna anteponiendo "urn:uuid" a la cadena para construir el ID de instancia como un UUID, usando URN la representación de cadena de un UUID.
- 30 2.- El método de la reivindicación 1, en el que el dispositivo móvil o el UE es compatible con los estándares 3GPP y soporta el agente de usuario globalmente enrutable, GRUU.
- 3.- Un aparato para su uso en una red de comunicación, que comprende:
- 35 medios para crear un identificador de instancia, ID, para identificar de manera única un dispositivo móvil o un equipo de usuario, UE, en la red de comunicaciones mientras se asegura la privacidad del dispositivo móvil o identidades del UE existentes, en el que los medios se configuran para crear el identificador de instancia basándose en:
- 40 seleccionar un algoritmo hash de uno de MD5 o SHA-1;
- crear un identificador único que pertenece al dispositivo móvil o al UE y es conocido para la red, DevID, extrayendo un código de asignación de tipo, TAC, y un número en serie, SNR, de una identidad de equipo móvil internacional, IMEI, del dispositivo móvil o UE;
- 45 cuando se usa el TAC y el SNR omitir el dígito de reserva de la IMEI por un total de 14 dígitos;
- colocar un ID de espacio de nombres y el DevID en orden de bytes de red;
- concatenar el ID de espacio de nombres y el DevID;
- 50 calcular un hash de la cadena concatenada usando el algoritmo hash seleccionado;
- establecer campos de un identificador único universalmente, UUID, usando el hash y creando una representación de cadena; y
- 55 colocar la representación de cadena en forma de urna anteponiendo "urn:uuid" a la cadena para construir el ID de instancia como un UUID, usando URN la representación de cadena de un UUID.
- 60 4.- El aparato de la reivindicación 3, en el que el dispositivo móvil o el UE es compatible con los estándares 3GPP y soporta el agente de usuario globalmente enrutable, GRUU.
- 5.- Un programa informático para crear un identificador de instancia, ID, para identificar de manera única un dispositivo móvil o un equipo de usuario, UE, en la red de comunicaciones mientras se asegura la privacidad del dispositivo móvil o identidades del UE existentes, estando dicho programa informático incluido en un medio legible por ordenador, que comprende:
- 65

ES 2 701 433 T3

seleccionar un algoritmo hash de uno de MD5 o SHA-1;

crear un identificador único que pertenece al dispositivo móvil o al UE y es conocido para la red, DevID, extrayendo un código de asignación de tipo, TAC, y un número en serie, SNR, de una identidad de equipo móvil internacional, IMEI, del dispositivo móvil o UE;

5

cuando se usa el TAC y el SNR omitir el dígito de reserva de la IMEI por un total de 14 dígitos;

colocar un ID de espacio de nombres y el DevID en orden de bytes de red;

10

concatenar el ID de espacio de nombres y el DevID;

calcular un hash de la cadena concatenada usando el algoritmo hash seleccionado;

15

establecer los campos del UUID, usando el hash y creando una representación de cadena; y

colocar la representación de cadena en forma de urna anteponiendo "urn:uuid" a la cadena para construir el ID de instancia como un UUID, usando URN la representación de cadena de un UUID.

20

6.- El programa informático de la reivindicación 5, en el que el dispositivo móvil o el UE es compatible con los estándares 3GPP y soporta el agente de usuario globalmente enrutable, GRUU.

La definición formal de la representación de cadena del UUID es provista por la siguiente ABNF:

```

UUID = time-low "-" time-mid
"-"   time-high-and-version
"-"   clock-seq-and-reserved
      clock-seq-low "-" node
time-low = 4hexOctet
time-mid = 2hexOctet
time-high-and-version = 2hexOctet
clock-seq-and-reserved = hexOctet
clock-seq-low = hexOctet
node = 6hexOctet
hexOctet = hexDigit hexDigit
hexDigit =
    "0" / "1" / "2" / "3" / "4" / "5" / "6" /
    "7" / "8" / "9" /
    "a" / "b" / "c" / "d" / "e" / "f" /
    "A" / "B" / "C" / "D" / "E" / "F"

```

Lo siguientes es un ejemplo de la representación de cadena de un UUID como un URN:

```

urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

```

FIGURA 1

```

/* Name string is an IMEI or other device ID*/
uuid_t NameSpace_DeviceID = { /* efcf4930-4caf-11dd-a616-
0800200c9a66 */
    0xefcf4930,
    0x4caf,
    0x11dd,
    0xae, 0x16, 0x08, 0x00, 0x20, 0x0c, 0x9a, 0x66
};

```

FIGURA 2

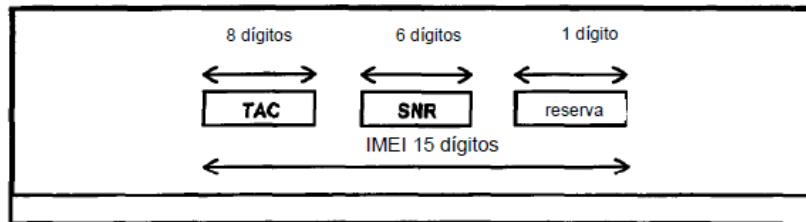


FIGURA 3

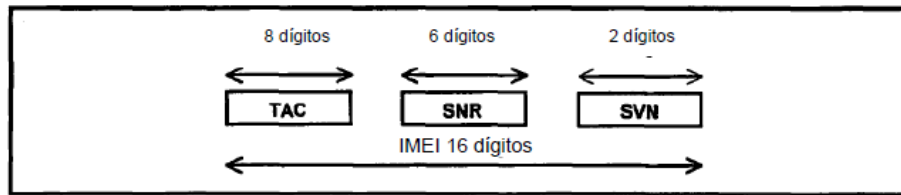


FIGURA 4



FIGURA 5

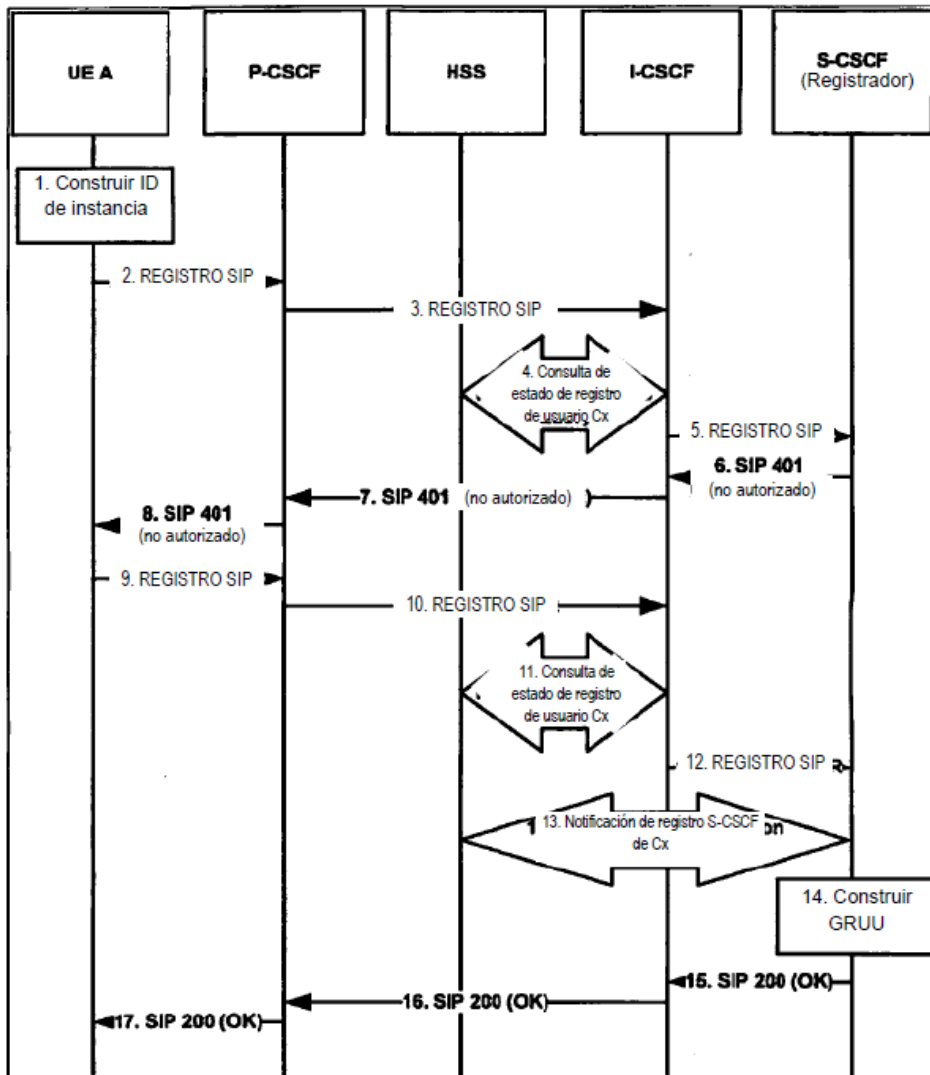


FIGURA 6

```
REGISTER sip:user1_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd];branch=z9hG4bKnashds7
Max-Forwards: 70
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact:
<sip:[5555::aaa:bbb:ccc:ddd]>;expires=600000;+sip.instance="urn:uuid:721c5fce-7fd8-63cc-1a99-9df549a58778";+g.3gpp.icsi_ref="urn:3Aurn-xxx:3gpp-service.ims.icsi.mmtel"
Call-ID: apb03a0s09dkjdfglkj49111
CSeq: 1 REGISTER
Supported: path, gruu
Content-Length: 0
```

FIGURA 7

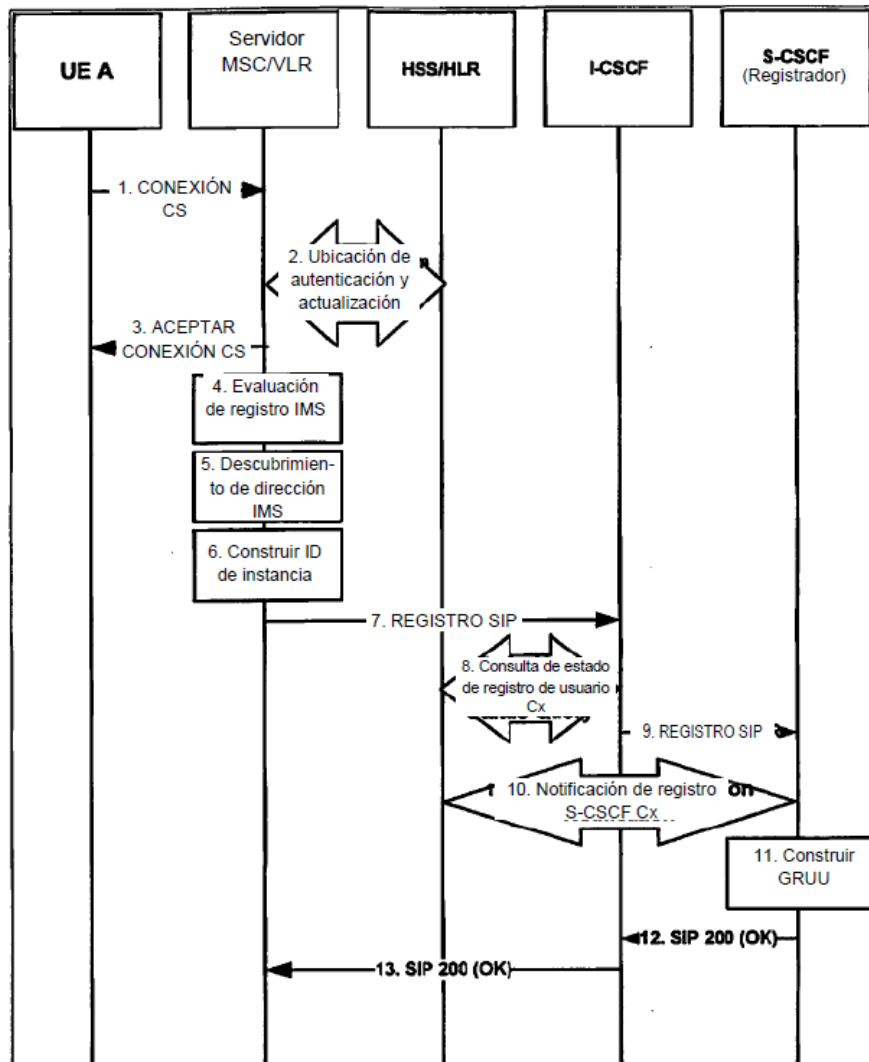


FIGURA 8

```

REGISTER sip: ics.mnc015.mcc234.3gppnetwork.org
SIP/2.0
Via: SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd];branch=z9hG4bKnashds7
Max-Forwards: 70
From:
<sip:234150999999999@ics.mnc015.mcc234.3gppnetwork.org>;ta
g=4fa3
To:
<sip:234150999999999@ics.mnc015.mcc234.3gppnetwork.org>
Contact:
<sip:[5555::aaa:bbb:ccc:ddd]>;expires=600000;+sip.instance
="<urn:uuid:721c5fce-7fd8-63cc-1a99-
9df549a58778>";+g.3gpp.icsi_ref="urn:3Aurn-xxx%3gpp-
service.ims.icsi.mmtel"
Call-ID: apb03a0s09dkjdfgkij49111
CSeq: 1 REGISTER
Supported: path, gruu
Content-Length: 0

```

FIGURA 9