(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 027**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 4/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.01.2006 PCT/IB2006/000726**

(87) Fecha y número de publicación internacional: **10.08.2006 WO06082528**

(96) Fecha de presentación y número de la solicitud europea: **31.01.2006 E 06710601 (3)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2020 EP 1844594**

(54) Título: **Método y aparatos para la transmisión de identidades de usuario en un subsistema multimedia IP**

(30) Prioridad:

04.02.2005 GB 0502383

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.07.2020

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

TAMMI, KALLE;
AITTOLA, MIKKO;
MYLLYMAKI, MINNA y
LEINONEN, ANU, H.

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y aparatos para la transmisión de identidades de usuario en un subsistema multimedia IP

Esta invención se refiere al registro de identidades de usuario en un sistema de comunicaciones.

La figura 1 muestra parte de la arquitectura del sistema 3GPP, que incluye el subsistema multimedia IP (IMS) 1. El IMS incluye una función de control de sesión de llamada en servicio (S-CSCF) 2 que puede comunicarse con un servidor de abonado doméstico (HSS) 3 a través de una interfaz de tipo Cx. El sistema también incluye una o más entidades de conexión 4, tales como dominios de paquetes conmutados o P-CSCF por medio de los cuales el IMS 1 puede comunicarse con las entidades de usuario 5, tales como teléfonos móviles. La interfaz 6 entre la S-CSCF 2 y el HSS 3 es una interfaz de tipo Cx, cuyas características están estrictamente especificadas.

La funcionalidad general de las unidades mostradas en la figura 1 en un sistema 3G actual se conoce bien. En particular, la S-CSCF proporciona servicios a las entidades de usuario y el HSS almacena información sobre suscripciones a las que puede acceder la S-CSCF y almacenarlas en una base de datos local 7 para ayudar a la prestación de servicios a los usuarios bajo esa suscripción.

La especificación actual para 3GPP Rev-6 TS 23.228 (versión 6.7.0, capítulo 4.3.3.4 figura 4.6) define la suscripción IMS, que puede consistir en múltiples identidades de usuario privadas. Las identidades de usuario privadas pueden emparejarse con identidades de usuario públicas dedicadas o compartidas.

Actualmente, el par identidad de usuario pública - identidad de usuario privada se registra explícitamente y se supone que la S-CSCF descubrirá sobre el emparejamiento de las identidades de usuarios privadas de una suscripción con la ayuda de las identidad/identidades de usuarios públicas compartidas cuando se registren. En algunas situaciones esto puede funcionar satisfactoriamente. Sin embargo, las identidades de usuario privadas también pueden tener identidades de usuario públicas dedicadas, que pueden registrarse independientemente de las identidades de usuario públicas compartidas. Se ha identificado que cuando esto sucede bajo el diseño actual, la S-CSCF no tiene medios para descubrir que los emparejamientos de una identidad de usuario pública registrada con una identidad de usuario privada pertenecen a la misma suscripción IMS.

Por lo tanto, existe la necesidad de un medio para permitir que la S-CSCF descubra dichos emparejamientos.

El documento WO 2004/000089 (US 2004/0196796) trata los problemas asociados con un HSS que vincula múltiples identidades de usuario al mismo suscriptor. Dichas identidades deben registrarse en el mismo S-CSCF y, en consecuencia, el HSS no proporciona capacidades de servidor para el segundo y el resto de registros, pero en cambio da el nombre de la S-CSCF ya usado.

"El sistema digital de telecomunicaciones móviles (Fase 2+); el sistema de telecomunicaciones móviles universal (UMTS); Las interfaces Cx y Dx de subsistema multimedia IP (IM); los flujos de señalización y contenidos de mensaje" (3GPP TS 29.228 versión 6.5.0 Versión 6) describe las interacciones entre el HSS (servidor de abonado doméstico) y las CSCF (funciones de control de sesión de llamada).

De acuerdo con un aspecto de la presente invención, se proporciona un método para ayudar en el registro de las características de suscripción en un sistema de comunicaciones en el que una característica de identidad de usuario privada puede emparejarse con una característica de identidad de usuario pública y puede asociarse más de una identidad de usuario privada con una suscripción; el método comprende transmitir desde una entidad de almacenamiento de información de suscripción del sistema a una entidad de prestación de servicios del sistema un primer mensaje que contiene datos que especifican las características de un emparejamiento de una primera identidad de usuario privada y una identidad de usuario pública, incluyendo también el mensaje una indicación de cualquier otra identidad de usuario privada que no sea la primera identidad de usuario privada asociada con la misma suscripción que la primera identidad de usuario privada.

La invención se expone en las reivindicaciones adjuntas.

La presente invención se describirá a continuación por medio de un ejemplo haciendo referencia a los dibujos adjuntos.

En el dibujo:

La figura 1 muestra un sistema de comunicación.

En resumen, este ejemplo de la presente invención implica la introducción de un nuevo atributo para la interfaz Cx. Este atributo tiene funciones que le permiten soportar suscripciones de IMS con múltiples identidades de usuario privadas.

Como se explicará con más detalle a continuación, en este ejemplo de la invención se agrega un nuevo atributo a la interfaz Cx. Este atributo se denomina en el presente documento como un atributo de identidades asociadas. El atributo es capaz de transportar información suficiente para informar en cuanto a la S-CSCF de las identidades privadas de la suscripción IMS para la S-CSCF durante el registro de un par identidad de usuario privada - identidad de usuario pública y cuando se agrega una nueva identidad de usuario privada a la suscripción.

Cuando un usuario registra un par identidad de usuario privada - identidad de usuario pública en el IMS, la S-CSCF recupera los datos de autenticación y los datos de usuario relacionados con el par de identidad del HSS a través de la interfaz Cx. Los comandos usados para esto son solicitud de autenticación multimedia (MAR) y solicitud de asignación de servidor (SAR). El HSS devuelve los datos de autenticación en la respuesta de autenticación multimedia (MAA) y los datos del usuario en el mensaje de respuesta de asignación de servidor (SAA).

Si el par de identidad privada - identidad pública pertenece a una suscripción IMS que contiene más identidades privadas, el HSS agrega una lista de las otras identidades de usuario privadas de la suscripción en la SAA. Para hacer esto, se usa el par atributo-valor de identidades asociadas (AVP). El AVP de identidades asociadas se conoce por las unidades que usan la interfaz Cx como que contiene una lista de los AVP de nombre de usuario, que contienen una identidad de usuario privada.

Usando el formato convencional para mensajes 3GPP, el mensaje SAA se define de la siguiente manera:

```
<respuesta de asignación de servidor>:: = <Encabezado de diámetro: 301, PXY, 16777216>
                                  <Id. de sesión>
                                  {Id. de aplicación específica de proveedor}
                                  [Código de resultado]
                                  [Resultado experimental]
                                  {Estado de sesión de autenticación}
                                  {Sistema central de origen}
                                  {Dominio de origen}
                                  [Nombre de usuario]
                                  * [Funciones soportadas]
                                  [Datos de usuario]
                                  [Información de carga]
                                  * [Información de proxy]
                                  * [Registro de ruta]
                                  [Identidades asociadas]
                                  * [AVP]
```

y el campo de identidades asociadas se define de la siguiente manera:

```
Identidades asociadas:: = < Encabezado AVP: xxx>
                  * [Nombre de usuario]
                  * [AVP]
```

El término "xxx" indica un número, que puede seleccionarse para cumplir con los requisitos del sistema.

En función de las identidades de usuario privadas asociadas que recibe, la S-CSCF es capaz de aprender las identidades de usuario privadas de la suscripción IMS antes de realizar otras acciones y almacenarlas anteriormente en su base de datos.

Si se agrega una nueva identidad de usuario privada a la suscripción IMS en el HSS, el HSS informa a la S-CSCF enviando una solicitud de perfil de inserción (PPR) a la S-CSCF. La PPR contiene como clave cualquiera de las identidades de usuario privadas que la S-CSCF ya posee y la lista actualizada de las identidades de usuario privadas asociadas en el AVP de identidades asociadas. El AVP también contiene la nueva identidad de usuario privada. La S-CSCF identifica que lo hace y almacena la nueva identidad en su base de datos.

El formato del mensaje de solicitud de perfil de inserción es el siguiente:

```
<Solicitud de perfil de inserción >:: = <Encabezado de diámetro: 305, REQ, PXY,
16777216>
  <Id. de sesión>
  {Id. de aplicación específica de proveedor}
  {Estado de sesión de autenticación}
  {Sistema central de origen}
  {Dominio de origen}
  {Sistema central de destino}
  {Dominio de destino}
```

```
{Nombre de usuario}
* [Funciones soportadas]
[Datos de usuario]
[Información de carga]
* [Información de proxy]
* [Registro de ruta]
[Identidades asociadas]
* [AVP]
```

Si una identidad de usuario privada existente se elimina de una suscripción, el HSS usa un mensaje de solicitud de terminación de registro (RTR) para informar a la S-CSCF. La base de un mensaje se especifica actualmente en los estándares 3GPP. Sin embargo, en la actualidad, la RTR puede contener solo una identidad privada (es decir, el AVP de nombre de usuario) a la vez. Los presentes inventores han identificado que la eficacia con la que se usa el mensaje RTR puede mejorarse incluyendo adicionalmente el AVP de identidades asociadas en el comando RTR. De acuerdo con esta mejora, el comando RTR tendría el siguiente formato:

```
<Solicitud de terminación de registro>:: = <Encabezado de diámetro: 304, 16777216, REQ
>
                                        <Id. de sesión>
                                        {Id. de aplicación específica de proveedor}
                                        {Estado de sesión de autenticación}
                                        {Sistema central de origen}
                                        {Dominio de origen}
                                        {Sistema central de destino}
                                        {Dominio de destino}
                                        {Nombre de usuario}
                                        * [Funciones soportadas]
                                        * [Identidad pública]
                                        {Motivo de anulación de registro}
                                        [Identidades asociadas]
                                        * [Información de proxy]
                                        * [Registro de ruta]
                                        * [AVP]
```

La siguiente es una lista de códigos AVP 3GPP adecuados para implementar las funciones descritas anteriormente junto con otras funciones del sistema 3GPP.

Tabla 7.1: Códigos AVP específicos 3GPP

Código de AVP	Nombre de atributo	Tipo de datos	Especificado en el TS 3GPP
Nota: Los códigos AVP del 1 al 255 están reservados para la compatibilidad con versiones anteriores con los atributos específicos del proveedor de RADIUS 3GPP (véase TS 29.061 [13])			
Nota: Los códigos AVP del 256 al 299 están reservados para uso futuro.			
			29.234 [6]
Nota: Los códigos AVP del 300 al 399 están reservados para TS 29.234			
			29,109 [7]
Nota: Los códigos AVP del 400 al 499 están reservados para TS 29.109			
500	Causa de abortar	Enumerado	29.209 [8]
501	Dirección de carga de red de acceso	Dirección	
502	Identificador de carga de red de acceso	Agrupado	
503	Valor de identificador de carga de red de acceso	Cadena de octeto	
504	Identificador de aplicación AF	Cadena de octeto	
505	Identificador de carga AF	Cadena de octeto	
506	Testigo de autorización	Cadena de octeto	
507	Descripción del flujo	Regla de filtro IP	
508	Agrupación de flujo	Agrupado	
509	Número de flujo	No firmado32	
510	Flujos	Agrupado	
511	Estado de flujo	Enumerado	
512	Uso de flujo	Enumerado	
513	Acción específica de Gq	Enumerado	
514	Anchura de banda solicitada máxima	No firmado32	
515	Anchura de banda máximo solicitado de enlace descendente	No firmado32	

(continuación)

Código de AVP	Nombre de atributo	Tipo de datos	Especificado en el TS 3GPP
516	Anchura de banda máximo solicitado de enlace ascendente	No firmado32	
517	Descripción de componente de medio	Agrupado	
518	Número de componente de medio	No firmado32	
519	AVP de subcomponente de medio	Agrupado	
520	Tipo de medio	Enumerado	
521	Banda ancha RR	No firmado32	
522	Banda ancha RS	No firmado32	
523	Indicación de bifurcación SIP	Enumerado	
Nota: Los códigos AVP del 524 al 599 están reservados para TS 29.209			
600	Identificador de red visitada	Cadena de octeto	29.229 [2]
601	Identidad pública	CadenaUTF8	
602	Nombre de servidor	CadenaUTF8	
603	Capacidades de servidor	Agrupado	
604	Capacidad obligatoria	No firmado32	
605	Capacidad opcional	No firmado32	
606	Datos de usuario	Cadena de octeto	
607	Artículos de autenticación de número SIP	No firmado32	
608	Esquema de autenticación SIP	CadenaUTF8	
609	Autenticación SIP	Cadena de octeto	
610	Autorización SIP	Cadena de octeto	
611	Contexto de autenticación SIP	Cadena de octeto	
612	Artículo de datos de autenticación SIP	Agrupado	
613	Número de artículo SIP	No firmado32	
614	Tipo de asignación de servidor	Enumerado	
615	Motivo de anulación de registro	Agrupado	
616	Código de motivo	Enumerado	
617	Motivo de información	CadenaUTF8	
618	Información de carga	Agrupado	
619	Nombre de función de carga de evento primario	DiámetroURI	
620	Nombre de función de carga de evento secundario	DiámetroURI	
621	Nombre de función de recopilación de carga primaria	DiámetroURI	
622	Nombre de función de recopilación de carga secundaria	DiámetroURI	
623	Tipo de autorización de usuario	Enumerado	
624	Datos de usuario ya disponibles	Enumerado	
625	Clave de confidencialidad	Cadena de octeto	
626	Clave de integridad	Cadena de octeto	
627	Tipo de solicitud de datos de usuario	Enumerado	
628	Funciones soportadas	Agrupado	
629	ID de lista de funciones	No firmado32	
630	Lista de funciones	No firmado32	
631	Aplicaciones soportadas	Agrupado	
632	Identidades asociadas	Agrupado	
Nota: Los códigos AVP del 633 al 699 están reservados para TS 29.229.			
700	Identidad de usuario	Agrupado	29.329 [4]
701	MSISDN	Cadena de octeto	
702	Datos de usuario	Cadena de octeto	
703	Referencia de datos	Enumerado	
704	Indicación de servicio	Cadena de octeto	
705	Tipo de solicitud de abonado	Enumerado	
706	Dominio solicitado	Enumerado	
707	Localización actual	Enumerado	
708	Conjunto de identidad	Enumerado	
Nota: Los códigos AVP del 709 al 799 están reservados para TS 29.329.			

(continuación)

Código de AVP	Nombre de atributo	Tipo de datos	Especificado en el TS 3GPP
			32.299 [5]
Nota: Los códigos AVP del 800 al 899 están reservados para TS 32.299			
			29.061 [13]
Nota: Los códigos AVP del 900 al 999 están reservados para TS 29.061			
			29.210 [15]
Nota: Los códigos AVP del 1000 al 1099 están reservados para TS 29.210			

La siguiente es una descripción. de un *procedimiento de notificación de registro/cancelación de registro de S-CSCF adecuado para implementar las funciones descritas anteriormente en el sistema 3GPP.*

Este procedimiento se usa entre la S-CSCF y el HSS. El procedimiento se invoca por la S-CSCF, corresponde a la combinación de las operaciones Cx-Put y Cx-Pull (véase 3GPP TS 23.228 [1]) y se usa:

- para asignar una S-CSCF a una identidad de usuario pública, o para borrar el nombre de la S-CSCF asignada a una o más identidades de usuario públicas.

- para descargar del HSS la información de usuario relevante que la S-CSCF necesita para servir al usuario.

Este procedimiento se mapea a los comandos solicitud/respuesta de asignación de servidor en la aplicación Diámetro especificada en 3GPP TS 29.229 [5]. Las tablas 6.1.2.1 y 6.1.2.2 describen los elementos de información involucrados.

Tabla 6.1.2.1: Solicitud de notificación de registro/anulación de registro de S-CSCF

Nombre de elemento de información	**Mapear al AVP de diámetro**	**Cat.**	**Descripción**
Identidad de usuario pública (véase 7.2)	Identidad pública	C	Identidad de usuario pública o lista de identidades de usuario públicas. Una y solo una identidad de usuario pública estará presente si el tipo de asignación de servidor es cualquier valor que no sea TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION o ADMINISTRATIVE_DEREGISTRATION. Si el tipo de asignación de servidor indica que se anula el registro de algún tipo y la identidad de usuario privada no está presente en la solicitud, al menos una identidad de usuario pública estará presente.
Nombre de S-CSCF (véase 7.4)	Nombre de servidor	M	Nombre de la S-CSCF.
Identidad de usuario privada (véase 7.3)	Nombre de usuario	C	Identidad de usuario privada. Estará presente si está disponible cuando la S-CSCF emite la solicitud. Puede estar ausente durante el inicio de una sesión a un usuario no registrado. En tal situación, el tipo de asignación de servidor deberá contener el valor UNREGISSTEM_USER. En el caso de anulación del registro, tipo de asignación de servidor igual a TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION o ADMINISTRATIVE_DEREGISTRATION, si no está presente los AVP de identidad de usuario pública, entonces estará presente la identidad de usuario privada.
Tipo de asignación de servidor t (véase 7.8)	Tipo de asignación de servidor t	M	Tipo de actualización de las solicitudes de S-CSCF en el HSS (por ejemplo, anulación del registro). Véase 3GPP TS 29.229 [5] para todos los valores posibles.
Datos de usuario ya disponibles (véase 7.16)	Datos de usuario ya disponibles	M	Esto indica si el perfil de usuario ya está disponible en la S-CSCF. En el caso de que el tipo de asignación del servidor no sea igual a NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION o UNREGISTERED_USER, el HSS no usará los datos de usuario ya disponibles al procesar la solicitud.

(continuación)

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Información de encaminamiento (véase 7.13)	Sistema central de destino	C	Si la S-CSCF conoce el nombre del HSS, el AVP de sistema central de destino estará presente en el comando. Esta información está disponible si la solicitud pertenece a un registro ya existente, por ejemplo, en el caso de un nuevo registro, donde el nombre de HSS se almacena en la S-CSCF. El nombre de HSS se obtiene del AVP de sistema central de origen, que se recibe del HSS, por ejemplo, incluido en el comando MAA. Esta información puede no estar disponible si el comando se envía como consecuencia de la finalización de la sesión para un usuario no registrado. En este caso, el AVP de sistema central de destino no está presente y el comando se encamina al siguiente nodo de diámetro, por ejemplo, SLF, en función de la tabla de encaminamiento de diámetro en la S-CSCF.

Tabla 6.1.2.2: Respuesta de notificación de registro/anulación de registro de S-CSCF

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Identidad de usuario privada (véase 7.3)	Nombre de usuario	C	Identidad de usuario privada. Deberá estar presente si está disponible cuando el HSS envía la respuesta. Puede estar ausente en el siguiente caso de error: cuando el tipo de asignación de servidor de la solicitud es UNREGISTERED_USER y el HSS no conoce la identidad de usuario pública recibida.
Resultado de registro (véase 7.6)	Código de resultado/Resultado experimental	M	Resultado del registro. El AVP de código de resultado se usará para los errores definidos en el protocolo de base de diámetro. El AVP de resultado experimental se usará para errores Cx/ Dx. Este es un AVP agrupado que contiene el ID de proveedor 3GPP en el AVP de Id de proveedor y el código de error en el AVP de código de resultado experimental.
Perfil de usuario (véase 7.7)	Datos de usuario	C	Perfil de usuario relevante. Deberá estar presente cuando el tipo de asignación de servidor en la solicitud sea igual a NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION o UNREGISSTEM_USER de acuerdo con las reglas definidas en la sección 6.6. Si la S-CSCF recibe más datos de los que está dispuesta a aceptar, realizará la anulación del registro del usuario con el tipo de autorización de usuario establecido en DEREGISTRATION_TOO_MUCH_DATA y enviará de vuelta una respuesta SIP 3xx o 480 (temporalmente no disponible), que deberá desencadenar la selección de una nueva S-CSCF por la I-CSCF, como se especifica en 3GPP TS 24.229 [8].
Información de carga (véase 7.12)	Información de carga	C	Direcciones de las funciones de carga. Deberá estar presente cuando el AVP de datos de usuario se envíe a la S-CSCF. Cuando se incluye este parámetro, se incluirá la dirección de la función de recopilación de carga primaria. Todos los demás elementos se incluirán si están disponibles.
Identidades privadas asociadas	Identidades asociadas	C	Este AVP contiene las identidades de usuario privadas, que pertenecen a la misma suscripción IMS que la identidad de usuario privada o la identidad de usuario pública recibida en el comando SAR. Si la suscripción IMS contiene una única identidad de usuario privada, este AVP no estará presente.

Comportamiento detallado

Al registrar/anular el registro de una identidad de usuario pública, la S-CSCF informará al HSS. La S-CSCF usa el mismo procedimiento para obtener la información de usuario que contiene el perfil de usuario y la información de cobro. El perfil de usuario relevante descargado se describe con más detalle en las secciones 6.5.1 y 6.6. El HSS contiene información sobre el estado de registro de todas las identidades del usuario. La S-CSCF usa este procedimiento para actualizar dichos estados. Para identidades registradas implícitamente, se aplicarán las reglas definidas en la Sección 6.5.1. El HSS deberá, en el siguiente orden (en el caso de error en cualquiera de las etapas,

el HSS detendrá el procesamiento y devolverá el código de error correspondiente, véase 3GPP TS 29.229 [5]):

1. Verificar que el usuario sea conocido. Si no es así, el código de resultado experimental se establecerá en DIAMETER_ERROR_USER_UNKNOWN. Si no se incluye una identidad de usuario pública ni una identidad de usuario privada, el código de resultado experimental se establecerá en DIAMETER_MISSING_USER_ID.

2. El HSS puede verificar si las identidades de usuario privadas y públicas recibidas en la solicitud pertenecen al mismo usuario. Si no es así, el código de resultado experimental se establecerá en DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. Verificar el valor de tipo de asignación de servidor recibido en la solicitud:

- Si indica REGISTRATION o RE_REGISTRATION, el HSS descargará la información de usuario relevante. Si se establece el indicador de autenticación pendiente de la identidad de usuario pública que es específico para la identidad de usuario privada, el HSS lo borrará. El código de resultado se establecerá en DIAMETER_SUCCESS y el HSS establecerá el estado de registro de la identidad de usuario pública como registrada (si aún no está registrada). Si hay múltiples identidades de usuario privadas, que pertenecen a la suscripción IMS servida, el AVP de identidades asociadas se agregará al mensaje de respuesta y contendrá todas las identidades de usuario privadas asociadas a la suscripción IMS.
  Solo una identidad de usuario pública estará presente en la solicitud. Si hay más de una identidad presente, el código de resultado se establecerá en DIAMETER_AVP_OCCURS_TOO_MANY_TIMES y no se devolverá ninguna información de usuario. Si no hay una identidad de usuario pública presente, el código de resultado experimental se establecerá en DIAMETER_MISSING_USER_ID.

- Si indica UNREGISTERED_USER, el HSS almacenará el nombre de S-CSCF, establecerá el estado de registro de la identidad de usuario pública como no registrado, es decir, registrado como consecuencia de una llamada finalizada y descargará la información de usuario relevante. Si hay múltiples identidades de usuario privadas asociadas a la identidad de usuario pública en el HSS, el HSS seleccionará arbitrariamente una de las identidades de usuario privadas y la incluirá en el mensaje de respuesta. El código de resultado se establecerá en DIAMETER_SUCCESS. Si hay múltiples identidades de usuario privadas, que pertenecen a la suscripción IMS servida, el AVP de identidades asociadas se agregará al mensaje de respuesta y contendrá todas las identidades de usuario privadas asociadas a la suscripción IMS.
  Solo una identidad de usuario pública estará presente en la solicitud. Si hay más de una identidad presente, el código de resultado se establecerá en DIAMETER_AVP_OCCURS_TOO_MANY_TIMES y no se realizarán las modificaciones especificadas en el párrafo anterior. Si no hay una identidad de usuario pública presente, el código de resultado experimental se establecerá en DIAMETER_MISSING_USER_ID.

- Si indica TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA o ADMINISTRATIVE_DEREGISTRATION, el HSS borrará el nombre de S-CSCF asociado a la identidad de usuario privada para todas las identidades de usuario públicas que la S-CSCF indicó en la solicitud y establecerá el estado de registro de las identidades como no registrado. Si no hay una identidad de usuario pública presente en la solicitud, la identidad de usuario privada estará presente; en este caso, el HSS borrará el nombre de S-CSCF para todas las identidades de usuario públicas asociadas a la identidad de usuario privada y establecerá su estado de registro como no registrado. El código de resultado se establecerá en DIAMETER_SUCCESS.

- Si indica TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME o USER_DEREGISTRATION_STORE_SERVER_NAME, el HSS decide si se debe mantener almacenado el nombre de S-CSCF asociado a la identidad de usuario privada o no para todas las identidades de usuario públicas que la S-CSCF indicó en la solicitud. Si no hay una identidad de usuario pública presente en la solicitud, la identidad de usuario privada estará presente. Si el HSS decide mantener el nombre de S-CSCF almacenado, el HSS mantendrá el nombre de S-CSCF almacenado para todas las identidades de usuario públicas asociadas a la identidad de usuario privada y establecerá su estado de registro como no registrado. El código de resultado se establecerá en DIAMETER_SUCCESS.
  Si el HSS decide no mantener el nombre de S-CSCF, el código de resultado experimental se establecerá en DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED. Si el HSS recibió las identidades de usuario públicas en la solicitud, el HSS establecerá el estado de registro como no registrado para las identidades de usuario públicas que la S-CSCF indicó en la solicitud. Si el HSS recibió una identidad de usuario privada en la solicitud, el HSS establecerá el estado de registro de todas las identidades de usuario públicas relacionadas con la identidad privada como no registradas.

- Si indica NO_ASSIGNMENT, el HSS verifica si el usuario está asignado a la S-CSCF que solicita los datos y descarga la información de usuario relevante. El código de resultado se establecerá en DIAMETER_SUCCESS. Si hay múltiples identidades de usuario privadas, que pertenecen a la suscripción IMS servida, el AVP de identidades asociadas se agregará al mensaje de respuesta y contendrá todas las identidades de usuario privadas asociadas a la suscripción IMS.

Si la S-CSCF solicitante no es el mismo que la S-CSCF asignada, el código de resultado se establecerá en DIAMETER_UNABLE_TO COMPLY.
Solo una identidad de usuario pública estará presente en la solicitud. Si está presente más de una identidad de usuario pública, el código de resultado se establecerá en DIAMETER_AVP_OCCURS_TOO_MANY_TIMES y no se devolverá ninguna información de usuario. Si no hay una identidad de usuario pública presente, el código de resultado experimental se establecerá en DIAMETER_MISSING_USER_ID.

- Si indica AUTHENTICATION_FAILURE o AUTHENTICATION_TIMEOUT, el HSS borrará el nombre de S-CSCF para la identidad de usuario pública asociada a la identidad de usuario privada que la S-CSCF indicó en la solicitud y establecerá el estado de registro de la identidad como no registrado. Si se establece el indicador de autenticación pendiente de la identidad de usuario pública que es específico para la identidad de usuario privada, el HSS lo borrará. El código de resultado se establecerá en DIAMETER_SUCCESS.
Solo una identidad de usuario pública estará presente en la solicitud. Si hay más de una identidad presente, el código de resultado se establecerá en DIAMETER_AVP_OCCURS_TOO_MANY_TIMES y no se realizarán las modificaciones especificadas en el párrafo anterior. Si no hay una identidad de usuario pública presente, el código de resultado experimental se establecerá en DIAMETER_MISSING_USER_ID.

Si el HSS no puede cumplir la solicitud recibida, por ejemplo, debido a un error en la base de datos, establecerá el código de resultado en DIAMETER_UNABLE_TO_COMPLY. El HSS no modificará ningún estado de usuario ni descargará ninguna información de identidad de usuario pública de usuario al S-CSCF.

Véanse los capítulos 8.1.2 y 8.1.3 para obtener una descripción del manejo de las situaciones de error: recepción de un nombre de S-CSCF diferente del almacenado en el HSS y recepción de un valor de tipo de asignación de servidor no compatible con el registro estado del usuario.

La siguiente es una descripción de un procedimiento de autenticación adecuado para implementar las funciones descritas anteriormente en el sistema 3GPP.

Este procedimiento se usa entre la S-CSCF y el HSS para intercambiar información para soportar la autenticación entre el usuario final y la red IMS doméstica. El procedimiento se invoca por la S-CSCF, corresponde a la combinación de las operaciones Cx-AV-Req y Cx-Put (véase 3GPP TS 33.203 [3]) y se usa:

- para recuperar vectores de autenticación del HSS.

- para resolver fallos de sincronización entre los números de secuencia en el UE y el HSS.

Este procedimiento se mapea a los comandos de solicitud/respuesta de autenticación multimedia en la aplicación Diámetro especificada en 3GPP TS 29.229 [5]. Las tablas 6.3.1 - 6.3.5 detallan los elementos de información involucrados.

Tabla 6.3.1: Solicitud de autenticación

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Identidad de usuario pública (véase 7.2)	Identidad pública	M	Este elemento de información contiene la identidad pública del usuario
Identidad de usuario privada (véase 7.3)	Nombre de usuario	M	Este elemento de información contiene la identidad privada del usuario
Artículos de autenticación de número (véase 7.10)	Artículos de autenticación de número SIP	M	Este elemento de información indica el número de vectores de autenticación solicitados
Datos de autenticación (véase 7.9)	Artículo de datos de autenticación SIP	M	Véanse las Tablas 6.3.2 y 6.3.3 para los contenidos de este elemento de información. El contenido mostrado en la tabla 6.3.2 se usará para una solicitud de autenticación normal; el contenido mostrado en la tabla 6.3.3 se usará para una solicitud de autenticación después de un fallo de sincronización.
Nombre de S-CSCF (véase 7.4)	Nombre de servidor	M	Este elemento de información contiene el nombre (URL SIP) de la S-CSCF.

(continuación)

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Información de encaminamiento (véase 7.13)	Sistema central de destino	C	Si la S-CSCF conoce el nombre de HSS, este AVP estará presente. Esta información está disponible si la MAR pertenece a un registro ya existente, por ejemplo, en el caso de un nuevo registro, donde el nombre de HSS se almacena en la S-CSCF. El nombre de HSS se obtiene del AVP de sistema central de origen, que se recibe del HSS, por ejemplo, incluido en el comando MAA. Es posible que esta información no esté disponible si se envía el comando en el caso del registro inicial. En este caso, el AVP de sistema central de destino no está presente y el comando se encamina al siguiente nodo de diámetro, por ejemplo, SLF, basándose en la tabla de encaminamiento de diámetro en el cliente.

Tabla 6.3.2: Contenido - solicitud de datos de autenticación

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Esquema de autenticación (véase 7.9.2)	Esquema de autenticación SIP	M	Este elemento de información indica el esquema de autenticación. Contendrá "Digest-AKAv1-MD5".

Tabla 6.3.3: Contenido - solicitud de datos de autenticación, fallo de sincronización

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Esquema de autenticación (véase 7.9.2)	Esquema de autenticación SIP	M	Esquema de autenticación. Contendrá "Digest-AKAv1-MD5".
Información de autorización (véase 7.9.4)	Autorización SIP	M	Contendrá la concatenación de nonce, tal como se envía al terminal, y auts, tal como se recibe del terminal. Nonce y auts serán codificados en binario.

Tabla 6.3.4: Respuesta de autenticación

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Identidad de usuario (véase 7.2)	Identidad pública	C	Identidad pública de usuario. Deberá estar presente cuando el resultado sea DIAMETER_SUCCESS.
Identidad de usuario privada (véase 7.3)	Nombre de usuario	C	Identidad privada de usuario. Deberá estar presente cuando el resultado sea DIAMETER_SUCCESS.
Artículos de autenticación de número (véase 7.10)	Artículos de autenticación de número SIP	C	Este AVP indica el número de vectores de autenticación entregados en el elemento de información de datos de autenticación. Deberá estar presente cuando el resultado sea DIAMETER_SUCCESS.
Datos de autenticación (véase 7.9)	Artículo de datos de autenticación SIP	C	Si el AVP de artículos de autenticación de número SIP es igual a cero o no está presente, entonces este AVP no estará presente. Véase la Tabla 6.3.5 para el contenido de este elemento de información.
Resultado (véase 7.6)	Código de resultado/Resultado experimental	M	Resultado de la operación. El AVP de código de resultado se usará para los errores definidos en el protocolo de base de diámetro. El AVP de resultado experimental se usará para errores Cx/ Dx. Este es un AVP agrupado que contiene el ID de proveedor 3GPP en el AVP de Id de proveedor y el código de error en el AVP de código de resultado experimental.
Identidades privadas asociadas	Identidades asociadas	C	Este AVP contiene las identidades de usuario privadas, que pertenecen a la misma suscripción IMS que la identidad de usuario privada recibida en el comando MAR. Si la suscripción IMS contiene una única identidad de usuario privada, este AVP no estará presente.

Tabla 6.3.5: Contenido - respuesta de datos de autenticación

Nombre de elemento de información	Mapear al AVP de diámetro	Cat.	Descripción
Número de artículo (véase 7.9.1)	Número de artículo SIP	C	Este elemento de información debe estar presente en un AVP agrupado de artículos de datos de autenticación SIP en circunstancias donde hay múltiples incidencias de los AVP de artículos de datos de autenticación SIP, y el orden en que deben procesarse es significativo. En este escenario, los AVP de artículos de datos de autenticación SIP con un valor de número de artículo SIP bajo deberían procesarse antes que los AVP de artículos de datos de autenticación SIP con un valor de número de artículo SIP alto.
Esquema de autenticación (véase 7.9.2)	Esquema de autenticación SIP	M	Esquema de autenticación. Contendrá "Digest-AKAvl-MD5".
Información de autenticación (véase 7.9.3)	Autenticación SIP	M	Contendrá, codificado en binario, la concatenación de la autenticación RAND de desafío y el testigo AUTN. Véase 3GPP TS 33.203 [3] para más detalles sobre RAND y AUTN.
Información de autorización (véase 7.9.4)	Autorización SIP	M	Contendrá codificada en binario, la respuesta esperada XRES. Véase 3GPP TS 33.203 [3] para más detalles sobre XRES.
Clave de confidencialidad (véase 7.9.5)	Clave de confidencialidad	O	- Este elemento de información, si está presente, contendrá la clave de confidencialidad. Estará codificado en binario.
Clave de integridad (véase 7.9.6)	Clave de integridad	M	- Este elemento de información deberá contener la clave de integridad. Estará codificado en binario.

Comportamiento detallado

El HSS deberá, en el siguiente orden (en el caso de error en cualquiera de las etapas, el HSS detendrá el procesamiento y devolverá el código de error correspondiente, véase 3GPP TS 29.229 [5]):

1. Verificar que el usuario existe en el HSS. Si no es así, el código de resultado experimental se establecerá en DIAMETER_ERROR_USER_UNKNOWN.

2. El HSS puede verificar que las identidades públicas y privadas pertenecen al mismo usuario. Si no es así, el código de resultado experimental se establecerá en DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. Verificar que el esquema de autenticación indicado se soporte en la solicitud. Si no es así, el código de resultado experimental se establecerá en DIAMETER_ERROR_AUTH_SCHEME_UNSUPPORTED.

4. Si la solicitud indica que hay un fallo de sincronización, el HSS comparará el nombre de S-CSCF recibido en la solicitud con el nombre de S-CSCF almacenado en el HSS:

- Si son idénticos, el HSS procesará los AUTS como se describe en 3GPP TS 33.203 [3] y devolverá la información de autenticación solicitada. El código de resultado se establecerá en DIAMETER_SUCCESS.

5. Verificar el estado de registro de la identidad pública recibida en la solicitud:

- Si está registrado, el HSS comparará el nombre de S-CSCF recibido en la solicitud con el nombre de S-CSCF almacenado en el HSS:

  - Si son diferentes, el HSS almacenará el nombre de S-CSCF. El HSS descargará el artículo de datos de autenticación almacenado hasta un máximo especificado en los artículos de autenticación de número SIP recibidos en el comando solicitud de autenticación multimedia. El HSS establecerá el indicador pendiente de autenticación de la identidad pública que es específico de la identidad privada que se recibió en la solicitud. El código de resultado se establecerá en DIAMETER_SUCCESS.

  - Si son idénticos, el HSS descargará el artículo de datos de autenticación almacenado hasta un máximo especificado en los artículos de autenticación de número SIP recibidos en el comando solicitud de autenticación multimedia. El código de resultado se establecerá en DIAMETER_SUCCESS.

- Si no está registrado (es decir, registrado como consecuencia de una llamada finalizada a un usuario no

registrado o hay una S-CSCF que mantiene el perfil de usuario almacenado), el HSS comparará el nombre de S-CSCF recibido en la solicitud con el nombre de S-CSCF almacenado en el HSS:

- Si son diferentes, el HSS almacenará el nombre de S-CSCF. El HSS descargará el artículo de datos de autenticación almacenado hasta un máximo especificado en los artículos de autenticación de número SIP recibidos en el comando solicitud de autenticación multimedia. El HSS establecerá el indicador pendiente de autenticación de la identidad pública que es específico de la identidad privada que se recibió en la solicitud. El código de resultado se establecerá en DIAMETER_SUCCESS.

- Si son idénticos, el HSS descargará el artículo de datos de autenticación almacenado hasta un máximo especificado en los artículos de autenticación de número SIP recibidos en el comando solicitud de autenticación multimedia. El HSS establecerá el indicador pendiente de autenticación de la identidad pública que es específico de la identidad privada que se recibió en la solicitud. El código de resultado se establecerá en DIAMETER_SUCCESS.

- Si no está registrado, el HSS almacenará el nombre de S-CSCF. El HSS descargará el artículo de datos de autenticación almacenado hasta un máximo especificado en los artículos de autenticación de número SIP recibidos en el comando solicitud de autenticación multimedia. El HSS establecerá el indicador pendiente de autenticación de la identidad pública que es específico de la identidad privada que se recibió en la solicitud. El código de resultado se establecerá en DIAMETER_SUCCESS.

6. Si hay múltiples identidades de usuario privadas, que pertenecen a la suscripción IMS servida, el AVP de identidades asociadas se agregará al mensaje de respuesta y contendrá todas las identidades de usuario privadas asociadas a la suscripción IMS.

Las excepciones a los casos especificados en este caso serán tratadas por el HSS como situaciones de error, el código de resultados se establecerá en DIAMETER_UNABLE_TO_COMPLY. No se devolverá información de autenticación.

Este elemento de información de identidades privadas asociadas indica al S-CSCF las identidades de usuario privadas, que pertenecen a la misma suscripción IMS. Véase 3GPP TS 29.229 [5].

La siguiente es una descripción del comando respuesta de asignación de servidor (SAA) adecuado para implementar las funciones descritas anteriormente en el sistema 3GPP.

El comando respuesta de asignación de servidor (SAA), indicado por el campo código de comando establecido en 301 y el bit 'R' borrado en el campo de indicadores de comando, se envía por un servidor en respuesta al comando solicitud de asignación de servidor. El código de resultado o AVP de resultado experimental puede contener uno de los valores definidos en la sección 6.2 además de los valores definidos en IETF RFC 3588 [6]. Si el código de resultado o el resultado experimental no informan acerca de un error, el AVP de datos de usuario deberá contener la información que la S-CSCF necesita para dar servicio al usuario. Formato de mensaje

<respuesta de asignación de servidor>:: = <Encabezado de diámetro: 301, PXY, 16777216>
<Id. de sesión>
{Id. de aplicación específica de proveedor}
[Código de resultado]
[Resultado experimental]
{Estado de sesión de autenticación}
{Sistema central de origen}
{Dominio de origen}
[Nombre de usuario]
*** [Funciones soportadas]**
[Datos de usuario]
[Información de carga]
[Identidades asociadas]
* [AVP]
* [Información de proxy]
* [Registro de ruta]

La siguiente es una descripción del comando de respuesta de autenticación multimedia (MAA) adecuado para implementar las funciones descritas anteriormente en el sistema 3GPP.

El comando de respuesta de autenticación multimedia (MAA), indicado por el campo código de comando establecido en 303 y el bit 'R' borrado en el campo indicadores de comando, se envía por un servidor en respuesta al comando de solicitud de autenticación multimedia. El código de resultado o AVP de resultado experimental puede contener uno de los valores definidos en la sección 6.2 además de los valores definidos en IETF RFC 3588 [6].

Formato de mensaje

<respuesta de autenticación multimedia>:: = <Encabezado de diámetro: 303, PXY, 16777216>
<Id. de sesión>
{Id. de aplicación específica de proveedor}
[Código de resultado]
[Resultado experimental]
{Estado de sesión de autenticación}
{Sistema central de origen}
{Dominio de origen}
[Nombre de usuario]
*** [Funciones soportadas]**
[Identidad pública]
[Artículos de autenticación de número SIP]
*** [Artículo de datos de autenticación SIP]**
[Identidades asociadas]
* [AVP]
* [Información de proxy]
* [Registro de ruta]

La siguiente es una descripción de los AVP adecuados para implementar las funciones descritas anteriormente en el sistema 3GPP junto con otras características del sistema.

La siguiente tabla describe los AVP de diámetro definidos para el protocolo de interfaz Cx, sus valores de código AVP, tipos, posibles valores de indicador y si el AVP puede o no estar encriptado. El encabezado de Id de proveedor de todos los AVP definidos en esta especificación se establecerá en 3GPP (10415).

Tabla 6.3.1: AVP de aplicación multimedia de diámetro

				Reglas de indicador de AVP				
Nombre de atributo	**Código de AVP**	**Sección definida**	**Tipo de valor**	**Debe**	**Puede**	**No debería**	**No debe**	**Puede Encr.**
Identificador de red visitada	600	6,31	Cadena de octeto	M, V				No
Identidad pública	601	6,32	CadenaUTF8	M, V				N
Nombre de servidor	602	6,33	CadenaUTF8	M, V				No
Capacidades de servidor	603	6,34	Agrupado	M, V				No
Capacidad obligatoria	604	6,35	No firmado32	M, V				No
Capacidad opcional	605	6,36	No firmado32	M, V				No
Datos de usuario	606	6,37	Cadena de octeto	M, V				No
Artículos de autenticación de número SIP	607	6.3.8	No firmado32	M, V				No
Esquema de autenticación SIP	608	6.3.9	CadenaUTF8	M, V				No
Autenticación SIP	609	6.3.10	Cadena de octeto	M, V				No
Autorización SIP	610	6,311	Cadena de octeto	M, V				No
Contexto de autenticación SIP	611	6.3.12	Cadena de octeto	M, V				No
Artículo de datos de autenticación SIP	612	6.3.13	Agrupado	M, V				No
Número de artículo SIP	613	6.3.14	No firmado32	M, V				No
Tipo de asignación de servidor	614	6.3.15	Enumerado	M, V				No
Motivo de anulación de registro	615	6.3.16	Agrupado	M, V				No
Código de motivo	616	6.3.17	Enumerado	M, V				No
Motivo de información	617	6.3.18	CadenaUTF8	M, V				No
Información de carga	618	6.3.19	Agrupado	M, V				No
Nombre de función de carga de evento primario	619	6.3.20	DiámetroURI	M, V				No
Nombre de función de carga de evento secundario	620	6.3.21	DiámetroURI	M, V				No

(continuación)

				Reglas de indicador de AVP				
Nombre de atributo	**Código de AVP**	**Sección definida**	**Tipo de valor**	**Debe**	**Puede**	**No debería**	**No debe**	**Puede Encr.**
Nombre de función de recopilación de carga primaria	621	6.3.22	DiámetroURI	M, V				No
Nombre de función de recopilación de carga secundaria	622	6.3.23	DiámetroURI	M, V				No
Tipo de autorización de usuario	623	6.3.24	Enumerado	M, V				No
Datos de usuario ya disponibles	624	6.3.26	Enumerado	M, V				No
Clave de confidencialidad	625	6.3.27	Cadena de octeto	M, V				No
Clave de integridad	626	6.3.28	Cadena de octeto	M, V				No
Tipo de solicitud de datos de usuario	627	6.3.25	Enumerado	M, V				No
Funciones soportadas	628	6.3.29	Agrupado	V	M			No
ID de lista de funciones	629	6.3.30	No firmado32	V			M	No
Lista de funciones	630	6.3.31	No firmado32	V			M	No
Aplicaciones soportadas	631	6.3.32	Agrupado	V			M	No
Identidades asociadas	632	6.3.33	Agrupado	M, V				No
NOTA 1: El bit de encabezado de AVP indicado como 'M' indica si se requiere soporte del AVP. El bit de encabezado de AVP indicado como 'V' indica si el campo de ID de proveedor opcional está presente en el encabezado de AVP. Para más detalles, véase IETF RFC 3588 [6]. NOTA 2: En función del comando concreto.								

El AVP de identidades asociadas es de tipo Agrupado y contiene las identidades de usuario privadas asociadas a una suscripción IMS.

Formato de AVP

```
Identidades asociadas:: = <Encabezado AVP: 632 10415>
                          * [Nombre de usuario]
                          * [AVP]
```

La presente invención puede aplicarse en sistemas distintos del presente sistema de comunicaciones 3G. En principio, la capacidad de informar a una entidad proveedora de servicios (por ejemplo, una S-CSCF) de los múltiples emparejamientos de identidades de usuarios públicas y privadas es útil en una amplia gama de sistemas. Es específicamente ventajoso lograr esto por medio del mismo mensaje que se usa para informar a la entidad proveedora de servicios de información con respecto a un par de identidad primario (por ejemplo, un mensaje SAR y/ o un mensaje PPR). En consecuencia, también es ventajoso poder activar la eliminación de múltiples emparejamientos a través de un único mensaje (por ejemplo, un mensaje RTR).

REIVINDICACIONES

1. Un método para ayudar en el registro de las características de suscripción en un sistema de comunicaciones en el que una característica de identidad de usuario privada puede emparejarse con una característica de identidad de usuario pública y puede asociarse más de una identidad de usuario privada a una suscripción; comprendiendo el método transmitir desde una entidad de almacenamiento de información de suscripción (3) del sistema a una entidad de prestación de servicios del sistema (2) un primer mensaje que contiene datos que especifican las características de un emparejamiento de una primera identidad de usuario privada y una identidad de usuario pública, caracterizado por que el mensaje también incluye una indicación de cualquier otra identidad de usuario privada que no sea la primera identidad de usuario privada que esté asociada a la misma suscripción que la primera identidad de usuario privada.

2. Un método de acuerdo con la reivindicación 1, en el que dichas características del emparejamiento de la primera identidad de usuario privada y la identidad de usuario pública incluyen uno cualquiera o más de: un estado de autorización de sesión, un sistema central de origen, un dominio de origen, un nombre de usuario y una información que especifica el régimen de tarificación a aplicar al emparejamiento.

3. Un método de acuerdo con la reivindicación 2, que comprende transmitir el primer mensaje en respuesta a un segundo mensaje de la entidad de prestación de servicios (2) que solicita información sobre el emparejamiento.

4. Un método de acuerdo con la reivindicación 3, en el que el sistema es un sistema 3GPP/UMTS y el primer mensaje es un mensaje de respuesta de autenticación multimedia o un mensaje de respuesta de asignación de servidor.

5. Un método de acuerdo con la reivindicación 2, que comprende transmitir el primer mensaje en respuesta a la incorporación a la suscripción de una identidad de usuario privada.

6. Un método de acuerdo con la reivindicación 5, en el que el sistema es un sistema 3GPP/UMTS y el primer mensaje es un mensaje de solicitud de perfil de inserción.

7. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el sistema es un sistema 3GPP/UMTS y la entidad de almacenamiento de información de suscripción (3) es un servidor de abonado doméstico.

8. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el sistema es un sistema 3GPP/UMTS y la entidad de prestación de servicios (2) es una función de control de sesión de llamada en servicio.

9. Una entidad de almacenamiento de información de suscripción (3) para su uso en un sistema de comunicaciones en la que una característica de identidad de usuario privada puede emparejarse con una característica de identidad de usuario pública y puede asociarse más de una identidad de usuario privada a una suscripción; estando la entidad de almacenamiento de información de suscripción (3) configurada para transmitir a una entidad de prestación de servicios (2) del sistema un primer mensaje que contiene datos que especifican las características de un emparejamiento de una primera identidad de usuario privada y una identidad de usuario pública, caracterizada por que el mensaje también incluye una indicación de cualquier otra identidad de usuario privada que no sea la primera identidad de usuario privada que está asociada a la misma suscripción que la primera identidad de usuario privada.

10. Una entidad de almacenamiento de información de suscripción (3) de acuerdo con la reivindicación 9, en la que dichas características del emparejamiento de la primera identidad de usuario privada y la identidad de usuario pública incluyen uno cualquiera o más de: un estado de autorización de sesión, un sistema central de origen, un dominio de origen, un nombre de usuario y una información que especifica el régimen de tarificación a aplicar al emparejamiento.

11. Una entidad de almacenamiento de información de suscripción (3) de acuerdo con la reivindicación 10, estando la entidad configurada para transmitir el primer mensaje en respuesta a un segundo mensaje de una entidad de prestación de servicios (2) que solicita información sobre el emparejamiento.

12. Una entidad de almacenamiento de información de suscripción (3) de acuerdo con la reivindicación 11, en la que el primer mensaje es una respuesta de autenticación multimedia o un mensaje de respuesta de asignación de servidor.

13. Una entidad de almacenamiento de información de suscripción (3) de acuerdo con la reivindicación 10, estando la entidad configurada para transmitir el primer mensaje en respuesta a la incorporación a la suscripción de una identidad de usuario privada.

14. Una entidad de almacenamiento de información de suscripción (3) de acuerdo con la reivindicación 13, en la que el primer mensaje es un mensaje de solicitud de perfil de inserción.

15. Una entidad de almacenamiento de información de suscripción (3) de acuerdo con cualquier reivindicación anterior, en donde la entidad de almacenamiento de información de suscripción (3) es un servidor de abonado doméstico.

16. Una entidad de almacenamiento de información de suscripción de acuerdo con cualquier reivindicación anterior, en la que la entidad de prestación de servicios (2) es una función de control de sesión de llamada en servicio.

17. Una entidad de prestación de servicios (2) para su uso en un sistema de comunicaciones en la que una característica de identidad de usuario privada puede emparejarse con una característica de identidad de usuario pública y puede asociarse más de una identidad de usuario privada a una suscripción; siendo la entidad de prestación de servicios (2) sensible a recibir de una entidad de almacenamiento de información de suscripción del sistema un primer mensaje que contiene datos que especifican las características de un emparejamiento de una primera identidad de usuario privada y una identidad de usuario pública, caracterizada por que el mensaje también incluye un indicación de cualquier otra identidad de usuario privada que no sea la primera identidad de usuario privada asociada a la misma suscripción que la primera identidad de usuario privada para almacenar un registro para la suscripción que incluye una indicación de las otras entidades de usuario privadas.

FIG. 1